Protecting Personal Data and Privacy in the EU in the Rise of the Internet of Things

Liliana Pereira Martins dos Santos

Thesis to obtain the Master of Science Degree in

Information Security and Cyberspace Law

(MSIDC)

Supervisors: Prof. Dr. Alexandre Sousa Pinheiro, Faculty of Law, University of Lisbon / Prof. Dr. Carlos Caleiro, Instituto Superior Técnico, University of Lisbon

September 2018

Abstract

The Internet of Things is considered to be the engine behind the 4th Industrial Revolution. Nowadays, it is becoming increasingly common to experience at firsthand the developments of the Internet of Things, be it in wearable computing, quantified self, home automation “domotics”, in the environment of the smart cities or using smart transportations.

Some even refer to the Internet of Everything, and the tendency is towards growth: the growth of connected devices and the growth of potential fields of application for this technology.

However, despite its many potential applications and benefits, due to certain singularities, it also poses a challenge when it comes to personal data protection and privacy.

Although, the Internet of Things is the background of our research, there are (and, there will be) other technologies that do not qualify as IoT, but also give grounds for the necessity of protecting personal data and privacy. Therefore, in a sense, we can state that it is the dynamic between “technology”, *lato sensu*, and the protection of personal data and privacy within the European Union, that is the purpose of our present reflexion, with the nuance that “technology” is embodied here as IoT.

Keywords

Internet of Things; Personal Data; Data Protection; Privacy; GDPR; ePrivacy

Contents

Abbreviations

Charter of Fundamental Rights of the European Union - Charter

COM (2017) 10 final (Proposal for a Regulation of the European Parliament and of the Council) - ePrivacy Proposal

Data Protection Impact Assessment – DPIA

Denial of Service - DoS

Digital Single Market – DSM

Electronic Communications Data - ECD

Electronic Communications Privacy Act (1986) - ECPA

European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms) – ECHR

European Court of Justice – ECJ

European Data Protection Supervisor - EDPS

European Union – EU

Directive 2002/58/EC (Directive 2002/58/EC of the European Parliament and of the Council) - ePrivacy Directive

General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council) - GDPR

Internet of Things – IoT

Internet of Robotic Things – IoRT

Machine-to-Machine - M2M

Privacy by Design – PbD

Privacy Enhancing Technologies - PETs

Proposal for a Directive establishing the European Electronics Communication Code – EECC Proposal

Radio Frequency Identification – RFID

Stored Communications Act – SCA

Technical and organisational measures - TOMs

Treaty on the Functioning of the European Union – TFEU

United States – US

Virtual Machines – VMs

Chapter 1

Introduction

The present dissertation on the subject "*Protecting Personal Data and Privacy in the EU in the Rise of the Internet of Things",* was elaborated in the scope of the Master's Degree in Information Security and Cyberspace Law, lectured at Instituto Superior Técnico (University of Lisbon), Faculty of Law (University of Lisbon), and the Naval School.

The aim of this research is to provide a contribution on the subject of personal data protection and privacy in the context of the Internet of Things (hereafter, IoT), having as background the new European legal framework regarding the protection of personal data and privacy, applicable to the IoT.

The scope and extent of the protection granted to personal data and privacy by this new European legal framework, that for our purposes can be translated into knowing "how" and "where" will it impact the IoT, is meant to be the core of this research, and also the landscape for several questions that arise when we combine the central topics of our research: IoT, personal data and privacy.

When we make reference to the new European legal framework regarding the protection of personal data and privacy, there are two main legal references that are relevant for the IoT, and thus will be our stepping-stones, namely: the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council[1], hereafter, GDPR) and the ePrivacy Proposal (COM (2017) 10 final[2])[3].

The GDPR repeals Directive 95/46/EC and became applicable from 25 May 2018 onwards (Art. 99 GDPR). The ePrivacy Proposal repeals Directive 2002/58/EC[4] (also known as "EU cookie Directive", hereafter, ePrivacy Directive), and although it was also intended to become applicable from 25 May 2018 onwards (Arts. 27 and 29 ePrivacy Proposal), the entry into force of the future ePrivacy Regulation was delayed, therefore we will make reference to the ePrivacy Proposal.

The two legal texts that the GDPR and the ePrivacy Proposal aim to replace will also be present in our research in order to address the topic of the changes that the new legal framework represents, specifically for the IoT.

The choice of this topic of the protection of personal data and privacy combined with the IoT, was largely influenced by the potential impact that this technology is foreseen to have in our lives.

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

[2] 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) 10 final, Brussels, 10 January 2017.

[3] On the same topic also the Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223), Brussels, 16 September 2014, 10. Although the Opinion makes reference to the previous legal framework applicable to the IoT, considering that "the relevant legal framework to assess privacy and data protection issues raised by the IoT in the EU is composed of Directive 95/46/EC as well as specific provisions of Directive 2002/58/EC as amended by Directive 2009/136/EC", the same reasoning is valid under the current legal framework.

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31 July 2002.

IoT is considered to be the engine that is powering the 4th Industrial Revolution and is also, as we will see in the course of our research, a challenge when it comes to personal data protection and privacy.

The option to focus only on the European legal landscape was firstly, due to the possible extent that this research can have, and secondly due to the fact that its scope is not aimed at building a comparative overview of several data protection frameworks, but instead to explore in detail the evolution of the European perspective regarding personal data protection and privacy and its meaning for the IoT (which is also a technology still on an ascending phase).

Despite this option, there are relevant subjects in our research that cannot be approached only from an European perspective, namely the difference between “privacy” and the “protection of personal data”, that to be understood requires that a comparison is made between the European view and the United States (hereafter, US) view, since these are in fact two different dogmatic dimensions that need to be set apart before going into detail on the European legal framework relevant for IoT.

Another argument in favor of our focus on the European landscape is the fact that this new legal framework represents a step forward in the harmonization of the EU data protection rules.

So far, EU member states have had a wider margin on how to regulate these matters on a national level, since the Directives in place were only concerned with setting out goals that all EU countries must achieve, but leaving to the countries the possibility to devise their own laws on how to reach those goals[5].

The two new main legal references that are relevant for the IoT, when it comes to personal data protection and privacy, assume the form of regulations[6] (considering the fact, that the ePrivacy Proposal, is soon to be the future ePrivacy Regulation).

Taking the form of regulations they will provide a harmonized EU data protection regime[7] with common standards, and this regime will provide the same data protection rights across the EU member States.

This means that from the moment the regulations became enforceable, they also became directly binding and applicable for the EU member States, without the requirement of the EU national governments to pass any enabling legislation.

Despite the direct effect of the regulations[8], and taking the example of GDPR, domestic laws are to be expected in all EU member states, complementing or even modifying what is set out in the regulation, but only in the areas where the regulation itself allows any deviation[9].

[5] More information regarding the legal acts that the European legislator can choose to achieve the aims set out in the EU treaties, available at: https://europa.eu/european-union/eu-law/legal-acts_en (accessed 29 October 2017).

[6] The Treaty on the Functioning of the European Union (hereafter, TFEU), in its article 288 establishes the legal acts that the European legislator can choose to regulate a matter.

[7] According to the European Commission more than 90% of Europeans say they wish to have the same data protection rights across the European Union (hereafter, EU), http://ec.europa.eu/justice/data-protection/reform/index_en.htm (accessed 29 October 2017).

[8] In Case 43/71 Politi s.a.s. v Ministry for Finance of the Italian Republic (1971) ECR 1039, para.9, the Court clarified that regulations have a complete direct effect.

[9] The German Parliament was the first to pass an entirely new Federal Data Protection Act on 27 April 2017, the *Bundesdatenschutzgesetz* (hereafter, BDSG). More information, available at: https://www.swd-rechtsanwaelte.de/blog/datenschutzgrundverordnung-eu-mitgliedslaender/ (accessed 29 October 2017).

In this introductory chapter we also make reference to a preliminary overview on the relationship of technology, personal data protection and privacy, we put forward the topic of our research, approach its scope and limitations and the nature of our sources.

1.1. Technology and the Protection of Personal Data and Privacy

Although IoT is the background of our research there are (and, surely will continue to be developed) other technologies that do not qualify as IoT, but also give grounds for the necessity of protecting personal data and privacy (e.g. the IT applications, present in every modern company for processing the payroll of their associates).

In a sense, we can say it is the dynamic between "technology", *lato sensu*, and the protection of personal data and privacy, that is the purpose of our present reflexion, with the nuance that "technology" is embodied here as IoT.

Technological advances (IoT included) have been altering the extension and the scope of the protection that is given to personal data and privacy, the need to review and adapt the legal frameworks is also one side effect of these advances.

Nowadays, there are growing references to the implications that technology already has (and may have) in our lives. There are documentaries, movies, television series and articles focused only in capturing the dystopian future that might be ahead of us, if we do not address the potential downsides that the new technologies and the ever growing tendency to live in a connected world can bring.

One good example, is the British science fiction television anthology series "Black Mirror"[10], that goes beyond the well-known dystopian future pictured in Orwell´s "Nineteen Eighty-Four", to bring us the dark side of life and technology, examining modern society and the possible consequences of the adoption of new technologies in our routine.

In Orwell[11], we saw the connection between the dangers of surveillance technologies[12] (that allowed the establishment of a totalitarian state with control over the public) and the consequent replacement of individual freedom and self-determination with an atmosphere of control, made possible with the resource to technology.

In comparison, in "Black Mirror", we can see the importance of social rating, the use of "grains" implants that record everything a person sees and hears, the consequences of ransomware, among others.

This comparison is only an example of our growing and modified perception (even when it comes to fiction) of the potential that technology has to shape our lives, and in some cases (e.g.

[10] Overview, http://www.imdb.com/title/tt2085059/ (accessed 29 October 2017).

[11] George Orwell, *Nineteen Eighty-Four* (Penguin Books, 2003), 1.

[12] For a more detailed analysis regarding the dynamics between surveillance and privacy protection, see: David H. Flaherty, "Controlling Surveillance: Can Privacy Protection Be Made Effective?", in *Technology and Privacy: The New Landscape* (Cambridge/US: MIT Press, 1997).

ransomware[13] or the “social credit” system that China plans to implement[14]) we are no longer in the field of imagination, but in a reality already experienced by many.

As E. Agre argues:

> *As new technologies are adopted and incorporated into the routines of daily life, new wrongs can occur, and these wrongs are often found to invalidate the tacit presuppositions on which ideas about privacy had formerly been based*[15]*.*

Although these preliminary references to the potential side effects of technology in our lives were focused on the downsides, there are more than enough examples of the advantages that the use of technology has brought to us in many different fields, from medicine, to heavy factory work (now done in many cases with the help of robots), and mainly everywhere where a computer can be found to assist us with our tasks.

Our option to start with a more detailed reference to the downsides of the use of technology has to do, on the one hand, with the demonstration of our altered perception of what is nowadays a “threat”, and on the other hand, with the fact that one of the potential (depending on the purposes) negative effects of the use of technology, is the possibility that it has to capture details about ourselves that makes us unique.

These details about ourselves that makes us unique and identifiable constitute in many cases personal data (afterwards, we will explore the legal definition of personal data and draw the boundaries of what is in and out of scope of this definition).

The need for a compromise between personal data protection (and, privacy) and the development of technology is clear, there is a visible link between the advances of technology and its ability to be embedded in our daily routines. As stated by Victoria Bellotti, when addressing the issue of a design for privacy in multimedia computing and communications environments:

> *New multimedia communications and computing technology is potentially much more intrusive than traditional information technology because of its power to collect even more kinds of information about people, even when they are not directly aware that they are interacting with or being sensed by it*[16]*.*

[13] For an overview about ransomware, its impact and major threats, see: Dick O´Brien*,”* Internet Security Threat Report, ISTR Ransomware 2017 – An ISTR Special Report”, Symantec Corporation (July 2017) https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf (accessed 29 October 2017).

[14] Regarding the “social credit” system planned for China, see: Celia Hatton*,”* China “social credit”: Beijing sets up huge system”, (October2015), http://www.bbc.com/news/world-asia-china-34592186 (accessed 28 January 2018). The planned system goes beyond the existing and implemented concepts of credit systems that are used to predict if individuals will pay their mortgages or credits on time, its aim is to evaluate and rate each individual’s trustworthiness. The idea behind is to have every citizen enrolled in a national database that compiles fiscal and government information, that information is aimed at ranking every citizen. Some pilot companies like “Sesame Credit” (a company that rates the online financial transactions of those who use Alibaba’s payment system) have already introduced the “social credit” system, and with it the judgment of the types of products that customers buy online, which in return impacts their trustworthiness.

[15] Philip E. Agre, *Technology and Privacy: The New Landscape* (Cambridge/US: MIT Press, 1997), 7.

[16] Victoria Bellotti, “Design for Privacy in Multimedia Computing and Communications Environments”, in *Technology and Privacy: The New Landscape* (Cambridge/US: MIT Press, 1997), 64.

1.2. Scope and Limitations

As we argued above, it is an undeniable truth that for better or worse, technology has become a relevant and increasingly important piece of our daily routines.

For the average citizen, the resource to technology has become a natural part of his activities in his work and private life. From the app in our mobile device that allows us to buy our subway ticket just in time for the next one, to the laptop that assists us in almost all sorts of tasks in our work, we have seen technological advances silently embedding in a wide range of areas in our lives.

However, these are just examples that by now, we are used to see basically everywhere (and probably, find it strange when they are not available), and are far from representing the full scope of technological advances that became a part of our daily routines and interactions.

Technology is developing faster than ever when compared to the advances we saw taking place in the 80´s or 90's[17], and we have now available an entire constellation of IoT devices, ready to make our lives easier. It is not just the ever growing variety of mobile apps, or powerful computers that are here to assist us just a "click" away, it is the promise of a "connected" existence that is just around the corner.

The IoT, is ready to make our connected world smarter and more efficient, presenting solutions for smart cities (e.g. smart roads, smart parking, waste management), smart environment (e.g. forest fire detection, air pollution), smart water (e.g. river floods, chemical leakage detection in rivers), smart metering (e.g. smart grid), and more, much more.

The study of the potential applications of IoT technology is also a part of our research, not only to provide an overview of the immense potential of this technology that is empowering what is becoming known as the 4th Industrial Revolution, but also to provide the "scenarios" where we might find a necessity to consider the requirements laid down by the new European legal framework for personal data protection and privacy.

Also relevant, is an understanding of the security issues that affect the IoT, as they may represent a source of potential risks for personal data if such data is being processed. This analysis of the security issues of the IoT does not intend to be exhaustive nor provide guidance or best practices for this area, since this is not the scope of our research.

However, as they may represent a risk for personal data (when this data is processed) they have to be considered here. These are issues that can assume a growing relevance for topics foreseen in the new European legal framework (e.g. they might have to be considered in regards to privacy by design or be included in a Data Protection Impact Assessment, hereafter, DPIA).

[17] Regarding the technological advances that have taken place and became embedded in our daily routines, see: Daniel Solove, *The Digital Person – Technology and Privacy in the Information Age (*New York University, 2004). Here the Author reflects about the protection of privacy in light of the technological developments of our time that affect the way we shop, bank and overall conduct our daily business, arguing that these changes have resulted in an unprecedented proliferation of records and data that did not exist before, since there was no technology available to make this possible. This collection of detailed data about an individual by digital means is referred to as "digital dossiers".

Although the study of the potential applications or security issues surrounding the IoT is a part of our research, for the reasons we briefly explained above, these topics are not the central subject of our research.

The central questions that we are aiming to answer in our dissertation are:

- How (applicable regulations, legal basis for processing, legal requirements to consider, among others), and;
- Where (in which situations) is the new European legal framework regarding the protection of personal data applicable to the IoT.

In our final chapter dedicated to the "*Key Aspects of Personal Data Protection and Privacy for the Internet of Things in the European Legal Framework"* we aim to "connect the dots" between the relevant points of the European legal framework and the IoT.

In sum, having these main purposes of our research in mind, by connecting the topics of IoT, privacy and personal data protection in the EU, we aim to provide our contribution, towards the goal of understanding and addressing the potential effects of the identified risks that the IoT technology represents for the protection of personal data and privacy of the data subjects/end-users, when the processing activity falls under the scope of the new European legal framework for personal data protection and privacy.

1.3. Sources

This dissertation is based on materials collected from publicly accessible sources of information which comprehend legal and non-legal subject related publications, as well as pertinent case law and EU legislation.

Chapter 2

Status Quo: the Coming of Age of Personal Data Protection and Privacy in the EU in the Rise of the Internet of Things

The overall objective of this chapter is to build an overview regarding the *status quo* of personal data protection and privacy in the EU and simultaneously of the IoT.

As it can be deducted already from the chosen title, these are topics that are in different maturity levels. IoT is a topic currently on the rise, and some even suggest that it is not currently a reality:

> *Although expectations in IoT are high, some experts think they may be "inflated" as the IoT would still be far from a real take-off. Studies suggest that IoT is not widely implemented and that, properly speaking, no Internet of Things exists as such (Gartner 2014)*[18]*.*

While personal data protection and privacy in the EU (especially with these new developments of the coming into force of the new European legal framework), is reaching what could be considered a state of maturity.

The aim of this chapter, similarly to the aim of the overall research, is not to have a separate approach of personal data protection and privacy in the EU and of the IoT, since to derive conclusions regarding our core questions both topics need to be "merged" .Therefore, this chapter is directed also at linking both topics together and finding out the preliminary contact points between them.

For the purpose, of bringing the two topics together, first it is required to gain a general vision, in terms of strategy for the IoT, on a European level. This means to understand the goals that are defined by the EU for the IoT and the role and importance of the IoT for the implementation of the Digital Single Market (hereafter, DSM).

In a next step, it is required to take a look at the European legal framework for the protection of personal data and privacy that is applicable to the IoT, and understand why and how it can be relevant for the IoT.

Also required (to put the applicable legal framework into perspective), is to gain an understanding of the "values" at stake behind the European regulations. This means to understand what are the fundamental right(s) that the regulations aim to protect, and in our particular case, also to approach the dogmatic difference between "privacy" and "data protection" (two expressions that are not synonyms).

Finally, a clearer understanding of the IoT and its background needs to be build.

2.1. An Overview of the European Strategy for the Internet of Things

As discussed above, to begin this chapter with an overview of the European strategy for the IoT, ensures the purpose of bringing the two topics together (personal data protection and privacy in the EU and the IoT), providing also a general vision, in terms of strategy for the IoT, on a European level.

Through the understanding of the European strategy for the IoT we can derive the role that IoT is planned to play in the future of Europe's digitization (namely, in the implementation of the Digital Single Market), and clarify the goals set by the EU for the IoT and the concerns regarding data protection.

The advent of the digital age, where IoT is included and foreseen to be one of its major "players", has brought several opportunities but also challenges and concerns both to States and organizations worldwide.

[18] Ugo Pagallo, Massimo Durante, Shara Monteleone, "What is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT", in *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer, 2017), 61.

> *Digitization and the free flow of information, in this sense, is conceived as a societal need of utmost importance both in order to maintain and develop Europe's prosperity and to demonstrate competitiveness and thus to underscore Europe's global influence[19].*

So, before going any further, we should first clarify why it has become so relevant that States (in our particular case, EU Member States) consider these topics in their policies and strategies on a European level.

Nowadays, it is has become clearer that keeping a "digital agenda" is not only a competitive advantage, but also a matter of keeping sovereignty in an ever growing digital world[20].

To understand the importance of Europe keeping up the pace with digital advances in order to ensure a digital sovereignty, some parallel and primary concepts need to be set forth since they are the "background" for any topic concerning the connected world, namely the concept of "cyberspace" and the concept of "global commons".

These two concepts, as we will clarify, are so deeply connected that one is actually a part of the other. As we describe below, the nature and characteristics of cyberspace should be taken into consideration in any strategy that involves connectivity, even if they are not mentioned as a goal to achieve.

The cyberspace has several dimensions, in line with Derek S. Reverson, we can consider it includes: physical hardware (e.g. networks and machines), information (e.g. data), the cognitive and the virtual. When these dimensions are combined we obtain the fifth dimension, what we think of as cyberspace[21].

There are several definitions of cyberspace, however it is common to refer to the definition of cyberspace presented by the DoD – *United States Department of Defense:*

> *A global domain within the information environment consisting of the interdependent network of information technology, infrastructures, and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers[22].*

As mentioned, cyberspace is deeply connected with another important concept, the concept of "global commons".

The "global commons" are areas that historically represent the principle of common heritage of mankind, and are traditionally identified by international law, as follows[23]:

- The High Seas;
- The Atmosphere;

[19] Murat Karaboga, Tobias Matzner, Hannah Obersteller, Carsten Ochs, "Is There a Right to Offline Alternatives in a Digital World", in *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer, 2017), 52.

[20] Manuel Castells, *The Power of Identity,* The Information Age: Economy, Society, and Culture, Volume 2 (Wiley-Blackwell, 2010), 303, approaches the topic of the changing role of nation-states along with the globalization of technology and its effects, namely the growing power of non-state actors.

[21] Derek S. Reverson, *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World,* (Georgetown University Press, 2012), 4.

[22]Available at: https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf, (accessed 21 December 2017).

[23] http://staging.unep.org/delc/GlobalCommons/tabid/54404/Default.aspx

- Antarctica, and;
- Outer Space.

In fact, cyberspace is also considered to be one of the “global commons”[24], due to its nature and characteristics highlighted above, thus assuming a key role alongside with the traditional global commons in which common property resources are found.

IoT (which by essence requires a connection to the internet) and the digital technologies, in general, are “components” of this most recent “global common”, the cyberspace.

IoT technologies can therefore be affected by some of the dangers that populate the cyberspace, and in return, can also (if not properly developed or implemented) create dangers that can affect the cyberspace.

This fact alone, demonstrates the strategic importance of IoT, not only in terms of its development in accordance with cyberspace “preservation” and security (thus the need to considerate also cyberspace nature and characteristics in any strategy involving connectivity), but also in terms of the strategic value it can add to those who are ahead in its development and implementation.

The States that are able to develop and implement IoT technologies, preserving the security of the required data flows that take place in the cyberspace, will reap its various benefits (in section 2.4., we develop the topic of the benefits and potential applications of the IoT).

After this brief overview of the “background” concepts that surround the IoT, we are now in a better position to clarify why it is important that EU Member States consider the IoT in their policies and strategies on an EU level, going through expected goals and the several aspects of the European strategy designed for the IoT that illustrate its connection with personal data protection and privacy.

As Karaboga, Matzner, Obersteller and Ochs clarify, both the EU Member States with their national strategies and the European Commission have been playing an active role, in order to boost and shape the developing IoT markets[25].

The first effort on this direction was COM (2007) 96 final, which had a focus on Radio Frequency Identification (hereafter, RFID)[26], and already there we could see a reflex of the concerns that were risen with the matters of data security and data privacy.

In point 3.2. of COM (2007) 96 final, entitled “Data protection, privacy and security” it is mentioned that the public debate held about RFID brought to light serious concerns that this technology could endanger privacy, since it could be used to collect information that is considered to be personal data (information that is directly or indirectly linked to an identifiable or identified person).

[24] Vítor Rodrigues Viana, *IDN Nação e Defesa*, 133 (Instituto da Defesa Nacional, 2012), 5.

[25] Karaboga, Matzner, Obersteller and Ochs, op. cit., 48-49.

[26] Communication from the Commission to the Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework,* COM (2007) 96 final, Brussels, 15 March 2007. As defined in this Communication: “Radio frequency identification (RFID) is a technology that allows automatic identification and data capture by using radio frequencies. The salient features of this technology are that they permit the attachment of a unique identifier and other information – using a micro-chip – to any object, animal or even a person, and to read this information through a wireless device. RFIDs are not just "electronic tags" or "electronic barcodes". When linked to databases and communications networks, such as the Internet, this technology provides a very powerful way of delivering new services and applications, in potentially any environment”.

Besides its advantages, improving efficiency in sectors such as transports (e.g. improving efficiency and security), healthcare (e.g. improving medication compliance), retail (e.g. reduce supply shortages or theft) and others[27], this technology could also bring several risks for personal data:

> *RFID tags may store personal data such as on passports or medical records; RFID technology could be used to track/trace people's movements or to profile people's behavior (e.g., in public places or at the workplace)[28].*

Even on its primary efforts, towards a strategy to actively develop the IoT markets (in case, initially oriented towards RFID), we can find a balance between the benefits of the technology and the concerns towards data protection, privacy and security.

On a later phase, the Commission published COM (2009) 278 final[29], contemplating an action plan for Europe concerning the IoT[30].

This paper highlights the importance of the IoT as "the umbrella for a new paradigm" recognizing this technology as the major next step in the growth of the Internet, by means of progressing and evolving from "a network of interconnected computers to a network of interconnected objects, from books to cars, from electrical appliances to food, and thus create an 'Internet of things'"[31].

Despite, this connection to the Internet, both in terms of functioning as of later development, the Commission clarifies that the IoT nature is complex, and it should not be seen as an extension of the Internet.

Instead, IoT should be seen, as a series of new independent systems that operate with their own infrastructures, and in doing so, also rely partially on the existing Internet infrastructures.

The paper mainly explores, existing IoT applications, discusses the issue of governance of the IoT (e.g. the role of public authorities) and how to lift the obstacles that stand in the way of the development and prosperity of the IoT.

It is on this last mentioned aspect, that we find once again some concerns related to privacy and the protection of personal data, as well as to security issues.

Privacy and the protection of personal data are seen as a potential obstacle in the development of the IoT, since when they are affected also the trust in this technology and its social acceptance are injured.

In order to prevent that, the Commission recommends, as a prerequisite, that appropriate data protection measures are put in place, and sets forth two distinct lines of action.

The first line of action, is focused on the continuous monitoring of the privacy and data protection questions, by means of:

[27] COM (2007) 96 final, 3-4.

[28] COM (2007) 96 final, 5.

[29] Communication from the Commission to the Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Internet of things – An action plan for Europe,* COM (2009) 278 final, Brussels, 18 June 2009.

[30] Karaboga, Matzner, Obersteller and Ochs, op. cit., 49, point out that this is still a strategy with a focus on RFID.

[31] COM (2009) 278 final, 2.

- Consulting the Article 29 Data Protection Working Party;
- Providing guidance on the adequate interpretation of EU legislation;
- Promoting dialogue among stakeholders, and if required;
- Proposing additional regulatory instruments.

The second line of action, is regarding the promotion of a debate around the topic “silence of the chips”, that expresses the possibility of individuals being able to disconnect from the network environment[32].

The security topic, *stricto sensu*, is considered to be closely linked to the privacy topic, and the importance of taking into account a privacy-and security-by-design mindset in the conception phase of the IoT components, is already mentioned by the Commission.

More recently, the Commission launched SWD (2015) 100 final, a DSM Strategy for Europe[33]. The paper central subject is focused on answering the question “Why we need a DSM?” the foundations required to make it a reality and the benefits that can be generated from its implementation.

The development of the DSM is aimed at ensuring that Europe maintains its position as a world leader in the digital economy and to help the global growth of European companies. Personal data protection is one of its ingredients:

> *A Digital Single Market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence[34].*

The paper also makes reference to the necessity of exploring innovations such as Cloud computing, Big Data tools and the IoT, considering them to be central to EU’s competitiveness[35].

The latest development, from the Commission in terms of its strategy for the IoT, was SWD (2016) 110 final, “Digitising European Industry - Reaping the full benefits of a Digital Single Market”[36], where it is recognized that advances in technologies such as the IoT are “transforming products, processes and business models in all sectors ultimately creating new industrial patterns as global value chains swift”[37].

[32] Regarding this particular topic, Karaboga, Matzner, Obersteller and Ochs, op. cit.

[33] Communication from the Commission to the Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Market Strategy for Europe,* SWD (2015) 100 final, Brussels, 6 May 2015.

[34] SWD (2015) 100 final, 3.

[35] SWD (2015) 100 final, 14.

[36] Communication from the Commission to the Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Digitising European Industry – Reaping the full benefits of a Digital Single Market,* SWD (2016) 110 final, Brussels, 19 April 2016.

[37] SWD (2016) 110 final, 2.

However, following the tendency of the previous papers, also here, the fact that the further development of Big Data and the IoT represent major trust and security challenges for the companies, as well as for public acceptance, is referenced as a concern[38].

Apart from these actions, also strategic efforts on research regarding the IoT have been made on an EU level, e.g. through the creation of the European Research Cluster on the Internet of Things (IERC) that is the center of IoT research in Europe and the Alliance for the Internet of Things Innovation (AIOTI), among others initiatives aimed to boost research and knowledge on this field.

When it comes to the foundations of the IoT, the policy priorities set by the European Commission, make clear they rest on three pillars[39], namely:

- A thriving IoT ecosystem;
- A human-centered IoT approach, and;
- A single market for IoT.

In sum, the role that IoT is expected to play in the future of Europe's DSM, can be summarized through the European Commission mission and vision for the IoT:

> *We believe that the Internet of Things has the potential to drastically improve our lives, our work places and our industrial efficiencies and capabilities while taking into account security, privacy and trust requirements*[40].

2.2. The European Legal Framework regarding the Protection of Personal Data and Privacy Applicable to the Internet of Things: The General Data Protection Regulation and the ePrivacy Regulation

In Chapter 1, we began our introduction with a reference to the new European legal framework regarding the protection of personal data and privacy that is applicable to the IoT, followed by an overview of the strategic approach for the IoT, on an European level, with the purpose of building a general vision that could help bring both topics together (IoT, privacy and personal data protection in the EU).

In the following sections we will proceed with a breakdown structured approach, starting with an analysis of the scope of application of both regulations in this section, going further into detail in the next section uncovering the different fundamental rights protected by both regulations, and to terminate this chapter once again "connecting the dots", providing an overview of the development and current status of the IoT which is required to achieve an understanding of the maturity levels of both, the IoT and the legal framework applicable to it.

[38] SWD (2016) 110 final, 5.

[39] https://ec.europa.eu/digital-single-market/en/blog/internet-things-iot-you-our-mission-and-vision, (accessed 23 December 2017).

[40] https://ec.europa.eu/digital-single-market/en/blog/internet-things-iot-you-our-mission-and-vision, (accessed 23 December 2017).

As mentioned the two main legal references that should be considered are: the GDPR and the ePrivacy Proposal.

In this section our goal is to provide an introductory overview of this legal landscape that will be the basis to find the answers for our central questions: how and where (in which situations) is the new European legal framework regarding the protection of personal data and privacy applicable to the IoT.

In order to do so, we have identified two primary questions that should be answered to place both regulations into perspective:

- What is the scope of both regulations?
- What are the contact points between both regulations?

An in depth overlapping of both, the GDPR and the ePrivacy Proposal, is reserved for Chapter 4, where we will place them into perspective having the IoT as a background, and look for answers to questions, such as the following one: will there be a prevailing regulation when it comes to IoT?

Starting with our first question, aimed at understanding the scope of both regulations (and ultimately, in which case will the regulations be applicable), there are two dimensions that need to be analyzed in order to delimit their scope of application, namely: the material scope and the territorial scope.

The GDPR regulation is clear regarding its material and territorial scope of application. The material scope is regulated in art. 2, where it is mentioned that:

> *1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system[41].*

As it can be understood from the wide material scope set by the European legislator, GDPR is applicable to “any processing of personal data”[42].

The first element that stands out in the material scope defined by the European legislator is that the data in question has to be “personal data” so that regulation is applicable. Art. 4 (1) GDPR clarifies that data is considered to be personal if the information is related to an *identified or identifiable natural person*, the “data subject”[43].

Therefore, for data to be considered “personal” it is enough if the identification of a person is made possible by using a combination of different factors or information.

[41] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) - A Practical Guide* (Springer, 2017), 11, give the example of a medical practice that stores patient data in paper records, organized alphabetically in several cabinets, based on surnames, as an example of records that contain personal data and are part of a filing system, to which GDPR is applicable.

[42] Ibid., 9. The Authors emphasize the fact that the Regulation will become relevant for organizations from the moment that any personal data processing takes place. There are, however, very residual cases in which organizations are left out of the GDPR scope regarding some specific obligations (rec. 13 and art. 30 (5) GDPR, where to take into consideration the situation of micro, small and medium-sized companies the EU legislator included a derogation for organizations with fewer than 250 employees with regard to record-keeping – also this derogation has its own “exceptions” – if the processing is likely to result in a risk for the rights and freedoms of the data subjects, if it’s not occasional or includes special categories of data, the derogation is not applicable).

[43] Rec. 27 GDPR, clarifies that the regulation does not apply to the personal data of deceased persons.

This identification can be done "directly" or "indirectly", by reference to an identifier that distinguishes and separates the individual from the "crowd".

Possible identifiers are:

- Name;
- An identification number (e.g. ID number, tax number);
- Location data;
- An online identifier[44] ;
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.

The broad material scope of GDPR application must be linked with the meaning of "processing", and also with the territorial scope defined in the regulation, in order to verify if the obligations imposed are indeed applicable to a given company that is processing personal data.

"Processing" operations set the context in which personal data is being handled, by analyzing the definition of processing for the purposes of GDPR, we are able not only to understand the several contexts in which personal data can be processed, but also to define a timeline of reference for the personal data processing relevant activities.

In a general sense, we can say that the beginning of the processing activities start with the "collection" of personal data and end with its "erasure or destruction".

As mentioned in art. 4 (2) GDPR, processing is:

- Any operation or set of operations;
- Performed on personal data or on sets of personal data;
- Whether or not by automated means.

The isolated operation or set of operations can range from collection to erasure or destruction of personal data, and include in between: recording; organization; structuring; storage; adaptation or alteration; retrieval; consultation; use; disclosure by transmission; dissemination or otherwise making personal data available; alignment or combination, and restriction of personal data.

This also broad definition of "processing" means that even the personal data that is displayed on a computer screen is being processed, the same happens with any personal data that is being stored in the cache of a browser for limited time[45].

This also means that, not only computers, but any device capable of processing data (e.g. smart devices, webcams, among others) can be relevant for the applicability of the regulation, thus the regulation can be applicable to IoT devices (if they process personal data).

Linking the definition of "processing" laid down in the regulation with its material scope, we can conclude that it was the intention of the European legislator to cover in all possible extent personal data processing activities, and as mentioned in rec. 15 GDPR, to prevent any serious risk of circumvention.

The territorial scope is regulated in art. 3, where it is mentioned that:

[44] Rec. 30 GDPR, gives examples of some online identifiers that can be associated to natural persons. Those identifiers can be provided by devices, applications, tools and protocols, and can be IP addresses, cookie identifiers or RFID tags, among others.

[45] Examples from Voigt and von dem Bussche, op.cit., 10.

1. *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*
2. *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
   a) *The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or;*
   b) *The monitoring of their behavior as far as their behavior takes place within the union.*
3. *This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*

The regulation sets forth an extended territorial scope of application. This broadened scope of application is one of the major changes introduced with GDPR[46].

However, before analyzing in detail, the territorial scope of application of GDPR, it is required to explain the concepts of "controller" and "processor" laid down in this article, and that are present in all GDPR.

If we take into consideration an overview of all the articles that compose GDPR, it is easy to identify that the vast majority of obligations that are contained in it, are destined to be fulfilled by the "controller". This logic has to do with the different roles that are to be played by the controller and the processor.

The "controller" is defined in art. 4 (7) GDPR, as being:

- The natural or legal person, public authority, agency or other body;
- That alone or with others;
- Determines the purposes and means of the processing of personal data.

This means, that it is the controller, the one who defines "why" and "how" personal data is processed.

On the other hand, the definition of "processor" laid down in art. 4 (8) GDPR, diverges from the above one, since there is no definition of purposes or means of processing personal data done by the processor, on the contrary, the processor only processes personal data on behalf of the controller[47].

[46] Regarding the major changes introduced with GDPR, the territorial scope principles and their application: Sontje Julia Hilberg*,"* EU General Data Protection Regulation – What remains? What changes?", Deloitte, https://www2.deloitte.com/dl/en/pages/legal/articles/eu-datenschutzgrundverordnung.html (accessed 17 February 2018).

[47] Art. 29 GDPR, also contributes to clarify the role of the processor, stating that neither the processor nor any person acting under the authority of the controller (or processor, if there was an engagement of another processor with prior specific or general written authorisation of the controller, according to art. 28 (2) GDPR) shall process personal data aside from the instructions given by the controller, unless the same is required by Union or Member State law.

After this brief introduction to the concepts of “controller” and “processor”, we can now go further in detail, into the extended territorial scope of application defined in GDPR. There, in art. 3 (1) GDPR we can find the *subsidiary or establishment principle.*

This principle states that what is relevant to determine if GDPR is applicable, is not the place where the data processing activities take place, but the place where the subsidiary is located.

This principle is complemented by the *market place principle* laid down in art. 3 (2) GDPR. For this principle to be applicable it is required that the controller or processor are not established in the Union and one of the processing activities foreseen in art. 3 (2) a) or b) GDPR takes place.

Both principles complement each other, with the clear intention to extend the scope of application.

The processing activities covered in art. 3 (2) a) GDPR, relate to the offering of goods or services, whether these offerings were made free of charge or if they were done in return for payment.

Since the establishment of the controller or processor is not in the Union, it becomes relevant to precise what are the conditions that have to be in place to presume that an offering of goods or services is intended to address citizens within the EU.

According to rec. 23 GDPR, some factors make it apparent that there is an intention of offering goods or services to data subjects in the Union. Such factors can be the use of a language or a currency generally used in one or more Member States (with the possibility of ordering goods or services in that other language), or the explicit mention to customers or users located in the Union.

The processing activities covered in art. 3 (2) b) GDPR, relate to the monitoring of data subjects behavior, but only if their behavior takes place within the Union. In this case it becomes relevant to determine whether a processing activity can be considered to monitor the behavior of data subjects.

According to rec. 24 GDPR, to determine if a processing activity has the purpose of monitoring the behavior of data subjects, it should be ascertained if the natural persons are being “tracked” on the internet.

This tracking includes the possibility of further use of personal data processing techniques that are able to do a profiling of the natural person, with the intention of taking decisions regarding this person or to analyze or predict personal preferences, behaviors and attitudes.

Now turning our attention to the ePrivacy Proposal, that alongside with GDPR will form the relevant legal landscape for IoT in Europe when personal data is processed, the same analysis regarding its scope of application can be performed.

Similarly to GDPR, also the ePrivacy Proposal regulates its material and territorial scope of application.

Starting with the material scope, defined in art.2 of the ePrivacy Proposal, it is stated that the regulation is applicable to:

> *The processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.*

From the definition of material scope alone that is provided, it is not clear if the regulation is potentially applicable to the IoT.

However, if the material scope describe in art.2 is interpreted in connection with rec.12, and alongside with this connection, also a clarification of the terms used to describe the material scope is performed (e.g. electronic communications service, terminal equipment, end-users), it becomes clear that the regulation applies to IoT[48].

The European legislator starts rec.12 with a recognition that IoT is becoming a growing issue, since connected devices and machines are increasingly communicating with each other by means of electronic communications networks (IoT).

It is also made clear in this recital that the transmission of Machine-to-Machine (hereafter, M2M) communications that is taking place in the IoT, involves the conveyance of signals over a network, therefore this communication usually constitutes an *electronic communications service[49].*

This clear application of the ePrivacy Proposal to IoT, is also corroborated by the materialization of the terms present in the definition of its material scope.

The terms used to describe the material scope of the regulation are defined in its art.4 under "definitions".

There it is stated that the applicable definitions of "electronic communications service" and "end-user", can be found in art. 2 of the Directive establishing the European Electronics Communication Code[50] (art.4 (1) b) of the ePrivacy Proposal), while the definition of "terminal equipment" can be found in point (1) of art.1 of Commission Directive 2008/63/EC[51] (art.4 (1) c) of the ePrivacy Proposal).

Starting with the definition of "electronic communications service", according to art.2 (4) of the *Proposal for a Directive Establishing the European Electronics Communication Code* (hereafter, EECC Proposal), the same can be decomposed in three main points:

- A service normally provided for remuneration;
- Via electronic communications networks;
- Encompassing "internet access service"; and/or "interpersonal communications service"; and/or services consisting wholly or mainly in the conveyance of signals (e.g. transmission services used for the provision of machine-to-machine services and for broadcasting).

[48] Also Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223), mentioned above, made clear that the specific provisions of Directive 2002/58/EC as amended by Directive 2009/136/EC were part of the relevant legal framework to assess privacy and data protection issues raised by the IoT in the EU.

[49] Not only M2M communication is common in the smart world, also Machine-To-Cloud (M2C) communication is considered a typical form of communication. More on this topic: Béni-Tresor Akimana, Maxim Bonnaerens, Jonas Van Wilder, and Bjorn Vuylsteker, "A Survey of Human-Robot Interaction in the Internet of Things", December 2016,https://www.researchgate.net/publication/318722691_A_Survey_of_HumanRobot_Interaction_in_the_Internet_of_Things (accessed 24 February 2018).

[50] Proposal for a Directive of the European Parliament and of the Council, establishing the European Electronic Communications Code (Recast), COM (2016) 590 final/2, Brussels, 12 October 2016.

[51] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008, 20-26).

This definition goes in line with rec.12 of the ePrivacy Proposal, confirming that the transmission of machine-to-machine communications that occurs in an IoT environment fulfills the definition of an electronic communications service.

Regarding the definition of "end-user", the same is provided in art.2 (14) of the EECC Proposal, as:

- A user not providing public communications networks, or;
- Publicly available electronic communications service.

This definition will be explored in detail in Chapter 4, alongside with the concept of "data subject" adopted by GDPR, to approach the hypothesis of this different terminology dwelling into a different level of protection for those who are under the radar of both legal instruments (e.g. those who interact with smart devices where their personal data is being processed).

Finally, the definition of "terminal equipment" that can be found in point (1) of art.1 of Commission Directive 2008/63/EC, states that:

- Equipment that is, directly or indirectly;
- Connected to the interface of a public communications network;
- To send, process or receive information.

A terminal equipment can therefore be a computer, a Smartphone, or any device connected to the internet, that is able to send, process or receive information, namely an IoT device (e.g. devices used in wearable computing, such as medical or fitness trackers, or in home automation, among many others).

Regarding the territorial scope, defined in art.3 of the ePrivacy Proposal, the same is defined with resource to the positive verification of one of three situations, clustered as below:

> *(1) This Regulation applies to:*
>
> *a) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;*
>
> *b) the use of such services;*
>
> *c) the protection of information related to the terminal equipment of end-users located in the Union.*

Once more, the materialization of the terms used to describe the material scope is useful to provide clarity to the territorial scope of application as well (e.g. electronic communications service, terminal equipment, end-users).

The regulation is therefore applicable to: electronic communications services that are provided to (or used by) end-users located in the Union, and also to the information related to their terminal equipment (when the end-user is located in the Union).

The logic of the application scope, both material and territorial, largely rests on the "end-user" concept that we will explore in detail in another chapter.

Another aspect that could be of relevance for the development and commercialization of IoT products (however, not for our research which is concerned with the protection of personal data), is the fact that the ePrivacy regulation is also potentially applicable to IoT, even if personal data is not being processed.

This is possible since the communications that are protected with the regulation may contain non-personal data, this aspect is clearly mentioned in point 3 of the ePrivacy Proposal, and it also constitutes a difference between both regulations.

While GDPR is aiming only for the protection of personal data, the ePrivacy Proposal is aiming to ensure the confidentiality of communications, these communications may contain non-personal data and data related to a legal person.

From what has been described so far, there is a duality of relevant regulations applicable to regulate over IoT topics when personal data is being processed (and, when we are within the scope of the regulations).

This duality of potential applicable dispositions of two different regulations that are relevant for the IoT could generate a conflict of rules, in case both regulations contained rules over the same matter. Therefore, the relationship between GDPR and the ePrivacy Proposal needs to be clarified.

To cast some light into this duality of potential applicable regulations, the European legislator clarified in the ePrivacy Proposal that it constitutes *lex specialis* in regards to the GDPR, complementing it in the cases that electronic communications data (hereafter, ECD) qualify as personal data.

This means, according to point 1.2. of the Explanatory Memorandum of the proposal, that all the issues concerning the processing of personal data that are not specifically addressed by the ePrivacy Proposal are covered by the GDPR[52].

As a brief conclusion of this overview of the application scope of both regulations, we can state that although there is a duality of regulations, (apparently) overlapping to regulate the topic of personal data protection and privacy in the IoT, the way the regulations are expected to relate to one another should dissipate most of the uncertainties.

Adding to this, both regulations are also far from being completely coincident even in terms of scope, a clear example of that, is the focus of the ePrivacy Proposal (similarly to the ePrivacy Directive) on the confidentiality of communications, which may contain non-personal data and data that is related to a legal person, which are distinct differences from GDPR, that is not concerned with non-personal data and only grants protection to natural persons (art. 1 (1) GDPR, regarding its "*subject-matter and objectives*").

[52]Tobias Lock, *The European Court of Justice and International Courts*, (Oxford University Press, 2015), 51, regarding the principle *lex specialis derogat legi generali*, states that the rationale behind this principle is to solve norm conflicts in favour of the more specific rule, because this is the rule that best reflects the intentions of the parties concerned. The Author also brings forward the conclusions drawn from the Koskenniemi Report, where a distinction is made between the four situations in which the *lex specialis* principle may operate, namely: 1) within a single instrument; 2) between two different instruments; 3) between a treaty and a non-treaty standard; 4) between two non-treaty standards.

2.3. Two Regulations, Two Different Fundamental Rights to Protect – The Right to the Protection of Personal Data and the Right to Respect for Private Life

In the previous section we focused on providing an overview of the scope and contact points between GDPR and the ePrivacy Proposal.

From this brief introduction to both regulations, we can conclude that despite the intersection areas they both revealed (e.g. they are both European regulations aimed at protecting close realities, personal data and privacy), they are not overlapping one another in the most significant matters (e.g. the ePrivacy Proposal is *lex specialis* in regards to GDPR) and have different scopes.

In fact, both regulations pursue different objectives and are also aimed at protecting different rights.

There is also, obviously, a connection between their distinct purposes and the different rights they aim to protect, these last ones representing the "core" concerns that justify the protection granted by the European legislator, brought to life in the form of regulations.

In order to clearly put both regulations into perspective and to drive conclusions on their relevance for the protection of personal data and privacy in the IoT environment, it is required to analyze their objectives and the fundamental rights behind them.

From the objectives point of view, the REFIT evaluation examined the efficiency of the ePrivacy Directive towards an adequate level of protection of the respect for private life and confidentiality of communications in the EU, and also aimed to identify any redundancies in the objectives of the existing legislation.

One of the conclusions drawn from this "fitness check" evaluation, was that even with GDPR implementation, the objectives that the ePrivacy Directive pursued remained relevant[53].

Since these overall objectives of the ePrivacy Directive remain valid and relevant independently from GDPR, they are also applicable to the ePrivacy Proposal.

In a general sense, placing the objectives pursued by both regulations into perspective, we can state that:

- The GDPR is aimed at ensuring the protection of personal data, while;
- The ePrivacy Directive is aimed at ensuring the confidentiality of communications (being that these communications may also contain non-personal data and data that is related to a legal person).

It is this different objective and material scope of the ePrivacy Directive (which is valid also for the ePrivacy Proposal) that largely contribute to its significance and added value, even with GDPR -

[53] COM (2017) 10 final, 5.

this last one does not cover under its scope non-personal data[54] and does not grant protection to legal persons[55] .

In a close relationship with the objectives pursued by these regulations are the rights they aim to ensure. As suggested by the title of this Chapter, each regulation has as a building block a distinct fundamental right to protect.

However, before we go any further into the realm of the rights that both regulations aim to protect, it is required to address the issue of the meaning behind the expression “fundamental rights”.

Certainly, not all rights are considered to be fundamental rights, so what grants rights this statute? And ultimately, what does it mean?

In its analysis to understand if data protection should be considered a fundamental right or not, Bart van der Sloot came necessarily to question “what is a fundamental right?”

He concluded that, both in terms of specialized literature as also in terms of EU law and international law, the fundamental rights are usually treated as equivalent to human rights[56], taken into consideration the classical distinction that is made between “rights”, “constitutional rights” and “human rights”. The human rights are inherent to the human condition and do not depend of nationality or citizenship[57].

However, the author rejects the views taken by EU law, international law and several other authors that consider data protection as a fundamental right, viewing it instead as a consumer right, arguing (among other aspects) that for data to be considered personal all it takes is that an individual can be identified or identifiable. This in turn, makes that even the processing of an address or a name, may become a processing activity covered under the umbrella of a fundamental right[58].

In a different direction, Gloria Fuster, considers the protection of personal data as a fundamental right of the EU, explaining that this right was not considered as a fundamental right since the beginning.

However, when EU institutions felt the need to reinforce the system of fundamental rights, the possibility of endorsement of rights already identified but not listed as fundamental, or rights that did not existed but were deemed necessary was opened.

[54] Art. 1 (1) GDPR regarding the *“subject-matter and objectives*” of the regulation, states that the regulation lays down rules related to the protection of natural persons with regard to the processing of personal data.

[55] Rec.14 GDPR, states that “the protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person”.

[56] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, (Springer, 2014), 166. Clarifies that “in the EU context, the idiom fundamental rights usually refers to the rights protected by EU law, whereas the expression human rights commonly designates rights recognized in international law (…) EU law has never provided a general definition of fundamental rights”.

[57] Bart van der Sloot, “Legal Fundamentalism: Is Data Protection Really a Fundamental Right?”, in *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer, 2017), 3-30.

[58] Ibid., 23-28, “the scope of “personal data” does not fit the classical scope of human rights; the type of rules facilitating data processing rather than curtailing or prohibiting, seems to diverge from the typical purpose of human rights instruments; and the role of the Data Protection Authorities and the detailed regulation of almost every aspect of data processing activities in a EU-wide Regulation seem more akin to the idea of market regulation than to the protection of human rights”.

This required update granted the statute of fundamental right, to the right to the protection of personal data[59].

In our opinion, one of the most notable objections against considering personal data protection as a fundamental right of the EU, brought to light by Bart van der Sloot, lies in the scope of "personal data" as data that identifies an individual or leads to its identification.

This "clustering" applies regardless of the type of data in question. For the processing of personal data to be protected as a fundamental right, it does not matter if it is not a special category of personal data (e.g. name, address, IP address), or if it is indeed a special category of personal data being processed (e.g. political opinion, religious or philosophical beliefs, among others).

The exercise made by the EU legislator, in order to separate personal data according to its sensitivity in special categories of personal data, as it is done in GDPR, seems to be due to the increased disadvantages or discrimination that an individual can suffer if sensitive data is wrongfully processed or breached.

However, since the moment a person is identified and its personal data (even non sensitive) is wrongfully processed or breached, there is a distinct possibility that a wide range of negative effects are produced for that person (e.g. damage to its reputation; financial loss; identity theft or fraud).

Protection against these damages, related to a violation of the right to personal data protection, is not made dependable in the EU data protection legal framework to the nationality or citizenship of an individual, and the protection against the types of damages that even a breach of non-sensitive personal data can cause should rest under the dignity of a fundamental right.

Furthermore, it is not the "data" itself that is in need of protection, but the individual to whom the data belongs[60]. Therefore, even the processing of personal data (not considered as a special category) requires that the individual to whom this data belongs is protected.

The right to the protection of personal data is considered to be linked "to the safeguarding of rights and freedoms in general, and to ensuring the right of privacy in particular"[61].

An example of the potential impact of personal data processing regardless of the fact that the data is not listed as a special category, is the case of *Google v. Spain*[62] that started to erupt when Mario Costeja González brought to light the damage that had been caused to him by the disclosure of a past social security debt.

[59] González Fuster, op.cit., 206, "In this context saw the light the EU right to the protection of personal data, established in 2000 by Article 8 of the Charter of Fundamental Rights of the EU".

[60] Viktor Mayer-Schönberger, "Generational Development of Data Protection in Europe", in *Technology and Privacy: The New Landscape* (Cambridge/US: MIT Press, 1997), 219.

[61] González Fuster, op.cit., 206. This understanding comes from the Explanations accompanying the EU Charter, which proclaimed that the right to personal data protection rested on several instruments and provisions, which in fact did not mention it, but linked it to the overall safeguarding of rights and freedoms, and to the right of privacy.

[62] Background information regarding *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 (13 May* 2014), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN (accessed 20 April 2018), "on 5 March 2010, Mr. Costeja González, a Spanish national resident in Spain, lodged with the AEPD a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, in particular in Catalonia (Spain) ('La Vanguardia'), and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr. Costeja González's name in the search engine of the Google group ('Google Search'), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr. Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts".

This case became known for the consecration of the “right to be forgotten”, that was approved by the European Court of Justice (hereafter, ECJ) in the Decision of May 2014 and applied in the Decision of December 2014 of the Spanish National High Court[63].

In this case, it was not a special category of personal data that was being affected (art. 9 (1) GDPR), nevertheless the damages to the right to the protection of personal data, as shaped in Art. 8 (1) of the Charter of Fundamental Rights of the European Union (hereafter, Charter), demonstrate why it became important to include this right in the catalogue of fundamental rights.

The right to the protection of personal data has a wide scope of application, and its substantiation is filled with relevant ramifications, namely the rights of the data subject clearly expressed in GDPR.

Now that we have addressed the issue of the meaning of “fundamental rights” and particularly also the issue of the right to the protection of personal data as a fundamental right, we can resume where we left off.

Starting with GDPR, the text of the regulation states in its Rec.1 that:

- The right to the protection of personal data granted to natural persons is a fundamental right, and;
- Arts. 8 (1) of the Charter and 16 (1) TFEU provide the basis for this right.

This means that, what GDPR ultimately aims to ensure is the fundamental right to the protection of personal data.

In addition to the considerations made above concerning this fundamental right to the protection of personal data referred in Rec.1 GDPR, we can also state that the wording used by the EU legislator is a reflection of the underlying difference between the concepts of “data protection” and “privacy”, with a clear option made in the regulation for the adoption of the concept of “data protection”.

Perhaps, the best way to materialize these fundamental rights, *the right to the protection of personal data* and *the right to the respect for private life,* is to explore the difference between *data protection* and *privacy*, two concepts that are often mixed and mentioned as if they were indeed the same.

This approach can prove to be particularly useful, since we will also try to demonstrate that *privacy* is in fact, closer to the *fundamental right to respect for private life*, than with the *fundamental right to the protection of personal data*, as enshrined in the European legal framework regarding the protection of personal data.

Data protection and privacy are not synonymous, as Alexandre Sousa Pinheiro points out, from a dogmatic perspective, privacy and data protection do not correspond to the same reality.

The origin of privacy dates back to the United States (hereafter, US)[64]. Privacy, is considered to be a legal creation of a doctrinal and jurisprudential nature, whereas data protection has a

[63] Ana Azurmendi, “Spain: The Right to be Forgotten”, in *Privacy, Data Protection and Cybersecurity in Europe* (Springer, 2017), 17-30.

[64] Regarding the origin of privacy in the US, Alexandre Sousa Pinheiro, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, (AAFDL, 2015), 267-423.

European origin anchored to a large extent in the work of an "aristocracy of the public administration"[65].

In the words of Mayer-Schönberger, we could briefly describe “data protection” has the right to control one`s own data[66].

In its origin, "privacy" was intended to protect the human personality in response to technological developments. We can point to its founding moment with the article "The Right to Privacy," by Samuel D. Warren and Louis D. Brandeis, published in 1890 in the Harvard Law Review.

The diversity of concepts is not just limited to the distinction between privacy and data protection, also privacy itself may have different meanings and different scopes.

In fact, a fundamental differentiation should be made between *informational privacy* and *decisional privacy*[67].

As pointed out by Daniel J. Solove, Marc Rotenberg and Paul M. Schwartz, among many others, decisional privacy concerns issues such as contraception, procreation, abortion, among others, that concern the freedom to make decisions about one's own body and family[68].

We can materialize informational privacy using the words of Herman T. Tavani:

> *Because of the increasing use of technology to gather and store personal information, many contemporary analysts view privacy as one's ability to restrict access to and control of one's personal information.*[69]

For its part, the concept of *informational privacy* will prove to be closer to the fundamental right to respect for private life that is protected on the ePrivacy Proposal and further from the fundamental right to the protection of personal data, protected in GDPR.

With respect to the legal basis on which informational privacy is built, the first observation to make is that the overall basis for the rights of privacy rests in the Fourth Amendment to the US constitution (Bill of Rights)[70], where it is stated that:

[65] Ibid., 49.

[66] Mayer-Schönberger, op.cit., 219-237. Providing a useful overview over the several generations of data protection norms: “the first data-protection laws were enacted in response to the emergence of electronic data processing within government and large corporations (…) The data-protection law of the German state of Hesse (1970), the Swedish Data Act (1973), the data-protection statute of the German state of Rheinland-Pfalz (1974), the various proposals for a German Federal Data Protection Act, the Austrian proposals for a Data Protection Act (1974), and the German Federal Data Protection Act (1977) can all be seen as direct reactions to the planned and envisioned centralized national data banks. In structure, language and approach, they represent the first generation of data-protection norms”.

[67] It was in a case concerning the domain of decisional privacy - *Griswold v. Connecticut, 381 U.S.479 (1965)* that the Supreme Court came to regard privacy, not merely as a “private good”, but as a true right with constitutional dignity. It was only after this consecration of privacy, as "constitutional law", that this construction was developed, with the merit of combining a double view between decisional and informational privacy, https://supreme.justia.com/cases/federal/us/381/479/case.html (accessed 14 April 2018).

[68] Daniel J. Solove, Marc Rotenberg, Paul M. Schwartz, *Privacy, Information and Technology*, (ASPEN PUBLISHERS, 2006), 1-2.

[69] Herman T. Tavani, *Ethics and Technology – Controversies, Questions, and Strategies for Ethical Computing*, (John Wiley & Sons, Inc., 2011), 136.

[70] *Bill of Rights* - document containing the first ten amendments to the US Constitution, http://billofrightsinstitute.org/wp-content/uploads/2011/12/BillofRights.pdf (accessed 14 April 2018).

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

In essence, the Fourth Amendment is the recognition that certain aspects of citizens' private lives should be protected from state intrusions [71] (this means that, any intrusions eventually carried out by private entities, are outside the scope of this Fourth Amendment).

Although, the Amendment is clear about the protection of citizens' housing and personal property, the same cannot be said for electronic communications.

This lack of inclusion or clarity, regarding electronic communications under the Fourth Amendment’s protection, occurred due to the fact that the possibility of storing digital content or matters related to electronic communications was not under consideration when this Amendment was formulated.

Despite this initial property-based view, and going further into the densification of informational privacy, we note that the Supreme Court case law sought to go beyond the restrictive wording of the Fourth Amendment, in a well-known 1960 case *"Katz v. United States* "[72].

In this case, it was considered that one could invoke the Fourth Amendment when a person has a *reasonable expectation of privacy*.

However, a *reasonable expectation of privacy* is a subjective concept, whose concreteness and eventual applicability to the concrete case will vary, according to the densification conferred by the interpreter.

It depends not only on the individual's invocation of the Fourth Amendment when he considers that he has a legitimate and reasonable expectation of privacy but also on the validation of that interpretation by the expectation of society[73].

Patricia L. Bellia[74], clarifies that state intrusion in communications can occur in three distinct ways:

I. The Government may acquire electronic communications in transmission;

II. The Government may acquire stored electronic communications;

III. The Government may acquire the transacted data related to the transmission or storage of electronic communications (e.g. IP addresses, e-mail messages).

It is now necessary to analyze, in a summary way, how US case law has interpreted these three possibilities of state intrusion in electronic communications. This interpretation will rest on the realization of the subjective concept "reasonable expectation of privacy".

[71] Concerning this topic in particular - *Oliver v. United States, 466 U.S. 170, 178 (1984),* https://supreme.justia.com/cases/federal/us/466/170/case.html (accessed 14 April 2018).

[72] *Katz v. United States, 389 U.S.347 (1967)*, https://supreme.justia.com/cases/federal/us/389/347/case.html (accessed 14 April 2018).

[73] Erin E. Wright, “The Right to Privacy in Electronic Communications: Current Fourth Amendment and Statutory Protection in the Wake of Warshak v. United States”, in I/S: A Journal for Law and Policy for the IS, 2007, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Wright.pdf (accessed 14 April 2018).

[74] Patricia L. Bellia, “The Fourth Amendment and Emerging Communications Technologies”, in IEEE SEC. & PRIVACY, 2006, http://ieeexplore.ieee.org/document/1637377/ (accessed 15 April 2018).

Regarding the issue of government intrusion into electronic communications in transmission, the case-law has considered that these may be subject to the same protection as that given by the Fourth Amendment to voice communications.

In the case of *United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F., 1996)*, a whole point is devoted to the expectation of privacy.

It is clear, from the outset, that privacy expectations in email transmissions depend to a large extent on the type of message in question and the intended recipient[75].

At this point, it should be noted that the intrusion into communications in transmission, even when deemed admissible, also raises various technical difficulties in its implementation (e.g. the *WhatsApp*[76] case).

Concerning the issue of Government intrusion into stored electronic communications, the case *United States v. Miller, 425 US 435 (1976)*, suggests that there is no "reasonable expectation of privacy", since it is the subscriber who abdicates the protection that could be granted under the Fourth Amendment when he voluntarily discloses his communications to a party third[77].

Regarding the issue of government intrusion into transacted data related to the transmission or storage of electronic communications (e.g. IP addresses, e-mail messages), several orders of argument have been considered by the Supreme Court to suggest that individuals are less likely to see consecrated the "expectation of privacy".

Although it is acceptable to invoke the Fourth Amendment, because it is considered that there is a legitimate and reasonable expectation of privacy, there are some strong arguments in the sense of the non-validation of this expectation by society. In particular:

- When the message is transmitted, the sender loses control over how the receiver will treat it, and the expectation of privacy is lost when the receiver opens the electronic communication[78];
- The sender depends on several third parties to get his message to the recipient, and with this resource to others, the initial expectation of privacy is frustrated[79];

[75] *United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996), c*larifies that: "messages sent to the public at large in the "chat room" or e-mail that is "forwarded" from correspondent to correspondent lose any semblance of privacy. Once these transmissions are sent out to more and more subscribers, the subsequent expectation of privacy incrementally diminishes", http://www.armfor.uscourts.gov/newcaaf/opinions/1996Term/95_0751.htm (accessed 15 April 2018).

[76]Speaking about a terrorist attack in the city of London, where terrorists had appealed to WhatsApp application, the Secretary of State for the Home Department of Britain, Amber Rudd, has argued that it is unacceptable that these messaging services offer a type of encryption which makes the work of the police and security services much more difficult. She added that organizations such as WhatsApp should not provide a secret place for terrorists to communicate. http://observador.pt/2017/03/26/whatsapp-nao-pode-ser-um-lugar-secreto-para-os-terroristas/ (accessed 15 April 2018).

[77] *United States v. Miller, 425 U.S. 435 (1976)*, in this ruling it is stated that "The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities. The Act's recordkeeping requirements do not alter these considerations so as to create a protectable Fourth Amendment interest of a bank depositor in the bank's records of his account", https://supreme.justia.com/cases/federal/us/425/435/ (accessed 15 April 2018).

[78] Deirdre K. Mulligan, "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act", The George Washington Law Review, 2004, 1590, http://scholarship.law.berkeley.edu/facpubs/2131/ (accessed 15 April 2018).

[79] Patricia L. Bellia, "Surveillance Law Through Cyberlaw's Lens", The George Washington Law Review, 2004, 1385 – 1386, http://scholarship.law.nd.edu/law_faculty_scholarship/766 (accessed 15 April 2018). In the same vein, the jurisprudence outlined by *Supreme Court* in *Miller, 425 U.S.*

- Internet's own vulnerabilities to attacks of the most varied orders, which represent a constant threat, make the society uncomfortable in the recognition of an expectation of privacy, on this point[80].

The Electronic Communications Privacy Act of 1986 (hereafter, ECPA), promulgated by the US Congress, also sought to address the uncertainties surrounding the application of the Fourth Amendment to issues related to electronic communications.

> *Due to this uncertainty, Congress enacted the Electronic Communications Privacy Act to fill the constitutional "gap" left by the Fourth Amendment's protection[81].*

Namely, protecting the privacy of individuals in electronic communications, while such communications are in transit and when stored on computers, and protecting individuals not only from state intrusions, but also from third parties.

The scope of the ECPA should also be clearly defined. The diploma is divided into three titles:

- Title I protects wire, oral and electronic communications during its transmission. It also sets requirements for search warrants that are tighter than in other configurations;
- Title II, the *Stored Communications Act* (hereafter, SCA), provides for privacy protection for e-mail and other digital communications stored on the Internet;
- Title III, the *Pen Registers and Trap and Trace Devices Statute*, prohibits the use of these devices to record the information concerning the marking, routing, address and signaling used in the process of transmitting communications (electronic or wire) without a judicial order.

However, the protection granted by this legislative route is not always superior to that of the Fourth Amendment, a good example of this is the case *United States v. Warshak*[82], which was decided by the United States Court of Appeals for the Sixth Circuit, where it was alleged that Government agents had violated the Fourth Amendment by forcing the defendant internet service provider to deliver its e-mails without obtaining a search warrant based on probable cause.

In this case, despite the constitutional breach, the evidence thus obtained was deemed admissible in the judgment, on the basis that Government agents acted in good faith under the SCA.

The Court further stated that, the SCA is unconstitutional since it allows the Government to obtain e-mails without a warrant.

Privacy, in this case specifically informational privacy, with its origins in the US and with the interpretation and corresponding protection granted by its courts of law, is a figure closer to the fundamental right to respect for private life, consecrated in art. 7of the Charter, than with the fundamental right to the protection of personal data consecrated in art. 8 (1) of the Charter.

[80] Ibid., 1386.

[81] The ECPA was altered by the *Communications Assistance for Law Enforcement Act (CALEA)* of 1994, by the *USA PATRIOT Act* (2001), by the *USA PATRIOT reauthorization acts* (2006), and by the *FISA Amendments Act* (2008).

[82] *USA v. Steven Warshak, No. 08-4085 (6th Cir.2010),* http://law.justia.com/cases/federal/appellate-courts/ca6/08-4085/10a0377p-06-2011-02-25.html (accessed 19 April 2018).

The fundamental right to respect for private life, laid down in art. 7of the Charter states that: “everyone has the right to respect for his or her private and family life, home and communications”, while art. 8 (1) of the Charter, is specifically concerned with the protection of personal data (e.g. with the right of access to such data, with the purposes and grounds on which such data is processed).

Looking back to our analysis of the scope of *informational privacy* and the protection granted to individuals in such cases by the US legal framework and case law, the same seems to be focused on the protection of privacy of individuals in the scope of electronic communications, which is closer (in scope and concept) to the intended protection granted by art.7 of the Charter to the fundamental right to respect for private life.

2.4. The Rise of the Internet of Things in the Dawn of a New European Legal Framework for the Protection of Personal Data and Privacy

The wording “Internet of Things” was brought to life by Kevin Ashton (pioneer in the field of technological research) in the year of 1999[83], in connection with an investigation carried out in the field of RFID devices that could be used by companies dedicated to distribution and logistics with the aim of locating and counting the goods that were traded.

This nomenclature arose with the intention of describing a system in which the objects belonging to the physical world could be connected to the Internet by means of sensors. Although the term in itself considered, is relatively recent, in fact the idea of combining computers and networks in order to monitor various devices was not new and already existed before the emergence of the popular terminology[84].

In fact, the first device connected to the Internet was brought to public notice at a conference that took place in 1989, and it was a toaster, connected to the internet using a stack of TCP / IP communication protocols and controlled with a Simple Network Management Protocol (SNMP)[85].

Since this first experience was made public, many other developments have followed in the field of IoT.

So, what is the IoT?

According to commonly accepted definition provided by CASAGRAS, it is:

> *A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving*

[83] Kevin Ashton, *“*That “Internet of Things” Thing*”*, in RFID Journal (June 2009), http://www.rfidjournal.com (accessed 21 April 2018).

[84] Karen Rose, Scott Eldridge, Lyman Chapin, “The Internet of Things: An Overview – Understanding the Issues and Challenges of a More Connected World”, in Internet Society (October 2015), http://www.internetsociety.org (accessed 21 April 2018).

[85] More about this topic can be found on: Nicole Kobie, “What is the internet of things?”, The Guardian (May 2015) https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google (accessed 21 April 2018).

> *Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications.*[86]*.*

Or, as Bruce Schneier would put it:

> *We no longer have things with computers embedded in them. We have computers with things attached to them. Your modern refrigerator is a computer that keeps things cold. Your oven, similarly, is a computer that makes things hot*[87]*.*

But, what is the concept behind IoT? What does it all amount to in the end?

In fact, the concept behind this intricate network of devices with its very "own life" can be summarized as a kind of equation for the IoT.

Adrien McEwen and Hakim Cassimally describe this equation as the sum of the following parts:

Physical object + controller, sensor and actuators + Internet = IoT [88]*.*

Two functionalities should be clarified in this concept / equation: the sensor and the actuator.

- The sensor aims to capture the information coming from the outside world that will be processed by the device, thus fulfils an input function;
- Whereas the actuator will produce a given output or result[89].

It is also worth noting the different logic that presides over this connectivity, from the one that is present, for example, in devices in which certain operating systems may be incorporated, such as the cases pointed out by the authors of washing machines that can operate using the Linux operating system, or a cash register machine that can work via the Windows operating system.

This is because the mere incorporation of operating systems into commonly used devices is not a sufficient condition to bring us back to the IoT domain.

Here we have the computational energy connected to electronic sensors and actuators that in turn, assimilate information / data from the outside world and transport it via the Internet.

Therefore, in the IoT world, we have an inherent predisposition for contact with the outside environment and a very rapid processing and transmission of relevant data, in each case provided by the surrounding environment[90].

[86] CASAGRAS, Final Report, "RFID and the Inclusive Model for the Internet of Things", EU Project Number 216803, 2009, 10.

[87] Bruce Schneier, "Security and the Internet of Things", in Schneier on Security (February 2017), https://www.schneier.com/blog/archives/2017/02/security_and_th.html (accessed 22 April 2018).

[88] Adrien McEwen, Hakim Cassimally, *Designing the Internet of Things* (Wiley, 2014), 9-11.

[89] Ibid., 11, exemplify with the case of the chair that can collect information about the number of times we sit and the time we are sitting (input) and can then send an output in the form of, for example, a vibration. This vibration (output) can both fulfill the prophylactic role of warning us to get up if we are sitting for a long time, or in the example pointed out by the Authors, can merely "vibrate to let us know that we have received an email".

[90] Ibid., 13, pointing out as an example of this reality the computers that exist in modern cars, which have sensors that determine the performance of the same, measuring, among others, aspects such as oil level or tire pressure. This information is collected and processed and assists not only in diagnostics of faults, but also in safety issues (see example of computerized braking systems). It should be noted that the storage and handling of this

In fact, this universe of the IoT presents certain characteristics that make it singular, Ovidiu Vermesan and Peter Friess, point out essentially the following ones[91]:

- *Interconnectivity*: this is so since, in the field of IoT technology everything can potentially be in connection with the global structure of information and communication (e.g. everyday objects, like watches and glasses are "turned" into wearable computing devices, by including sensors that extend their abilities[92]);

- *Services related to things*: this attribute refers to IoT's ability to provide services related to things, with limitations, but that may affect areas such as data protection;

- *Heterogeneity*: this feature has to do with the diversity of hardware platforms and networks on which IoT objects are based;

- Dynamism in change: this characteristic is related not only to the number of devices that can constantly change and grow with great dynamism, but also with the states of the devices themselves, which can switch between connected or disconnected, and present changes of "state" according to the context in which they are inserted, being able to register changes according to the location and speed, among others;

- *Large Scale*: in comparison, the number of IoT devices that are expected to be available in a near future, and that will need to be managed, will exceed the number of devices connected to the Internet today.

In line with the opinion above, but adding also a different perspective, considering both the functionality and the data collected, we consider that the main singularities that differentiate the IoT from other realities are essentially six, namely:

- It is possible to identify an inherent predisposition for a contact and reception of information from the outside world at a very intense pace that is performed via the IoT devices (connectivity) ;

- Large amounts of information (data) are collected and processed from users of these devices (connectivity oriented towards data collection);

- The data of the users that is the object of collection and treatment constitutes, in the vast majority of situations, "personal data", plus there is a predisposition to "profiling" since the devices and services offered usually operate under the premise that data will be aggregated in order to extract patterns, derive behaviours and foresee habits[93];

information is tailor-made according to the data that the automobile manufacturer in question has chosen to program in a given vehicle.

[91] Ovidiu Vermesan, Peter Friess, *Internet of Things – From Research and Innovation to Market Deployment* (River Publishers, 2014), 12-13.

[92] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223), 5.

[93] Ibid., 4. This conclusion is also supported by the Article 29 Data Protection Working Party, "IoT stakeholders aim at offering new applications and services through the collection and the further combination of this data about individuals – whether in order to measure the user's environment specific data "only", or to specifically observe and analyse his/her habits. In other words, the IoT usually implies the processing of data that relate to identified or identifiable natural persons, and therefore qualifies as personal data in the sense of article 2 of the EU Data Protection Directive".

- There are several relevant stakeholders for an IoT device that need to be in coordination for the device to be launched in the market and even afterwards, for some lifecycle issues that may arise (e.g. device manufacturers, data brokers, application developers, social platforms)[94];

-The lifecycle of an IoT device needs to consider in parallel not only the product itself, but also the data collected by it. This will have an impact also in other realities relevant for the data protection framework, such as the rights of the individuals (e.g. data portability, right to erasure, among others);

- The diversity of this type of devices and its willingness to explore the Man-Machine interface, generates a dynamic focused on the search and development of interface modes that are increasingly complex and close to contact with humans.

Now that we have addressed the concept behind IoT, its characteristics and singularities, it is time to focus on its (foreseen) impact.[95]

In the beginning of our research, we made reference to the opinion some share regarding the inflated expectations over IoT, suggesting that IoT (as such) is not yet a reality, since it is not widely implemented.

While this scenario may prove to be truth nowadays, it is also truth that the path towards making IoT a worldwide reality is taking shape every day.

There is a "tipping point" of 1 trillion sensors connected to the internet, which is expected to have been reached by 2025[96]. When this somehow "symbolic barrier" has been reached, it will be possible to argue that IoT will have fulfilled its current expectations, and will be as such a common part of our daily routine and habits[97].

However, it should be mentioned that not all forecasts are so optimistic and the degree of scepticism is not only due to the current growth rate of IoT devices being purchased, it is also due to other factors, such as the fact that IoT has been around since the year 2000 (although it has only been more aggressively pushed since 2010 onwards), making the most skeptic recognize fragilities between the most optimistic forecasts and the current reality, plus the very definition of what constitutes an IoT device is not unanimous.

One common example is the Smartphone. It is debatable whether this device can actually be considered an IoT device, and of course any forecast that assumes a positive view over the integration of Smartphones as IoT devices will be considerably more optimistic, due to the large number of this devices currently in circulation and the expected purchase rate in future years[98].

The recognition of IoT`s potential is also present in the overview provided initially regarding the European strategy for the IoT, from which we could precise the role that IoT is to play in Europe's digitization and from which we could gain an overview of the goals set by the EU for the IoT.

[94] Ibid.

[95] Pagallo, Durante and Monteleone, op.cit., 72.

[96] Klaus Schwab, *The Fourth Industrial Revolution* (Portfolio Penguin, 2017), 137.

[97] Other forecasts: Cisco foresees that 500 billion devices will be connected to the Internet by 2030. https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf, while Gartner making forecasts in a closer range, expects 20 billion internet-connected things by 2020 - Mark Hung, "Leading the IoT – Gartner Insights on How to Lead in a Connected World", Gartner (2017), https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf (accessed 25 April 2018).

[98] Alasdair Gilchrist, *IoT Security Issues* (Walter de Gruyter Inc., Boston/Berlin, 2017), 6-9.

It is just not a matter of holding big expectations towards IoT, both for States and for companies worldwide, it has become a matter of building a strategy for a growing scenario, that becomes clearer and closer by the day, even if not at the most optimistic growth rates.

Many companies and scholars even prefer to use the term "*internet of everything*", instead of using IoT, and the reason behind it does not reside in the huge number of connected devices that are expected to populate our lives, but in the influence IoT represents to other areas.

In fact, it is not just the growing number of connected devices that can prove to reach impressive numbers, but also the very concept of IoT which is evolving due to IoT's ability to cause change and "merge" with a considerable number of areas that are starting to use IoT technology, for example:

- Internet of Mobile Things (IoMT);
- Autonomous Internet of Things (A-IoT);
- Internet of Things Clouds (IoT- C), and;
- The Internet of Robotics (hereafter, IoRT), among others.

Particularly interesting, is the concept of IoRT, which is considered to be the *next phase* in the development of IoT applications, being a result of the combination of artificial intelligence (AI), robotics, machine learning algorithms, and swarm technologies and having as a background the knowledge of Human-Robotics Interaction (HRI), as a discipline devoted to study the benefits of the interaction between humans and robots[99].

Regarding the topic of IoRT, Ugo Pagallo, Massimo Durante and Shara Monteleone, argue that we should add the notion of "artificial agent", in a way similarly to what has already been done when constructing the notion of "artificial legal person" (e.g. States, organizations and corporations).

To support this understanding they bring forward the field of robotics and the notion that many applications should be considered as "agents" and not mere tools to whom humans resort to.

For that matter three characteristics of robotic behavior are pointed out, that provide substance to the agency concept, namely:

- Robots perceive their environment and interact with it;
- Robots are also autonomous, since they are able to modify inner states or properties without human action;
- Robots are adaptable, being able to make improvements on the rules that govern their properties or inner states[100].

In a similar direction, also the European institutions are considering such legal constructions. There are already initiatives, on the EU side, to consider robots as "electronic persons"[101] with the purpose of holding them responsible for acts or omissions.

[99] Ovidiu Vermesan, Arne Broring, Elias Tragos, Martin Serrano, Davide Bacciu, Stefano Chessa, Claudio Gallicchio, Alessio Micheli, Mauro Dragone, Alessandro Saffiotti, Pieter Simoens, Filippo Cavallo and Roy Bahr, "Internet of Robotic Things – Converging Sensing/Actuating, Hyperconnectivity, Artificial Intelligence and IoT Platforms", in *Cognitive Hyperconnected Digital Transformation - Internet of Things Intelligence Evolution* (River Publishers, 2017), 97.

[100] Pagallo, Durante and Monteleone, op.cit., 71-72.

[101] May Bulman,"EU to Vote on Declaring Robots to Be "Electronic Persons"", Independent (January 2017), https://www.independent.co.uk/life-style/gadgets-and-tech/robots-eu-vote-electronic-persons-european-union-ai-artificial-intelligence-a7527106.html (accessed 25 April 2018).

These initiatives came under the radar in the scope of implementing liability rules, and while there is recognition for an urgent need of harmonized rules for autonomous vehicles (e.g. the implementation of a mandatory insurance scheme plus a fund to ensure victims are fully compensated if an accident is caused by an autonomous vehicle), there is also a long-term recognition of the possibility of creating the legal status of "electronic persons" for more advanced autonomous robots, in order to clarify responsibility issues in case of damages[102].

The IoT, with its ramifications, specially IoRT (and the role robots are designed to play due to their characteristics), is expected to become more than just connected devices that make our life easier, provide us comfort, improve efficiency in consumptions, and act a little bit everywhere as a "digital glue" connecting our existence with the "things" we own.

It is expected that these "artificial agents" combined with IoT generate new possibilities for the consumers and for society[103] and also new challenges for data protection, when the connected robot becomes a part of our daily lives in the near future.

Instead of having devices that "communicate" with the user, or even that communicate between them (e.g. the example of a smart home where several devices are connected), we can also have a robot that due to its structure can perform many of the human tasks, with the improved capacity of collecting information from the "outside" and analyzing it by accessing information from the cloud in real time, which in turn allows complex tasks to be performed in a more efficient manner.

Connected with the areas that are starting to "merge" with IoT technology, is the topic of the developments made in IoT. These developments can be clustered as below (without the intention of providing an exhaustive catalogue)[104]:

- Wearable computing;
- Quantified self;
- Home automation "domotics";
- Smart cities;
- Smart transportations.

The first three development clusters, share a common trait, all of them have a direct interface to the user.

[102] The Legal Affairs Committee requests for EU-wide rules to regulate robots and artificial intelligence http://www.europarl.europa.eu/news/en/press-room/20170110IPR57613/robots-legal-affairs-committee-calls-for-eu-wide-rules (accessed 25 April 2018).

[103] Vermesan, Broring, Tragos, Serrano, Bacciu, Chessa, Gallicchio, Micheli, Dragone, Saffiotti, Simoens, Cavallo and Bahr, op. cit., 4 provide the example of the Da Vinci robot, that is a clinical robot already able to perform several tasks (e.g. suturing), but that is still a stand-alone robot. The authors claim that with IoRT, this robot and others could grow their potential exponentially "for example, while performing certain tasks, assistance could be provided by using cloud services and patient monitoring could be improved by connecting the sensors to the Da Vinci system. With the help of cloud computing, complex operational decisions could also be computed in real-time".

[104] Developments catalogue extracted from Article 29 Data Protection Working Party, op.cit., 5-6. For another view on the developments of IoT, but considering a division made according to application areas, see the following report from McKinsey: James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, Dan Aharon, "The Internet of Things: Mapping the Value Beyond the Hype", McKinsey Global Institute(June2015),http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world (accessed 25 April 2018).

Wearable computing, as it may be inferred by the nomenclature, are smart devices with a connection to the internet that form part of an individual "props" (e.g. clothes[105], watches[106], glasses[107], among others).

This smart "props" are objects that we already use on a daily basis, but which include sensors, cameras or even microphones[108] that allow information from the user's surrounding environment to be captured and transferred.

Quantified self, differs from wearable computing since they are not props to be weared or dressed by an individual, although they are also objects that are meant to be frequently carried by them in order to measure data related to habits and lifestyle and derive trends and patterns (e.g. a sleep tracker that is able to record and derive sleep patterns, devices that record burned calories or distances)[109].

Home automation or "domotics", are IoT devices that equip the home with a multiplicity of possible functionalities[110]:

- Security systems (e.g. monitors, alarms, cameras, sensors);
- Energy saving (e.g. smart thermostats and smart lighting);
- Smart appliances (e.g. refrigerators, washing machines).

These IoT devices can, according to their objective, improve security, energy consumption and efficiency (and therefore also contribute to the reduction of environmental impact and costs).

Besides the pros, home automation still holds a few considerable cons (not just focused on data protection issues), namely:

- They are usually more expensive than other "not connected" devices (although, this is a characteristic that seems to be common when we compare most IoT devices with their counterparts), and;
- If a consumer buys IoT products from several different companies, he will have several different applications to setup and some troubles to make them work as one connected system (e.g. to have the outdoor lights to turn on after the garage door unlocks requires two separate applications and one event is not triggered by the other[111]).

[105] Samsung's wearable clothing prototypes include: a belt that allows keeping track on weight gain, a golf shirt that tracks swings, among others https://www.digitaltrends.com/wearables/smart-clothing-is-the-future-of-wearables/ (accessed 25 April 2018).

[106] Overview of several smart watches, currently available. The watches may include features such as: heart rate monitor, sleep tracking, music storage, connected GPS among others (depending on the function they are aimed to fulfill – a fitness watch is different from a "fashion" watch) https://www.wareable.com/buyers-guides/what-is-the-best-smartwatch-2018 (accessed 25 April 2018).

[107] Overview of several smart glasses, currently available. The glasses abilities vary according also to its function (e.g. "Everysight Raptor" glasses are built for cyclists and are able to collect data related to mapping, heart rate and other ride information with its sensors) https://www.wareable.com/ar/the-best-smartglasses-google-glass-and-the-rest (accessed 25 April 2018).

[108] Article 29 Data Protection Working Party, op.cit., 5.

[109] Ibid., 5-6, also, a wearable device, like a smart watch can perform measurements related with Quantified Self assessment.

[110] Andrew Meola,"How IoT and smart home automation will change the way we live", Business Insider (December 2016), http://www.businessinsider.com/internet-of-things-smart-home-automation-2016-8 (accessed 25 April 2018).

[111] Example extracted from Patrick Moorhead, "The Problem With Home Automation's Internet of Things (IoT)", Forbes (September 2013), https://www.forbes.com/sites/patrickmoorhead/2013/09/26/the-problem-with-home-automations iot/#217da6da70ec (accessed 25 April 2018). Other issues that can occur are also mentioned, such

Smart cities, have a different (indirect) connection with the user, according to a report commissioned by the European Parliament's Committee on Industry, Research and Energy, they can be defined as:

> *A city seeking to address public issues via ICT-based solutions on the basis of a multi-stakeholder, municipally based partnership*[112]*.*

Initiatives focused on fostering the growth of smart cities around Europe are already realities, and they are aimed at addressing the increased complexity of urban life that will come with the expected doubling of the world's urban population by 2050. The implementation of these cities is a part of the European strategy to reduce poverty, inequality and unemployment and improve energy management[113].

Smart transportations, can be described as the use of IoT technology applied to the common means of transportation we are now using. However, vehicles are not the only ones in the wider "transportation sector" that can profit from the IoT transformation, also infrastructures management, road conditions, and connected areas such as logistics, are targeted for enhancement.

And, how precisely can IoT help the transportation industry?

Several companies are providing solutions to be integrated in the current transportation industry, one of them is the giant Microsoft, who is providing several types of IoT enabled solutions, such as[114]:

- Solutions that help maintain the vehicles performance, by doing monitoring and forecast of the vehicles maintenance needs;
- Solutions for real-time monitoring and processing of traffic data, to help in the management of infrastructures, improve traffic flows and roads conditions;
- Focused on logistics, the optimization of fleet operations, in order to enhance delivery routes.

There are several examples of how IoT is helping the transportation industry advance towards a more efficient reality, not only by land, but also by sea and air.

For example, when it comes to land vehicles Telit, like other companies, is providing solutions to manage traffic and also parking needs[115].

Another example, but thinking now on air traffic, comes from NAV CANADA (a civil air navigation service provider from Canada), which has developed a system (ADS-B) that contributes to aviation safety by offering a better alternative against the limitations of the traditional radars and other

as: different devices may require different wireless adaptors to be plugged into the wall. There are also solutions existing in the market, as pointed out, for example the consumer can go to a service and device aggregator that provides one application and a consolidate wireless adapter box.

[112] Directorate General for Internal Policies – Policy Department A: Economic and Scientific Policy, Mapping Smart Cities in the EU, European Union, 2014, 9.

[113] Ibid., 17.

[114] https://www.microsoft.com/en-us/internet-of-things/transportation (accessed 28 April 2018).

[115] https://www.telit.com/industries-solutions/smart-cities-smart-transportation/traffic-and-parking/ (accessed 28 April 2018).

types of ground-based surveillance systems when airplanes are flying across oceans (these ground systems present a weakness in terms of surveillance, since they have a limited range of 200 miles).

Since, ADS-B still had some limitations due to a high dependency on ground-based systems, a joint venture (Aireon) was developed in order to gain access to the sky.

The next step in the project came with IoT with the implementation of Microsoft Azure IoT technology (still focused on the initial purpose, tracking planes to achieve navigation safety), by providing high computing power and secure and scalable storage, to the large data flows that were generated.

Further developments supported by IoT technology implemented in planes, can be:

- The optimization of routes;
- A better exploration of conditions (e.g. winds) to reduce costs, among others.[116]

With the overview provided, regarding the rise of the IoT, it becomes clearer and easier to contextualize its role in empowering a fourth industrial revolution.

This last industrial revolution that is beginning to take shape follows the revolutionary path drawn by the other industrial revolutions that marked their time setting forces into motion that changed not only productive structures, but also (in some extent) the very fabric of society.

The first revolution was based on water and steam to give power to the mechanized production industry, the second was based on electricity and enabled the dawn of mass production, finally, the third was characterized by automation (aided by electronics and information technology)[117].

As mentioned by Klaus Schwab, regarding his selection of key technologies that will empower the fourth industrial revolution, the same is based on the research done by the World Economic Forum and also on the work of several of the Forum's Global Agenda Councils, and it encompasses among others:

- Autonomous vehicles;
- 3D printing;
- Advanced robotics;
- New materials, and;
- The IoT.

The IoT is described as one of the main connections between the physical and digital applications enabled by this new industrial revolution, and it is this ability of bridging the gap between both worlds (physical and digital) that will also contribute for its integration in our daily routines. [118]

[116] More regarding this example of IoT transformation for the transportation industry: Barb Edson, "Azure IoT Technology helps NAV CANADA revolutionize air-traffic control", Microsoft Internet of Things, (March 2016), https://blogs.microsoft.com/iot/2016/03/17/azure-iot-technology-helps-nav-canada-revolutionize-air-traffic-control/#JvuzE3WFYvjuqU6h.99 (accessed 28 April 2018). "Extending the Internet of Things (IoT) to track planes is opening the door to massive opportunity for aviation related companies. Commercial aircraft using ADS-B will be able to send a constant stream of rich data while in flight through Aireon's systems to receiving stations on the ground, creating a new source of insight and efficiency that could benefit the entire aviation industry".

[117] Symantec DeepSight Adversary Intelligence Team, "The Fourth Industrial Revolution – Opportunities and Challenges with the Internet of Things (IoT) and Why You Need Threat Intelligence ", Symantec Corporation (April 2018), https://www.symantec.com/blogs/expert-perspectives/fourth-industrial-revolution (accessed 28 April 2018).

[118] Schwab, op. cit., 14-25.

Chapter 3

Connecting Personal Data to the Industry 4.0: Privacy, Data Protection and Security Challenges of the Internet of Things

This chapter is devoted to provide an overview of privacy, data protection[119] and security challenges that impact the IoT, while contextualizing also the topic "security" in our research and providing a working definition that can be used to identify the relevant "layers" of security for IoT.

Also the typical vulnerabilities that can affect IoT are important when addressing security concerns, since it is through them that an attacker can find an open door to compromise the device, and eventually access personal data.

This bi-dimensional approach is necessary since both realities are intertwined, in fact it is common, that from a flaw in security, adverse consequences are felt by the user/data subject, if personal data is being processed.

We can find several examples of this close relationship between security, privacy and data protection in IoT products.

For instance, a connected refrigerator, which is composed by a regulator refrigerator enabled with a connection to the internet and computer components, is able to process an individual (or an entire family's) food and beverage related data, with the primary purpose of providing warnings of shortages of supplies or even automatically order what is missing, according to derived consumption patterns.

These functionalities can be useful, however the amount of data that can be accumulated over time can make room for identifying very intimate information about someone (e.g. its lifestyle, possible eating disorders or drinking habits) and if a data leakage were to happen and this data was not anonymized, the effects (seen now from a privacy and data protection point of view) could cause serious damages to those affected[120].

Security flaws can go even further, than to produce serious privacy and data protection concerns, ultimately they can culminate in physical injuries or even death. Let us think on the example of the autonomous vehicles being hacked and "hijacked" by an attacker[121].

There are several privacy and data protection issues that affect the IoT, some of them are even predictable to happen since they are typical, and therefore can be "clustered", analyzed and addressed when a new device is engineered and prompted into market.

The aim of this chapter, is not only to provide an overview of the major security, privacy and data protection issues that are usually present in the IoT, but also to explore in which directions we can find solutions for them.

[119] As we have discussed in a previous chapter, privacy and data protection are two different dogmatic dimensions, both being relevant for IoT.

[120] Regarding this example and others Alasdair Gilchrist, op. cit., 12-13.

[121] About this issue and the Jeep Cherokee example, see Peter Campbell," Driverless vehicles – Hackers have self-driving cars in their headlights", Financial Times (March 2018), https://www.ft.com/content/6000981a-1e03-11e8-aaca-4574d7dabfb6 (accessed 28 April 2018).

3.1. Security Issues in the Internet of Things: a Source of Potential Risks for Privacy and Personal Data

Let us begin by addressing the concept of "security" which constitutes the background of our current topic, focused in understanding the security issues that can occur in the IoT.

Without an overview of the meaning and scope of the concept of security, it is not possible to properly derive all the relevant layers of security that matter for IoT.

So, how can "security" be defined?

In general, security can be seen as "the quality or the state of being secure - to be free from danger"[122].

In other words, it is a protection against opponents - of those who could cause harm, intentionally or unintentionally.

This common definition of security, places us in the right path, but it does not answer the more concrete needs of our topic, since we cannot extract from it all the relevant layers of security that should be addressed in IoT.

If we think about security implementation at the organizational level (be it state or private), we can find already an approach on security issues that is focused on the several layers of security.

Here, we observe that security should take the form of a multi-layered or "tiered" approach, focused on protecting the organization assets, its resources and its people.

Therefore, a successful organization must implement the following layers of security to protect its operations [123].

- *Physical security*, to protect physical items, objects or areas of unauthorized access and misuse;
- *Security of personnel,* in order to protect the individual or a group of persons, who are authorized to access the organization and its operations;
- *Operational safety*, to protect the details of a particular operation or series of activities;
- *Communications security*, to protect the media, technology and content;
- *Network security,* to protect network components, connections, and content;
- *Information security*, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing or transmission.

From this multi-layered approach to security at an organizational level, we are still on a very high level of security, and we lack the vision that can grant us the "connection to the device" itself.

The sight of IoT architecture cannot be dismissed from the analysis of the relevant security layers to be implemented in IoT, since the tiered security approach will be applied to it.

However, before we proceed to conclusions regarding the relevant layers of security in IoT, there is a need to analyse one particular layer of security at an organization level, namely "information security".

[122] The meaning of "security" according to Merriam-Webster, Merriam-Webster Online, https://www.merriam-webster.com/dictionary/security (accessed 28 April 2018).

[123] Michael Whitman, Herbert Mattord, *Principles of Information Security*, (Course Technology Cengage Learning, 2011), 8.

This layer is transversal to our topic, connecting data protection with security, and is therefore essential to understand what we need to ensure on a security level to protect data.

Information security is wider in scope than the legal notion of “personal data”, but it is certainly applicable to it[124].

In this layer it is the data itself that is the aim of protection and that needs to be secured, when it is stored, transmitted or processed.

The Committee on National Security Systems (CNSS) glossary defines information security, as:

> *The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.*
>
> *Source: 44 U.S.C. Sec 3542*[125]

According to Jason Andress, this means in essence that, in information security the intention is to protect the data (wherever it is), and also all the assets of the system from those who seek its misuse[126].

Thus, when we speak of "information security" in organizations (public or private), there are invariably three orders of common ideas or objectives that are to be achieved, namely: the confidentiality, availability and integrity of such information[127].

- *Confidentiality* must be governed by the “Need-to-Know” principle, which is to say that access to information must be based on the logic of the *minimum privilege*. Therefore, information should not be disclosed to unauthorized persons, processes or devices;
- *Availability* means, that the information must be available in a timely manner to those to whom access is authorized; if this does not happen we may face a Denial of Service (hereafter, DoS);
- *Integrity* means that the information available must be reliable, and to reach this objective the adequate security measures must ensure that the information is protected against unauthorized changes or eventual destruction.

These three general objectives pursued in information security, are also applicable to the IoT since data is being processed, and its security in all these three pillars needs to be ensured.

Confidentiality of information is essential to ensure users' right to the protection of their personal data (as we argued above, most of the data processed in IoT is often personal).

Therefore, the information that is collected and processed by IoT devices should be made available only for those who need to know it, according to the established purpose(s) of processing.

[124] Art. 5 (1) f) GDPR, refers that personal data should be processed in a manner that ensures an appropriate level of security, which includes “protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (“integrity and confidentiality”).

[125] Committee on National Security Systems, Committee on National Security Systems Glossary (CNSS), April 2015, 64 https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf (accessed 28 April 2018).

[126] Jason Andress, *The Basics of Information Security – Understanding the Fundamentals of InfoSec in Theory and Practice* (Elsevier, 2011), 3.

[127] Joseph G. Boyce, Dan W. Jennings, *Information Assurance – Managing Organizational IT Security Risks* (Butterworth-Heineman, 2002), 14.

That same information needs to be available on time for those who need to access it, and its integrity must be ensured, in order that the data that is being processed can represent the reality in a reliable way.

As an example, let us think of smart meters used to measure the consumption of water, electricity and gas. The data collected by these smart meters must be reliable in order to represent the actual consumption, so that they meet their informative purpose of measurement, must be available for analysis and must be protected against unauthorized access.

Similarly, to the case of the information available in a bank statement, which can reveal a lot about a given individual (e.g. location, preferences), the consumption of a home can also, by hypothesis, reveal that in a given period the owner is absent, which can constitute a danger if this information "falls" into the wrong hands. Also, from a legal perspective, the topic of the detailed measurements done by these devices, requires that a balance is made between data protection requirements and the specific implementation of the detailed metering[128].

To begin our conclusion of the relevant layers of security in IoT, let us first consider the architecture layer classification commonly referred for IoT, to which the tiered security approach will be applied[129]:

- Application layer;
- Network layer, and;
- Perception layer;

The perception (or recognition[130]) layer is the first level, or the lowest level in the architecture model. It is fundamentally responsible for the collection of the required data from the surrounding environment or from other things[131].

The network layer is the second level in the IoT architecture model, and its function is to process and transmit the input it has received from the previous layer (the perception or recognition layer) with the support of technological platforms[132].

The application layer is the last layer of the conventional IoT architecture model, and it is the layer that will interact with the user, bridging the gap that exists between the individual and the applications[133].

[128] In the same direction, Colette Cuijpers, Bert-Jaap Koops, "Smart Metering and Privacy in Europe: Lessons from the Dutch Case", in *European Data Protection: Coming of Age* (Springer, 2013), 269-292. In the Dutch case, it was considered that a comprehensive privacy impact assessment is of the most importance, in order to introduce smart metering, since smart meters can involve personal data and private life, home and communications.

[129] K. Zhao, L. Ge, "A Survey on the Internet of Things Security", in *Computational Intelligence and Security (CIS), 2013 9th International Conference* (IEEE, 2013), 663-667.

[130] H. Suo, J. Wan, C. Zou, J. Liu, "Security in the Internet of Things: a Review", in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference* (ICCSEE, 2012), 648-651.

[131] Muhammad Bilal*,"* A Review of the Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D Printers", Cornell University Library (June 2017) https://arxiv.org/abs/1708.04560 (accessed 29 April 2018).

[132] Diego Mendez*,* Ioannis Papapanagiotou, Baijian Yang," Internet of Things: Survey on Security and Privacy", Cornell University Library (July 2017) https://arxiv.org/abs/1707.01879 (accessed 29 April 2018).

[133] Bilal, op. cit.,6.

These layers are susceptible to several types of attacks that can compromise the security of IoT user's, on that matter N. Jeyanthi describes the various possible attacks, according to the different architectural layers.

The perception layer, can suffer from a variety of possible attacks. For example, *HELLO flood attacks* (in which, every object presents itself with a HELLO message to all its neighbors - since it is a flooding attack it causes the non-availability of resources to its rightful users), *wormhole attacks* (these attacks occur mainly in Mobile Adhoc Networks (MANETs)[134], here the data is captured by the attacker, there is a forward to another node and subsequently the attacker retransmits from that node), *sewage pool attacks* (the malicious node attracts all the messages of a selected area of the network towards it and then it replaces the base station node[135]), among other types of possible attacks[136].

The network layer, is susceptible to attacks on *routing protocol* [137](e.g. a feature of the routing protocol RPL that is usually destined to ensure a loop and error free topology, can be misused in a version number attack – this is done by the modification of the version number with a malicious node, which in turn generates the necessity of building again the routing tree in full[138]) and *address compromise* (this is done by spoofing the IP address of virtual machines (hereafter, VMs), thus giving the attacker the possibility to get the IP address of the VMs and implant malicious machines in order to access data of the users of those VMs[139]).

At last, the application layer can suffer from user *authentication issues* (the data can be compromised in its integrity and it is not originated from the intended or legitimate user), *data destruction*, and *disclosure of sensitive data* (these last two attacks do not require an introduction regarding the way they work and the results they aim to reach), among others types of attacks.

This architecture model requires that end-to-end security is implemented, to ensure that not only the IoT device (as a physical object) is secure, but also that the communications are not intercepted and the information stored in the cloud is not compromised or lost[140].

Therefore a multi-layered security approach is required, taking also into consideration lifecycle issues[141]:

[134] Gulshan Shrivastava, Prabhat Kumar, B. B. Gupta, Suman Bala, Nilanjan Dey, *Handbook of Research on Network Forensics and Analysis Techniques* (IGI Global, 2018), 74.

[135] Ibid.

[136] N. Jeyanthi, "Internet of Things (IoT) as Interconnection of Threats (IoT)", in *Security and Privacy Internet of Things (IoTs) – Models, Algorithms, and Implementations* (Taylor & Francis Group, LLC, 2016), 8 and 10-11.

[137] Linus Wallgren, Shahid Raza, Thiemo Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things", International Journal of Distributed Sensor Networks (August 2013) http://journals.sagepub.com/doi/full/10.1155/2013/794326 (accessed 29 April 2018). Explain that RPL, which is short for Routing Protocol for Low-Power and Lossy Networks (LLNs, also known as IPv6 or Low-powered Wireless Personal Area Networks(6LoWPAN)), is a light weight protocol that was standardized as a routing protocol for the IoT.

[138] Anthéa Mayzaud, Rémi Badonnel, Isabelle Chrisment, "A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks", in *Network and Service Management IEEE Transactions* (IEEE, 2017), 472-486.

[139] Jeyanthi, op. cit., 9-10.

[140] Rec. 15 GDPR claims that the solutions implemented in order to protect the natural persons should be technologically neutral and should not depend on the techniques used. This approach from the EU legislator is intended at preventing serious circumvention risks.

[141] Levels or layers of security according to the proposal of Padraig Scully,"5 Things to Know About IoT Security", IoT Analytics GmbH (November 2017) https://iot-analytics.com/5-things-to-know-about-iot-security/ (accessed 29 April 2018).

- Secure device (hardware);
- Secure communications;
- Secure cloud;
- Secure lifecycle management.

Let us explore briefly the physical security aspect, which constitutes a serious threat if compromised. According to Alasdair Gilchrist, physical security can be compromised by means of “theft, DoS, tampering, vandalism or physical re-engineering”[142].

Physical security in the IoT, should be seen in two perspectives (organizational and individual/user) due to its close contact with the user in most of the cases (e.g. wearable computing; quantified self; home automation “domotics”).

What does physical security encompasses? The traditional vision of physical security does not fully apply to IoT. At an organizational level, as Michael Whitman and Herbert Mattord point out, it involves the design, implementation, and also the maintenance of countermeasures with the goal of protecting an organization's physical resources.

These resources include people, hardware and system support elements, and also resources that control information at all levels[143].

By the very nature of IoT, we are dealing with devices that are developed and marketed by organizations but that are physically and geographically (in most cases) intended to remain with their users, with whom we have a very personal connection, collecting large quantities of data (often personal), and even drawing profiles of consumption habits.

It is difficult in this regard, given the physical and geographical barrier that separates these devices from the organizations responsible for their development and market placement, to see physical security as a concern strictly from their side.

In this field of physical security, although organizations developing such devices and collecting user data can protect themselves internally by implementing physical security measures and preventing attackers from having access to information made available by users through attacks on the perimeter of their premises (e.g. to servers), they cannot implement the same physical security measures in the physical spaces where the users are located, and thus prevent attackers from gaining physical access to the devices.

As pointed out by Mario Ballano Barcena and Candid Wueest, analyzing the issue of physical access in smart home devices, when there is an attack on a device, where physical security is compromised, this allows the attacker to alter configuration settings, which could include:

> *Issuing a new device pairing request, resetting the device to factory settings and configuring a new password, or installing custom SSL certificates and redirecting traffic to a server controlled by the attacker*[144]*.*

[142] Gilchrist, op. cit., 124.

[143] Whitman and Mattord, op. cit., 339.

[144] Mario Ballano Barcena, Candid Wueest,”Insecurity in the Internet of Things”, Symantec (March 2015), https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things-en.pdf

As we started to mention, there are several possible attacks from a physical security point of view to which users of IoT products are exposed, for example, an attacker gaining access to someone's house also gains physical access to IoT devices located there, or a user who purchases IoT devices in second-hand, unknowingly may be buying devices that have been altered by attackers so that it becomes possible to spy on who gets them, among other types of possible attacks[145].

From a physical security perspective, the IoT case is not so different from any other case, in which we buy a laptop, a mobile phone (if we do not consider Smartphones as IoT devices, or if we think about older versions of mobile phones), or any other device that is able to store and transmit data and is under our responsibility, with the nuance that IoT devices tend to collect a great amount of data from their surrounding environment (which includes their users).

Therefore, in the IoT domain and in the field of physical security, it is imperative to raise awareness and alert the users of the IoT devices to the risks they are exposed to, highlighting the necessity of maintaining the physical security of their devices.

The layer of security of communications, with the overall scope within an organization to protect media, technology and content, when directly applied to the IoT reality, is aimed at protecting the mediums over which data is being transmitted or received. This layer refers to the "connectivity networks of the IoT solution"[146].

The purpose of the cloud layer, is considered to be an ideal IoT building block:

> *Firstly, because cloud services can operate across a range of systems, services, and devices, it provides the natural point for (1) data aggregation and analysis, and (2) the management, control and coordination of the range of systems and services. Further, (3) cloud services offer benefits in terms of resource management, as clouds are always on, can scale to meet demand, and can allow the offloading from constrained hardware of data (for computation and storage) and management specifics[147].*

But, the ideal features of this layer may come with a heavy price tag for security, depending on the security solutions adopted by the cloud service providers themselves, among other factors.

The clustering of the security risks of the cloud varies, but it is common to find references to the following ones[148]:

- Unauthorized access to customer and business data;
- Security risks at the vendor side;

(accessed 29 April 2018). Physical access may also grant the attacker the possibility to read the device's internal memory and firmware.

[145] Ibid., 11.

[146] Padraig Scully," Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers", IoT Analytics GmbH (November 2016) https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/ (accessed 29 April 2018).

[147] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, David Eyers, "Twenty Security Considerations for Cloud-supported Internet of Things", in *IEEE Internet of Things Journal* (IEEE, 2016), 269-284.

[148] Available at: https://www.calyptix.com/research-2/top-5-risks-of-cloud-computing/ (accessed 29 April 2018).

- Compliance risks (e.g. specific industry regulations that must also be met, such as HIPPA who requires healthcare providers to protect patients data, or PCI DSS who imposes the protection of the cardholder data for those who accept credit card);
- Risks due to lack of control (e.g. vendor may change prices, features);
- Availability risks (access to data stored on the cloud requires availability requirements must be in place from the vendor side, plus internet access available from the internet service provider of the company using the cloud);

Security measures should also be present in the lifecycle management, covering the entire lifecycle of the device, from conception to decommissioning. It is important to define a lifecycle management approach for IoT devices, and this approach should focus not only on the IoT device itself (e.g. required updates and patches), but also on the user data that is collected and processed.

Here it is relevant both the role of the organization that collects the data and the third parties to whom such data may have been made available.

In terms of the collected data, not only the *primary data* is to be integrated in this lifecycle approach (e.g. in the case of sensors embedded in vehicles which collect data on distance, destination, speed), but also the *data that can be inferred* from such primary data (e.g. profiles, habits).

These security layers should be present to ensure users can trust their IoT devices and use them without the common fear that something will go wrong and their personal data will be unduly accessed by others.

In the path towards security in the IoT, considerations should also be made regarding the typical “weaknesses” or vulnerabilities that affect IoT, giving room of maneuver for an attacker to gain access to the user´s data.

In that sense, the OWASP (Open Web Application Security Project) came to list the ten biggest vulnerabilities[149] of IoT, where potentially attacks[150] may occur.

Attacks on IoT products can tend to have two types of consequences: they may endanger not only the use of the product but also the privacy of its users (essentially due to improper access to personal data).

The biggest vulnerabilities in IoT, which can act as a "gateway" to an attacker, are[151]:

1. Insecure web interface;
2. Insufficient authentication/authorization;
3. Insecure network services;
4. Lack of transport encryption;
5. Privacy concerns;
6. Insecure cloud interface;
7. Insecure mobile interface;

[149] As mentioned by Whitman and Mattord, op. cit., 11, vulnerability is a weakness or failure in a system or protection mechanism that makes it permeable to attack or damage.

[150] Ibid., 9, an attack is an intentional or unintentional act that may cause harm or compromise information and/or the system that support that same information.

[151] https://www.owasp.org/index.php/IoT_Security_Guidance (accessed 29 April 2018).

8. Insufficient security configurability;
9. Insecure software/firmware;
10. Poor physical security.

Side by side with these vulnerabilities, the OWASP project identified also a set of overall measures that could be implemented to address them.

In our opinion, a good level of security in IoT can be achieved, considering:

- Security on an organizational level;
- Awareness from the IoT users;
- A multi-layered security approach, considering the security of the device (hardware), communications, cloud and lifecycle management (taking into account identified IoT vulnerabilities and the corresponding countermeasures for risk elimination or mitigation).

3.2. Privacy and Data Protection Challenges in the IoT

Ziegeldorf, Morchon and Wehrle have identified a comprehensive set of seven privacy threats. This classification has the merit of clustering well known privacy concerns that are prone to appear in the IoT[152]. Therefore, we will take this clustering as a starting point for our analysis, decomposing it while also aiming to add our point of view on the matter.

The first threat is considered to be *identification*. The identification issues are more likely to appear during the “information processing” phase.

Identification is not seen in this context, as a benign synonym for authentication (the process of validating the user’s identity), but as a threat in an increasing framework of possibilities, constantly in expansion due to the great amount of databases available and the growing resort to more ways of performing identification (e.g. identification performed through camera images, or speech samples or fingerprints).

The threat with identification of the users and the IoT, has precisely do to with the fulfillment of its functionality – identify an individual using his data e.g. name, address, online identifiers – but, in a privacy violating context, also contributing to strengthen other threats (e.g. profiling and tracking by means of combining different data sources).

In fact, the threat doesn’t come from the “apple”, but from the act of “eating the apple”, it is not the identification itself that is the issue or threat, but the misuse of its potential when applied to a context where the processing of data is not (or is no longer) allowed because it lacks a legal ground.

Therefore, in our opinion it is not identification itself that is a threat, but the misuse of its potential, ultimately dwelling into processing without a legal ground as the real threat.

The second threat is localization and tracking who are functionalities necessary for many IoT systems, but who may also have a damaging potential to privacy, originating from the possibilities of determining and recording an individual’s location through space and time.

[152] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, Klaus Wehrle, “Privacy in the internet of things: threats and challenges”, in *Secur. Commun. Netw. 7(12)*, 2014, 2728–2742.

Tracking mechanisms include GPS or mobile phone location, among others. The harms connected to this threat are usually due to surveillance[153] of the users made possible with these technologies.

One of the possible applications of the IoT is in the security and surveillance industry (e.g. giving users the possibility to manage and control surveillance devices remotely, among others)[154].

The same reasoning, applied to the threat to privacy coming from identification, is in our opinion partially valid for the threat of localization and tracking.

It is a fact that the technologies enabling localization and tracking exist, and they are necessary in many IoT contexts, but the exploitation of these technologies potential in a harming manner is first of all a case of processing personal data without a valid legal ground.

The difference between a valid personal data processing activity and its opposite, is not found in the technology available, but on the context of the processing activity itself (it is necessary to know if personal data is processed only with a valid legal purpose and in respect of the individual's rights).

However, if the localization and tracking mechanisms are intended to be used for surveillance purposes (e.g. when there is a "surveillance use of technologies")[155] then, a valid legal ground and an evaluation in terms of necessity and proportionality needs to be made.

According to the European Data Protection Supervisor (hereafter, EDPS):

Surveillance is an intrusion on the fundamental rights to the protection of personal data and to the right to privacy. It must be provided for by law and be necessary and proportionate[156].

It is important to notice that this reasoning is applied to surveillance purposes, whether they are practiced with or without the help of IoT enabled devices. It has to do with the very nature of the surveillance activities themselves and not specifically with IoT.

The threat of profiling[157] in the IoT will probably become one of the most constant ones. In a study from Cognizant, regarding smart product economy, it is explicitly recognized that product data

[153] Going through the broader topic of surveillance, Minna Tiainen, "Solving the Surveillance Problem: Media Debates About Unwanted Surveillance in Finland", in *Privacy, Data Protection and Cybersecurity in Europe* (Springer, 2016), 61-76, follows the understanding of surveillance as a collection of information in order to manage or control. It is recognized that surveillance itself can be used in a beneficial way for society, but it also holds significant risks for privacy and other civil rights.

[154] For example Telit: https://www.telit.com/industries-solutions/smart-buildings/security-surveillance/ (accessed 05 May 2018).

[155] Elisa Orrù, "Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance", in *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer, 2017), 115. Explains that it is more appropriate to talk of "surveillance uses of technologies" than of "surveillance technologies". We can talk about a "surveillance use of technology" when "a technology application contributes to the realization of one of the surveillance mechanisms described above (discipline through actual or potential visibility, classification on the basis of collected information, prediction of future behavior, exclusion of particular groups and normalization of the majority)".

[156] https://edps.europa.eu/data-protection/our-work/subjects/surveillance_en (accessed 05 May 2018).

[157] The meaning of "profiling" according to Merriam-Webster, Merriam-Webster Online, https://www.merriam-webster.com/dictionary/profiling (accessed 05 May 2018), can be described as: "the act or process of extrapolating information about a person on known traits or tendencies".

has a radical impact on how products are built and sold, revealing also unprecedented customer insight (e.g. how the customer uses or wishes to use a smart product)[158].

As pointed out by Natali Helberger, on the topic of profiling and targeting customers in the IoT, the data collected by smart things is far more situational than the data collected about users online behavior, since it is real-time data collected by things that surround the customers[159], therefore it is very valuable data.

The threat of interaction and presentation is a very real IoT threat, and in a general manner it has to do with the difficulty of delimiting an "audience" for the messages (e.g. data, images, sound) that are conveyed by smart devices. This issue has a root cause on the interaction that the devices themselves are expected to have with their users and with the fact that those interactions can be observed by the public.

Ziegeldorf, Morchon and Wehrle, provide interesting examples of how this may occur (e.g. a query made by a user to a specific health clinic should not be answered by displaying the route on a public display close to the user and visible to others). The concerns brought by such examples, should be addressed by implementing privacy by design (hereafter, PbD) mechanisms, since the smart devices conception phase (we will explore this topic on chapter four).

The threat of lifecycle transitions goes in line with the topic we discussed above regarding security issues in the IoT, where we approached the subject of the necessity of security measures in the lifecycle management, from conception to decommissioning, considering both the device and the data perspective.

It is in fact, an indispensable measure in terms of the protection of the user's privacy to consider that the lifecycle of a device that collects personal data is not limited to the device itself.

The threat of inventory attacks, is a concrete type of attack that can be performed through IoT enabled devices. As we also discussed regarding the topic of security issues there are several types of possible attacks to IoT devices, many of them compromising also the privacy and personal data of the affected users.

In this particular type of attack, there is an unauthorized gathering of information about the existence and types of personal things. How is this attack processed?

> *With the realization of the All-IP and end-to-end vision, smart things become query-able over the Internet. While things can then be queried from anywhere by legitimate entities (e.g. the owner and authorized users of the system), non-legitimate parties can query and exploit this to compile an inventory list of things at a specific place, e.g. of a household, office building, or factory.*[160]

[158] The study also considers that digital data from the smart products is the real value. Euan Davis, "The Rise of the Smart Product Economy", Cognizant (May 2015), https://www.cognizant.com/InsightsWhitepapers/the-rise-of-the-smart-product-economy-codex1249.pdf (accessed 05 May 2018).

[159] Natali Helberger, "Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law", in *Digital Revolution: Challenges for Contract Law in Practice* (Nomos, 2016), 135-160.

[160] Ziegeldorf, Morchon, and Wehrle, op. cit., 9.

The threat of linkage has to do with the possibility of linking different (previously separated) systems, therefore contributing to an increased risk in data breaches, re-identification of data that had been anonymized and unauthorized access to personal data of the users.

With linkage there is a combination of data sources that were previously isolated and now come together, making more information available about the users than they meant to provide.

To sum up the subject of privacy and data protection threats in the IoT, and taking into consideration all that has been discussed so far:

- The problem of identification and (partially) also the problem of localization and tracking in the IoT (as presented), can be directed to the threat of processing personal data without a valid legal ground and/or in disrespect of the individuals rights;
- All types of possible attacks (not just inventory attacks) that exploit IoT vulnerabilities and grant undue access to personal data of the users are a threat to privacy and personal data protection;
- Another threat for privacy and for the protection of personal data, typical of the IoT, is the multiplicity of users that can share the same IoT devices (e.g. a common situation in home automation);
- In the scope of “future threats”, IoRT and the discussions over the statute given to more sophisticated robots is a legal challenge for the IoT, originated by the merge of both areas. Some of the legal challenges faced by robotics will have repercussions in IoRT.

With the purpose of addressing the current privacy and data protection challenges raised by the IoT, several approaches have been proposed by the research community[161]:

In order to reach the goal of protecting the user’s privacy and personal data, these approaches should not be implemented in an isolated manner, but instead in a cumulative logic, taking also into consideration the specific requirements of each device.

The use of encryption, or better said *cryptographic techniques*, is one of the main approaches used to protect personal data and privacy. Cryptography, which is in fact applying encryption to the concrete case, requires that some preliminary considerations are made in order contextualize this approach within the background of the IoT.

Cryptography, lato sensu, can be defined as "the practice of encryption, using secret codes for private communication"[162], and this practice - although with remarkable evolutions - began thousands of years ago, according to Michael Spiser, during the time of the Romans already Julius Caesar codified the messages that he sent to his generals, so that if they were intercepted their content was not immediately intelligible.

Cryptography is divided into three main branches[163]:

- Symmetric algorithms (the same secret key is shared between sender and receiver, being used for both encryption and message decryption);

[161] Clustering of proposed approaches based on the literature review from Noura Aleisa, Karen Renaud, “Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion)”, Cornell University Library (September 2016) https://arxiv.org/abs/1611.03340 (accessed 05 May 2018).

[162] Michael Spiser, *Introduction to the Theory of Computation* (Cengage Learning, 2013), 433.

[163] Christof Paar, Jan Pelzl, *Understanding Cryptography – A Textbook for Students and Practitioners* (Springer, 2010), 3-4.

- Asymmetric or public-key algorithms (there is a pair of different keys, using a public key to encrypt the message and a private key to decrypt it - the idea was proposed by Diffie, Hellman and Merkle) and;
- Cryptographic protocols (that in a simple way, deal with the application of the cryptographic algorithms - the Transport Layer Security (TLS) scheme used in Web browsers is an example of a cryptographic protocol).

Entering now in the area of IoT, and in connection to what was discussed above, it is clear that the use of cryptography is a powerful tool to guarantee the *confidentiality* and *integrity* of the information provided by users.

Mario Ballano Barcena and Candid Wueest report some worrying facts regarding the lack of encryption, for example, about 19% of all tested mobile applications that are used to control IoT devices do not rely on SSL connections to the cloud[164].

SSL (Secure Socket Layer) basically has the function of establishing an encrypted link between a server and a client, allowing sensitive information such as credit card numbers or login credentials to be transmitted in a secure way.

The lack of transport encryption raises serious privacy concerns, as users can share personal data, login credentials, and other relevant information about their habits that can cause serious harm if intercepted by attackers.

Another cumulative approach is the use of *privacy awareness or context aware systems*. These systems are based on location and gather information regarding the context. One example is the privacy preserving solution that provides context aware services based on location (e.g. a middleware, named Precise, should provide users with custom context-aware recommendations considering context information, location, privacy policies and previously visited places)[165].

The next cumulative approach identified is *access control*. However, the subject of access control presupposes that the user (program or device) who is accessing the data is “legitimate”, that there was an authorization to such access.

It is common in the scientific community, to distinguish between “authentication”, “authorization” and “access control”. The first two set the foundations for the access control policies, while this last one will set the requirements that describe how access to information is managed, to whom it should be granted, and in which cases.

The solutions available nowadays to implement access control policies are based on three different models[166]. We will adopt this distinction, and briefly approach the available models for access control policies.

[164] Ballano Barcena and Wueest, op. cit., 12.

[165] Alberto Huertas Celdran, Manuel Gil Perez, Felix Garcia Clemente, Gregorio Martinez Perez, “Precise: Privacy-aware Recommender Based on Context Information for Cloud Service Environments”, in *IEEE Communications Magazine* (IEEE, 2014), 90-96.

[166] David Ferraiolo, Rick Kuhn, Vincent Hu, “Authentication, Authorization, Access Control and Privilege Management”, in *Wiley Handbook of Science and Technology for Homeland Security* (John Wiley & Sons, 2010), 965-974.

Starting with *authentication*, an adequate authentication mechanism is necessary to ensure/validate that the user (program or device) who is accessing the data is actually a legitimate user (program or device).

The implementation of such mechanisms in an IoT context can prove to be complex, since many of the IoT devices are intended to interact with more than one user (e.g. the autonomous car who can be shared by more than one driver, the several home automation products that are intended to be used by a family, among several other examples).

The process of authentication corresponds to the process of validating an identity, the identity of a user, process or device[167].

As Michael Whitman and Herbert Mattord mention, there are three commonly used authentication mechanisms or factors, namely[168]:

- Things the user knows (e.g. passwords, PIN codes - this authentication mode is the most common, but it is also considered a weak authentication mode);
- Things the user has (ID cards, smartcards, electronic keys, digital signatures – these are personal objects and are also forms of authentication considered stronger than the previous ones), or;
- Something the user is (it has to do with personal characteristics - biometric – it is considered the strongest authentication method, although also with some orders of limitations, e.g. – false negative results in speech recognition caused by a common cold).

However, when we think about the IoT, the process of authentication is usually done by different means. These means are usually things the user has (or to be precise, considering the examples below, "things" the device itself has), and they can be *identifiers* or *network addresses*[169].

They include[170]:

- Medium Access Control (MAC) address, this is a unique identifier with 48 bits that is given by the manufacturer to every wireless and Ethernet device;
- Quick Response (QR) Codes, are mobile phone readable bar codes that are able to store a variety of data, such as: website URL's, text, phone numbers, email addresses[171];
- RFID[172];
- IPv4/IPv6, are global IP addresses schemes. The smart devices that are connected to the internet use IPv4 or IPv6 schemes[173] (the devices could also resort to private addressing schemes).

[167] Ibid, 965.

[168] Whitman and Mattord, op. cit., 248.

[169] The Factsheet on "Identification" of the Expert Group on the Internet of Things (IoT-EG), available at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2514 (accessed 06 May 2018), differentiates between the role of the identifiers and the network addresses. The ID of a smart device provides a unique handle to the device itself, whereas the address could change depending on the "physical location of object, its logical membership in one or several networks, or the current role of the object".

[170] Somayya Madakam, Hema Date, "Security Mechanisms for Connectivity of Smart Devices in the Internet of Things", in *Connectivity Frameworks for Smart Devices – Computer Communications and Networks* (Springer, 2016), 23-41.

[171] https://www.qrstuff.com/ (accessed 06 May 2018).

[172] Definition of RFID available on footnote 26.

As mentioned by Ferraiolo, Kuhn and Hu, authentication and authorization are fundamental to the process of access control, and they are also distinct concepts who are often confused due to their relationship with one another.

Authorization differs from authentication since it is "limited" to the yes or no decision of granting or denying access rights to a given user, program, or process. While authentication determines "who" is accessing, authorization determines what those who were previously authenticated are allowed to do[174].

Regarding the models for access controls policies, we note that they can be mandatory, non-discretionary or discretionary[175]:

- *Mandatory access controls* (MAC) are based on data classification systems, giving users limited access to information. Information is classified according to the different levels of relevance, and users can access only the information to which they are granted access;
- *Non-discretionary access controls* (e.g. RBAC) are managed by a central entity in the organization. They can be based on the roles assigned to a given individual - role-based controls - or can be also based on the tasks the individual has to perform - task-based controls;
- *Discretionary access controls* (DAC) are implemented in accordance with the discretion of the user of the data, so that users may allow general and unrestricted access or may allow specific individuals or groups of individuals to access the data.

IoT presents its very own set of challenges in access control due to some particularities, namely[176]:

- Low power requirements of IoT devices;
- Low bandwidth between IoT devices and the Internet;
- The distributed nature of the system;
- Ad-hoc networks and;
- The potential for extremely high numbers of connected IoT devices.

This means that the traditional access control models must be analyzed in detail before being applied to IoT.

For example, in the case of ACL (Access Control List) used in LBAC (lattice-based access control – a variant of mandatory access controls), we find that these lists store the users who hold

[173] Regarding the differences between IPv4 (the 32 bits long (4bytes) address) and IPv6 (the 128 bits long (16 bytes) address), additional details concerning the different concepts, the corresponding IP functions and also the use of IP addresses in internet protocols between IPv4 and IPv6, can be found in IBM Knowledge Center, https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzai2/rzai2compipv4ipv6.htm (accessed 06 May 2018).

[174] Ferraiolo, Kuhn and Hu, op. cit., 965-966.

[175] Andress, op. cit. 49-50; Boyce and. Jennings, op. cit., 17-18; Whitman and Mattord, op. cit., 246-247.

[176] Regarding this clustering, see Ilpo Suominen,"Access Control for Internet of Things", Intopalo, (May 2015) https://www.intopalo.com/blog/2015-05-25-access-control-for-internet-of-things/ (accessed 06 May 2018). Explaining also that, "On a high level, there are two ways to implement access control for IoT. In a distributed architecture, an access control server grants access tokens to users, who use them to access the IoT devices directly. In a centralized architecture, the user accesses only cloud-based servers that authorize the request and relay data between the user and the IoT devices."

authorization for each resource, which can be a challenge in the IoT domain where devices have low processing capacity making it difficult to update the list of users in a distributed system.[177].

Finally, another approach to address the privacy and data protection threats, is to conduct all personal data processing activities in accordance with the *data minimization* principle.

This approach is not IoT typical, in fact this principle who tells us that personal data should be adequate, relevant and also limited to what is necessary in connection with the purposes for which it is processed, is a legal requirement (art.5 (1) c) GDPR).

According to the EDPS glossary[178], compliance with this principle also requires that the controller only retains data for as long as it is necessary to fulfill the purpose(s) of processing.

Other approaches that can be applied (and in some cases, must be) to address privacy and data protection challenges are:

- The DPIA, and;
- PbD.

In the following chapter we will explore these approaches, in the context of the European legal framework regarding data protection and privacy, since they are also “prescribed” by the GDPR.

Chapter 4

Key Aspects of Personal Data Protection and Privacy for the Internet of Things in the European Legal Framework

The overall objective of this final chapter is to approach in detail the main points of the current European data protection and privacy legal framework that are “in scope” for the IoT.

An overview of the applicable legal framework was provided already in chapter 2, where the two relevant regulations were examined and their scope of application (material and territorial) was analyzed. Also, the topic of the fundamental rights behind them (the right to the protection of personal data and the right to respect for private life) was addressed, which provided a better understanding of “what” are the core rights they aim to protect.

In the previous chapters we answered already, partially, the two central and generic questions of our research that were always addressed within the context of the IoT, namely:

- How (applicable regulations, legal basis for processing, legal requirements to consider, among others), and;
- Where (in which situations) is the new European legal framework regarding the protection of personal data and privacy applicable to the IoT.

By answering these questions to the full and possible extent, while having also built an adequate technical background to place the “IoT” topic into perspective, we will have a complete

[177] Ibid.

[178] https://edps.europa.eu/data-protection/data-protection/glossary/d_en (accessed 06 May 2018).

overview of the status quo of personal data protection and privacy in Europe, when IoT is in the background.

Having answered these overall questions (with their own particular subset of questions embedded), we intend to contribute to the solution (or mitigation) of the potential effects of the identified risks that the IoT technology represents (or is foreseen to represent) for the protection of personal data and privacy, and ultimately for the data subjects/end-users.

In this chapter, we will go in depth to find the missing pieces for our answers, beginning by "overlapping" both European regulations that are relevant for the IoT, to understand if we will have a prevailing regulation when it comes to IoT.

Next, we will address in detail the concepts of "user, "end-user" and "data subject", the last two being two different designations and concepts to which both regulations resort to, and understand if there is any potential conflict between the two conceptual approaches adopted by the two regulations regarding the receiver of protection.

An understanding of the legal basis deemed legitimate to process personal data in the IoT and the principles that apply to this processing is vital. Alongside with the scope of application, these two topics set the main boundaries applied to IoT in the context of our research.

The remaining legal requirements to be observed by the data controller (and eventually) data processor are also relevant, since as we concluded in Chapter 3, they represent approaches prescribed the European legislator to address privacy and data protection challenges.

Another key aspect of personal data protection and privacy that is pertinent in an IoT context, is the determination of "who is who" in the IoT legal framework (data controller, data processor, supplier or integrator), since the obligations vary according to the given role.

4.1. Overlapping the General Data Protection Regulation, the ePrivacy Proposal and the Internet of Things

As we analyzed in point 2.3 of chapter 2, the two regulations, GDPR and the ePrivacy Proposal, at their core are designed to protect distinct fundamental rights (the right *to the protection of personal data* is protected by GDPR, while the *right to respect for private life* is protected by the ePrivacy Proposal).

These different fundamental rights, in turn, are connected to two different dogmatic realities that are often mixed and perceived has having a similar meaning, but are not synonyms: *data protection* and *privacy*.

As we demonstrated through a brief excursion of both dogmatic perspectives, the fundamental right to respect for private life is closer to privacy, while the fundamental right to the protection of personal data is closer to data protection.

Both regulations have a different scope and are tied to different dogmatic realities, however as we also briefly concluded, they also share certain common traits:

- Together they form the relevant legal landscape for IoT in Europe when personal data is processed;

- The ePrivacy Proposal is *lex specialis* in regards to GDPR.

The "overlapping" issue between GDPR and the ePrivacy Proposal is therefore only possible and relevant in an IoT environment, when personal data is being processed.

There are certain legal requirements that will only arise (and be applicable) if personal data is being processed in an IoT environment, and certain legal requirements that will arise (and be applicable) regardless the processing of personal data is taking place in an IoT environment or not.

This last category of legal requirements, due to the analyzed scope of the ePrivacy Proposal and its applicability to IoT, requires that the requirements set out by this regulation are respected even when personal data is not processed.

In our opinion, and in a certain way, GDPR can be seen as a *plus* whenever personal data is being processed in an IoT context, since:

- On the one hand, we can also have the (residual case) case of smart devices that do not process personal data[179], and;
- On the other hand, we can have additional data protection legal requirements, whenever personal data is processed in an IoT context, since GDPR is to cover eventual "gaps" regarding the processing of personal data in the ePrivacy Proposal (as mentioned in point 1.2. of the Explanatory Memorandum," all matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR).

Therefore, it seems there is not a real "overlapping" of regulations (they are not aimed at regulating over the same topics[180]), but if we attend to the logic behind considering the ePrivacy Proposal as *lex specialis* we can say we do have a "prevailing" EU regulation when it comes to the IoT[181].

As stated by Tobias Lock, among many others, the rationale behind the principle *lex specialis derogat legi generali*, is to solve norm conflicts in favour of the more specific rule, in this case in favour of the ePrivacy Proposal, as *lex specialis*[182]*.*

It is possible, that any additional demands that might come with GDPR bring an increased complexity to the legal framework set by the EU legislator. However, it should be noticed that this complexity is more a product of the increased challenges that are set forth with the new regulations (in fact, not only GDPR, but both regulations bring new challenges), than a product of a need to attend to the landscape of two regulations in the IoT when personal data is being processed, since this was already the case with the previous EU Directives regulating over IoT[183].

In our opinion, a strategy that could prove to be helpful in tackling the complexity and increased difficulty brought by the new EU legal framework for privacy and data protection, could be

[179] The Opinion of Article 29 Data Protection Working Party, already stated in footnote 93, considers that in the IoT there is usually a processing of personal data.

[180] Rec.5 of the proposal for the ePrivacy regulation states: "The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data".

[181] Raising the question of the possibility of a prevailing regulation: Gabriela Zanfir-Fortuna*,"* Will the ePrivacy Reg overshadow GDPR in the age of IoT?", (February 2017), https://iapp.org/news/a/will-the-eprivacy-reg-overshadow-the-gdpr-in-the-age-of-iot/ (accessed 13 May 2018).

[182] Tobias Lock, op. cit., 51.

[183] According to Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, mentioned previously on footnote 3.

the "clustering" of cases in which the ePrivacy Proposal is clearly *particularizing* the general rules on the protection of personal data laid down by GDPR regarding ECD that qualifies as personal data, and the cases in which the ePrivacy Proposal is *complementing* GDPR (Rec. 5 of the ePrivacy Proposal)[184].

In the first case, when the ePrivacy Proposal particularizes the general rules of GDPR, there is an underlying conflict between the rules of both regulations that cover the same topic on a distinct manner. In the second case, when the ePrivacy Proposal complements the general rules of GDPR, there is no underlying conflict of rules, merely an additional rule that is to be applied.

Let us consider the following examples relevant for the IoT, of situations for both possible scenarios:

1) *Example of a situation in which the ePrivacy Proposal complements GDPR:*

Consent, a lawful ground for processing, according to art 9 (3) of the ePrivacy Proposal, requires that the end-user who has consented to the processing of ECD can withdraw its consent at any time, and additionally is reminded of such possibility at periodic intervals (of 6 months), or as long as the processing activities continue.

The first obvious difference is that this article unlike what happens with GDPR (which is only concerned with the processing of personal data), applies to the processing of ECD (which may or may not contain personal data)[185]. The second less obvious difference that constitutes an addition to GDPR on the topic of "consent", is that the ePrivacy Proposal, contemplates the inclusion of a "reminder" function regarding the withdraw of the previously given consent.

2) *Example of a situation in which the ePrivacy Proposal particularizes GDPR:*

Third parties – art.10 of the ePrivacy Proposal regarding "*Information and options for privacy settings to be provided*", sets as a requirement that end-users are provided with the option of determining by means of software settings, if they allow third parties to access or store information on the devices.

This provision not only particularizes what is determined in GDPR, as it is also considered by EDPS as being inconsistent with art.25 GDPR, regarding "*Data protection by design and by default*".

Art.25 GDPR, requires from the data controller to implement technical and organisational measures (hereafter, TOMs), to ensure that, by default, only the necessary personal data for each purpose of processing is indeed processed (this obligation is applicable, among others, to the storage and accessibility of personal data that has been collected).

Therefore the EDPS recommends the ePrivacy Proposal to:

> *Impose an obligation on hardware and software providers to implement default settings that protect end users' devices against any unauthorised access to or storage of information on their devices*[186].

[184] Regarding this topic, Zanfir-Fortuna, op. cit.

[185] According to art.4 (3) b) of the ePrivacy Proposal, ECD means: electronic communications content and metadata.

[186] EDPS, Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Brussels, 24 April 2017, 19.

The relationship between GDPR as *lex generalis* and the ePrivacy Proposal as *lex specialis*, requires that, specially, in those cases in which the ePrivacy Proposal is particularizing the GDPR by setting rules to regulate differently over the same matters, there is not a conflict that results in a lower level of protection that is enjoyed by natural persons under the scope of the GDPR (Rec. 5 of the ePrivacy Proposal).

There is still a third "cluster" of cases (those ones not raising the same difficulties as the above ones), in which GDPR acts as a general rule in the matters concerning the processing of personal data that are not specifically addressed by the ePrivacy Proposal(e.g. rights of the data subject (end-user)), as mentioned in point 1.2. of the Explanatory Memorandum.

4.2. End-user and Data Subject: Different Levels of Protection?

Unlike previous generations, characterized by the absence or limited amount of technologies that allow the instant access to information and entertainment contents worldwide, and the sending and receiving of information with a few simple "clicks", today's generations would find it hard to live without everyday technologies, such as the Internet, computers or Smartphones, that among others, became embedded in our routines.

It is this particular "belonging" to a life surrounded by these technological advances that turns an individual into a "Digital Native", a term coined by Marc Prensky in 2001, to refer to the following reality:

> *Our students today are all "native speakers" of the digital language of computers, video games and the Internet[187].*

There is also a differentiation to be made between the so called "Digital Natives" and the "Digital Immigrants", who are those not born into the digital world, but that have, in a latter point in life, adopted the majority of the aspects of the new technologies used by the Digital Natives.

Therefore, it is a fact that either by "birth" or by "naturalization" we are living in a digital era, where the individual is fragmented into a "user" of these technologies (in fact, into a multiplicity of "users", if we consider the individuality of each digital platform or smart device we as individuals use).

As we have made reference to before, the concepts that are relevant to our research are those of the "end-user" and "data subject", considered to be the concepts that represent the individuals who are granted protection, either under the ePrivacy Proposal ("end-user"), either under the GDPR ("data subject"), and when it comes to the IoT (since both regulations are applicable in their own way), both concepts come together and give shape to the designated recipient of protection.

[187] Marc Prensky, "Digital Natives, Digital Immigrants Part 1", in *On the Horizon*, Vol. 9 Issue: 5, 1-6, doi: 10.1108/10748120110424816

In the GDPR, the data subject is primarily referred to as an *identified or identifiable natural person* (art.4 (1) GDPR, while providing the definition of "personal data", also delimiting the concept of "data subject").

As previously mentioned, the definition of "end-user" adopted by the ePrivacy Proposal, rests on the definition provided in art. 2 (14) of the EECC Proposal (art.4 (1) b) of the ePrivacy Proposal).

Having in mind this diversity of approaches regarding the recipient of protection, and taking into consideration our background, the IoT, and the necessity of considering both regulations that have opted not only for a different terminology for the recipient of protection, but also for different conceptual meanings, one must ask:

- Is this different conceptual terminology equivalent to a different (perhaps, lower) level of protection granted to the "end-user" in the ePrivacy Proposal, when compared to the protection granted to the "data subject" in the GDPR?

The relevance of this question rests on the following facts:

- The same individual (natural person) can be a "data subject" and an "end-user" for the same processing, in an IoT context, plus;
- As previously mentioned, the ePrivacy Proposal should not lower the level of protection of natural persons provided by the GDPR.

Concerning the root-cause for this question, the EDPS in its *Opinion on the Proposal for a Regulation on Privacy and Electronic Communications*[188], considered that the definition of end-user has a central role in the ePrivacy Proposal (as we also mentioned previously in section 2.2., regarding the logic of the application scope, both material and territorial of the ePrivacy Proposal, largely resting on the "end-user" concept).

According to the EDPS, this central role should provide an indication of the entity whose fundamental rights are to be protected[189].

However, there are critics to be pointed out to the definition of "end-user" as it is contemplated in the EECC Proposal.

This definition makes reference to:

> *Natural persons or legal entities who have a contract with an electronic communications service provider and do not provide electronic communications services*[190]*.*

It seems the answer to our question is, for the current moment of uncertainty regarding the final text of the ePrivacy Proposal (which will probably take into consideration some remarks that have been made, including by the EDPS), not in favor of the current terminology used.

There is in fact a negative impact on the level of protection in the ePrivacy Proposal for the end-users, due to the fact that the meaning behind the terminology "end-user" affects the protection granted to individuals.

[188] EDPS, Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), 12.
[189] Ibid.
[190] Ibid.

In line with the understanding of the EDPS, we consider that the use of the wording "end-user" with the meaning above does not provide the necessary guarantee, in order to ensure that the fundamentals rights of all the intended receivers of protection (all "end-users" using electronic communications services), in scope of the regulation are covered.

Giving that we are in the realm of fundamental rights, the proposal of the EDPS would be to resort to a terminology purposely defined for the objective. The terminology should make reference to *a natural person using electronic communications services without necessarily having subscribed to it*[191].

Furthermore, and in line with the *Opinion on the Proposed Regulation for the ePrivacy Regulation* of the Article 29 Data Protection Working Party (point 40 a)), the definition of "end-user" in art.2 (14) of the EECC Proposal should clarify that the individuals who contribute to networks are not outside from the protection scope of the ePrivacy Proposal (e.g. those who mesh networks with their router)[192].

There are, however some positive aspects to be noticed regarding the protection granted to the "end-users", namely:

- According to the *Opinion on the Proposed Regulation for the ePrivacy Regulation* of the Article 29 Data Protection Working Party (point 8), the fact that the proposed regulation has dispensed the differentiation between "subscribers" and other users of electronic communication services, is a welcomed improvement towards the goal of granting an equal level of protection to all end-users[193];
- We observe that also, in the EECC Proposal (from where some of the key concepts are originated, including the "end-user" one), there is no longer a definition of "subscriber", and the term "subscriber" has been replaced with "end-user", in the vast majority of cases (in recs.64, 241, 258, arts. 2 (9), 83, 91, 99 (2), (5) and (6), 104 (1), 114 (3)).

Both the EDPS and the Article 29 Data Protection Working Party, raise attention to the problematic of the use by the ePrivacy Proposal of definitions for some of its key concepts (including, the concept of "end-user") from the proposed EECC, which is a different legal instrument and currently merely a Proposal (and therefore, can be subject to changes thus, is surrounded by a certain degree of uncertainty).

According to the Article 29 Data Protection Working Party these definitions can become "moving targets", and the ideal solution for this issue would be that, all the concepts that come from the EECC Proposal would be independently defined in the ePrivacy Regulation[194]. As we just analysed above, the proposal from the EDPS is in the same direction, of adopting a terminology designed for the objective.

[191] Ibid.

[192] Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), (WP247), Brussels, 04 April 2017, 26.

[193] Ibid., 8.

[194] Ibid, 25.

If the ePrivacy Regulation takes into consideration the remarks made by both, the EDPS and the Article 29 Data Protection Working Party regarding this particular topic, individuals using IoT products will not experience in practice the issues raised by this different level of protection.

Nevertheless, even if the suggested improvements are welcomed by the EU legislator, it is still noteworthy how an apparently simple imbalance in the extension granted to a concept can create a lack of harmony between two intertwined regulations, and ultimately dwell into a disadvantage for the affected natural persons (eventually, affecting fundamental rights).

4.3. Lawful grounds for processing in the IoT

The lawful grounds for processing personal data in the IoT, are yet another manifestation of the strategic relationship established between the GDPR (as *lex generalis*) and the ePrivacy Proposal (as *lex specialis*).

In fact due to this relationship model, the overall delicate articulation between both regulations, in this particular topic of the legal grounds for processing personal data, is filled with additional complexity.

Due to the intrinsic dynamic between *lex generalis* and *lex specialis,* the first question to be raised is the following:

Are the legal grounds of processing, a topic where the ePrivacy Proposal, as *lex specialis*, particularizes or complements the GDPR?

If it is the first case, as mentioned previously, there could be a potential underlying conflict between the rules of both regulations covering the same topic, if they aim into different directions. If it is the second case, the ePrivacy Proposal just complements the general rules of GDPR.

In this particular case, the answer from the EU legislator is quite explicit: rec.5 of the ePrivacy Proposal, specifically mentions the following[195]:

Processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation.

Ultimately, the inclusion of this wording leads to the exclusive application of the legal grounds of processing of the ePrivacy Proposal (and the exclusion of the legal grounds presented by the GDPR), in all the cases in which[196]:

- ECD is qualified as personal data, plus;
- The electronic service providers are qualified as data controllers for that particular processing.

Let us proceed with a brief analysis of the lawful grounds for processing, both under the GDPR and the ePrivacy Proposal.

[195] Regarding this topic, Zanfir-Fortuna, op. cit.
[196] Ibid.

Beginning with the GDPR, the first remark to be made is that in fact, its catalogue of legal grounds for processing personal data is different, and wider, than the one presented in the ePrivacy Proposal.

Art.6 (1) GDPR, presents a cast of six potential legal grounds for the processing to be compliant with the regulation, namely:

- *Consent* - art.6 (1) a) GDPR;
- *Performance of a contract* - art.6 (1) b) GDPR;
- *Compliance with a legal obligation* (e.g. data retention periods coming from tax or business law requirements) - art.6 (1) c) GDPR;
- Protection of *vital interests* (of the data subject or of another natural person) - art.6 (1) d) GDPR;
- Performance of a task carried out in the *public interest* or in the *exercise of official authority* - art.6 (1) e) GDPR;
- *Legitimate interests* (pursued by the controller or a third party) - art.6 (1) f) GDPR.

The ePrivacy Proposal, presents a more restricted catalogue of options for data processing, in its art.6, regarding the "*permitted processing of electronics communications data"*.

This article aims to dictate the grounds on which all processing activities concerning ECD are allowed. The article is structured in the following manner:

(1) Legal grounds for *providers of electronic communications networks and services* to process *electronic communications data*;

(2) Legal grounds for *providers of electronic communications services* to process *electronic communications metadata*, and;

(3) Legal grounds for *providers of electronic communications networks and services* to process *electronic communications content.*

Consent, is in fact the most common legal ground for processing, being considered a legal ground for processing in art.6 (2) c), (3) a) and b) of the ePrivacy Proposal.

Other grounds of processing include: *a criteria of necessity to achieve the transmission of the communication* art.6 (1) a), or the *maintenance or restoration of the security of electronic communications networks and services*, among others of diminished application for our context.

Also article 8 of the ePrivacy Proposal regarding the "*protection of information stored in and related to end-users' terminal equipment"*, needs to be considered in the realm of legal grounds for processing[197].

On a similar logic to article 5(3) of Directive 2002/58/EC, it applies:

[197] Ibid. This nuance regarding *storing of information*, or *gaining access to information that has already been stored in the smart device*, predates the era of the GDPR and the ePrivacy Proposal. In fact, it was targeted by the Working Party's guidance on several occasions, concerning the *simultaneous application of the requirements of Article 7(a) and Article 5(3) of Directive 2002/58/EC.* The Opinion of Article 29 Data Protection Working Party *on Apps on smart devices*, 14 and ff., stresses that regarding *storing of information*, or *gaining access to information that has already been stored in the smart device*, there was a tighter restriction of the legal grounds that could be taken into account, introduced by Article 5(3) of the ePrivacy Directive.

> *To situations when an IoT stakeholder stores or gains access to information already stored on an IoT device, in as much as IoT devices qualify as "terminal equipment "[198].*

Article 8 of the ePrivacy Proposal lays down a set of exceptions, to the *overall prohibition* regarding the *use of processing and storage capabilities of terminal equipments*, as well as *the collection of information from end-users' terminal equipment* (including about its hardware and software), other than by the end-user.

Ultimately it means, that one of the exceptions laid down in art.8 of the ePrivacy Proposal, must be applicable so that someone else apart from the end-user (e.g. device manufacturer or other stakeholders) can use the information stored in the terminal equipment, including information (hardware and software) about the equipment itself.

From the four exceptions foreseen in art.8 (1) of the ePrivacy Proposal, the ones that present a greater relevance for the IoT are:

- *Consent*, and;
- A necessity criteria originated in the *provision of an information society service*[199], upon request of the end-user.

This last exception can also be applied to the IoT, since the *apps on smart devices are considered to be information society services*[200].

There is also a need to consider art.8 (2) of the ePrivacy Proposal due to its impact for the IoT, namely, in the *connection between IoT devices*. The article states, as a general rule, that:

> *The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited*

There are, however, two exceptions granted:

[198] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, 14. Also providing an illustrative example that can be transported to the context of the ePrivacy Proposal on how this provision can be applied: "*A pedometer records the number of steps made by its user and stores this information in its internal memory. The user installed an application on his computer to download directly the number of steps from his device. If the device manufacturer wants to upload the data from the pedometers to its servers, he has to obtain the user's consent under Article 5(3) of directive 2002/58/EC. Once the device manufacturer has uploaded the data on its servers, it only keeps aggregated data about the number of steps per minute. An application requesting access to such data, in as much as it is stored on the server of the device manufacturer, is then not subject to article 5(3) of the e-Privacy Directive but to the provisions of Directive 95/46/EC relating to the legitimacy of this further processing*."

[199] In this case it is the definition of "information society service" to which GDPR resorts to that is applicable, according to art.4 (1) a) of the ePrivacy Proposal. Art. 4 (25) GDPR, in turn, states that:" *'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council*". Directive (EU) 2015/1535, defines an "information society service", as: "*(…) any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*". In Article 1(1) b), i), ii) and iii) of Directive (EU) 2015/1535, the several components of the definition are also clarified: *"'at a distance' means that the service is provided without the parties being simultaneously present; by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request*".

[200] Article 29 Data Protection Working Party, Opinion 02/2013 on Apps on Smart Devices (WP202), Brussels, 27 February 2013, 25 (footnote 46).

- If the collection of information emitted by the terminal equipment, is done exclusively, and only for the necessary time, to establish a connection - art.8 (2) a) of the ePrivacy Proposal, or;
- As a minimum standard, there is a very clear and visible notice displayed, with information regarding the modalities of the collection, its purpose, the responsible for the collection and other information required under art.13 GDPR, as well as the measures available for the end-user, to stop or minimize the collection.

After this brief analysis of the lawful grounds for processing under the GDPR and the ePrivacy Proposal, two central questions remain to be answered:

1) When are the legal grounds for personal data processing of the GDPR applicable in the IoT context?
2) From those legal grounds, which of them can be of use to the IoT context?

Regarding our first question, the answer can be found by means of a negative delimitation: whenever we fall outside the restricted scope provided by the EU legislator that requires the exclusive applicability of the ePrivacy Proposal (rec.5 of the ePrivacy Proposal), and only then, it is possible to consider the legal grounds of the GDPR.

Furthermore (even on this particular case), it should be noticed that this is only of relevance for our topic if the second cumulative condition is not present, meaning: *the electronic service providers are not qualified as data controllers for that particular processing*. Since the first condition must be present for the GDPR to be applicable - the data has to be personal data.

Therefore, if we come under the conclusion that the ECD that is being processed, does not qualified as personal data, the GDPR would not be part of the equation.

Regarding our second question, of knowing from the legal grounds present in the GDPR which of those can be applied to the IoT context, the Opinion of Article 29 Data Protection Working Party on the *Recent Developments on the Internet of Things*, while still resting on the previous Directive (art.7 of the Directive 95/46) can be transposed to the current reality of the GDPR[201], providing us the adequate legal "clustering".

Therefore, in practice, there are three relevant legal grounds in the GDPR that can be applied to the IoT context[202].

Starting with *consent*, it is considered to be the first and most reliable legal ground to be applied to the IoT landscape by the several stakeholders involved (e.g. device manufacturers, social or data platforms, device lenders or third party developers[203]).

Under the GDPR (recs. 32, 42 and 43, and arts. 6 (1) a), and 7 GDPR[204]), consent should be:

- Given by a *clear and affirmative act*;

[201] On the same direction, considering the same legal basis for processing in the IoT and already in the GDPR context, Voigt and von dem Bussche, 241-242.

[202] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, 14.

[203] Ibid.

[204] Also the requirements laid down in art.8 GDPR, regarding the specific situation of child's consent in relation to information society services, need to be considered for the processing of personal data of a child below the age of 16 years old.

- Establishing a *freely given*, *specific*, *informed* and *unambiguous* indication of the data subjects' acceptance to that processing of personal data;

For that purpose consent is to be provided by means of a written statement, which includes electronic means (e.g. *ticking a box in a website or choosing technical settings for information society services, such as apps, are possibilities*), or by an oral statement.

Since consent requires a *clear and affirmative act*, the silence of the data subject, its inactivity when receiving a request for consent, or the use of pre-ticked boxes should not be considered as valid means of obtaining consent.

Due to the fact that consent needs to be *specific*, *informed* and *unambiguous*, it should cover all processing activities that are carried out under the same purpose(s), and if there is a multiplicity of purposes, consent needs to be obtained for all of them.

Regarding consent on the IoT context there are yet, two important considerations that need to be made.

The first consideration is a result of the relationship between GDPR and the ePrivacy Proposal, as noted by the EDPS it is not clear under the current wording of the ePrivacy Proposal, in cases where there is a consent of the end-user to a service provider to transfer content or metadata to a third party (acting as a controller), if the processing of this data by the third party will have to abide by the GDPR rules or by the ePrivacy Regulation (assuming the wording from the ePrivacy Proposal remains unchanged)?

The application of the ePrivacy Regulation, based on the current wording of the ePrivacy Proposal, would mean that processing by a third party would need to be based on consent or another exception foreseen, while the application of GDPR opens the possibility of considering all its legal grounds for processing to this third party[205].

Therefore, and to prevent any circumvention, the EDPS recommends:

> *That the Proposal specify, in a substantive provision, that 'neither providers of electronic communications services, nor any third parties, shall process personal data collected on the basis of consent or any other legal ground under the ePrivacy Regulation, on any other legal basis not specifically provided for in the ePrivacy Regulation.'*[206]*.*

The second consideration is a result of the unclear definition of the provider of consent, namely, the end-user which was adopted by the ePrivacy Proposal. As pointed out by EDPS, the ePrivacy Proposal must ensure the following[207]:

[205] EDPS, Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), 15.

[206] Ibid, 16.

[207] Ibid, 13-15. The EDPS recommends that a stand-alone definition of the concept "end-user" is adopted in the Regulation: *"The definition should build on the following four elements: (i) natural person (ii) using a publicly available electronic communications service (iii) for private or business purposes, (iv) without necessarily having subscribed to this service"*. Plus, when consent is requested from the end-user the ePrivacy Proposal, for a matter of consistency, should make reference to "all end-users".

- That the consent obtained is given by the individuals using the service, for example, tenants, employees, hotel guests, among others (the subscriber may not be the one or the only one using a service);
- Consent must be obtained from all parties (both senders and receivers);
- The rights and freedoms of other individuals (other than the communicating parties) must also be ensured, and any processing based on end-user consent must not affect them adversely.

The other two legal grounds for personal data processing enshrined in the GDPR, possibly applicable in the IoT context are[208]:

- Performance of a contract (art.6 (1) b) GDPR) – this legal ground is considered to be of diminished application, since the processing based on the performance of contract where the data subject is part, must abide by a *necessity criteria*. According to the Article 29 Working Party, the criteria of necessity, requires "*a direct and objective link between the processing itself and the purposes of the contractual performance expected from the data subject*"[209].
- Legitimate interests, pursued by the controller or a third party (art.6 (1) f) GDPR) – the processing of personal data based on the legitimate interests of a controller or a third party requires that those legitimate interests are not outweighed by the interests or the fundamental rights and freedoms of the data subject (an example of possible cases of legitimate interest is when the data subject is a client or in the service of the data controller - rec.46 GDPR).

4.4. Applying the Principles Related to Personal Data Processing to the Internet of Things

Concerns about safeguarding individuals' personal data must be present, in several dimensions, in every processing of personal data that is carried out. Those dimensions are intended to cover matters such as, the amount of data collected, why and how is data collected, for what is it collected, how long can it be kept, and other issues that relate with data quality and information security objectives (integrity and confidentiality).

To ensure this ever present necessity, the EU legislator regulated the matter, placing it under the aegis of principles intended to be transversal to any processing of personal data. These principles enshrined in the GDPR, are also applicable to the IoT, as they were before when the Directive 95/46/EC was in place.

As mentioned, by Article 29 Working Party, in their *Opinion on the Recent Developments on the Internet of Things*:

[208] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, 15.

[209] Ibid.

> *Taken together, the principles enshrined in Article 6 of Directive 95/46/EC constitute a cornerstone of EU data protection law[210].*

Currently, it is art.5 GDPR who enshrines the principles for processing personal data that constitute the basis for personal data processing in compliance with the EU legal framework:

- *Lawfulness, fairness and transparency* – this principle requires that personal data is always processed lawfully, fairly and in a transparent manner in relation to the data subject – art.5 (1) a) GDPR. This means that:
    - The data subject should be informed of the existence of the processing operation and its purposes, according to the principles of fair and transparent processing (rec.60 GDPR), plus;
    - There are previous requirements that need to be fulfilled in order to ensure that personal data is processed in a lawful manner (art.6 GDPR);
- *Purpose limitation* – requires that data is only collected for specified, explicit and legitimate purposes. The collected data cannot be further processed in a manner that is incompatible with the initial purpose(s), and those purposes need to be defined *before* the processing activities start, this aspect takes away the possibility of having sudden changes in the "key conditions" of the initial designed purpose(s)[211] – art.5 (1) b) GDPR;
- *Data minimization* - only the data that is necessary should be processed, there should be a minimization of the storage time, and the erasure of personal data after it has fulfilled its purposes and there is no other legal ground to justify a longer data retention period.

  However, the implementation of the data minimization principle in the IoT can prove to be a challenge, due to the large quantities of data the devices are expected to collect from their surrounding environment. In fact:

  > *All those interconnected devices produce an amount of data that is almost literally unimaginable. IoT data is measured in zettabytes, a unit equal to one trillion gigabytes. Cisco estimates that by the end of 2019, the IoT will generate more than 500 zettabytes per year in data[212].*

  This high volume of collected data can produce an impact in data breaches, since the possibilities of a data breach also increase with a greater amount of data being collected – art.5 (1) c) GDPR.
- *Accuracy* – the principle of accuracy is intimately connected with data quality. Personal data needs to be accurate and kept up to date, and whenever this data is inaccurate it should be erased or rectified without delay – art.5 (1) d) GDPR.

[210] Ibid, 16.

[211] Ibid.

[212] Melissa Liton, "How much data comes from the Internet of Things?", (February, 2018), https://www.sumologic.com/blog/machine-data-analytics/iot-devices-data-volume/ (accessed 26 June 2018).

- *Storage limitation* – aims to ensure that personal data that is no longer necessary is not kept in a form which allows the identification of data subjects when the processing purpose(s) are exhausted – art.5 (1) e) GDPR.
- *Integrity and confidentiality* – were already discussed above, since alongside with "availability", they are also part of the information security objectives – art.5 (1) f) GDPR.
- *Accountability* – this principle determines that the data controller must be able to demonstrate compliance with all the above principles - art.5 (2) GDPR.

  The principle of accountability means that abiding by the principles for processing personal data described in art.5 (1) GDPR is not enough, the evidence of compliance must also be produced. This evidence can be supported by several instruments, namely audits, certifications or even through other obligations imposed by the GDPR (e.g. the record of processing activities - art.30 GDPR, among others).

How are those principles applied to the IoT? IoT products need to consider these principles in an early stage, especially when implementing privacy by design and privacy by default concerns.

Personal data processing activities (which start with the collection of personal data), need already to be compliant with the principles defined in GDPR before the data collecting activities start.

The link between the implementation of these principles and PbD is evident, and was also included in art.25 (1) GDPR, which is concerned with privacy by design and by default. There the EU legislator made reference to the fact that the controller should implement appropriate TOMs, which in turn are designed to implement data protection principles in an effective manner.

Furthermore, it is through the observance of these principles in an early stage of product or services development, and its consideration in the development of a privacy by design and privacy by default framework, that the rights of the data subjects foreseen in GDPR will be considered and protected even in complex environments where large amounts of data are processed, such as IoT.

4.5. Data Protection by Design and by Default: Engineering Privacy in the Internet of Things

One of the novelties brought by the EU legal framework regarding data protection with particular relevance for the IoT domain, is the requirement of developing services and products that process personal data according to the principles of data protection by design[213] and by default (art.25 GDPR).

As discussed in the above section, the topic of PbD is intimately connected with the implementation of the principles that relate to personal data processing enshrined in the GDPR.

In fact, in a recent report from the Norwegian Consumer Council (Forbrukerrådet), concerning the use of dark patterns by tech companies to discourage us from exercising our rights to privacy, data protection by design is defined by reference to GDPR principles:

[213] The framework of Privacy by Design was created previously by Ann Cavoukian. This framework was built with the purpose of proactively embedding privacy into the design specifications of information technologies, network infrastructure and business practices. Ryerson University – Privacy by Design Centre of Excellence, "Dr. Ann Cavoukian, Distinguished Expert in Residence", https://www.ryerson.ca/pbdce/about/ann-cavoukian/ (accessed 05 July 2018).

> *Data protection by design means that services should be designed to ensure that data minimisation, purpose limitation, and transparency are safeguarded. In addition to limiting the data collected, appropriate and effective measures to ensure the integrity and confidentiality of the data should also be implemented*[214]*.*

As pointed out by the creator of the PbD framework, Ann Cavoukian, PbD was a result from the evolution of initial efforts to express Fair Information Practice Principles straight into the design and operation of information and communication technologies, which resulted in the implementation of Privacy Enhancing Technologies (hereafter, PETs)[215].

The PbD framework[216] rests on seven foundational principles that describe its implementation on an abstract level. This framework and its principles find a fertile ground of application in the IoT[217], for example the first principle that asks for a proactive (and not reactive) approach, when applied to the IoT context should anticipate and eliminate any imbalances and abuses, let us analyze one example of the utility of this principle for the IoT domain.

For instances, the value of a toaster with no added functionalities and no capacity for data collection, but able to execute its primary purpose (toast bread) should be weighed against the value of a toaster equipped with sensors and connectivity and the extra functionalities provided by them[218].The added value of an IoT enabled device should be clear in order to transit from its analog version to the connected one.

In turn, data protection by default, is directed towards the implementation of TOMs that *by default*, ensure that only the personal data that is necessary for each specific purpose of the processing is being processed.

As clarified in art.25 (2) GDPR, the obligation to implement privacy by default, extends to: the amount of personal data collected, the extent of the processing, the period of storage and the accessibility of such data.

This means that by default - without the necessity of taking any action to ensure it – personal data should only be collected if it is necessary to ensure a specific purpose of processing. In practice, this means that the data subject should not have to actively opt-out, to prevent the data processing.

[214] Norwegian Consumer Council (Forbrukerrådet), ”Deceived by Design – How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy”, Forbrukerrådet, June 2018, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/ (accessed 05 July 2018), 8.

[215] Ann Cavoukian, "Privacy by Design: Leadership, Methods, and Results", in *European Data Protection: Coming of Age* (Springer, 2013), 175-194.

[216] Elisa Orrù, op. cit., 107-108, highlights the fact that "(…) one of the core assumptions of PbD is the 'win-win' principle, according to which there is no trade-off between privacy and security."

[217] Ann Cavoukian, Claudiu Popa, "Embedding Privacy Into What's Next: Privacy by Design for the Internet of Things", Ryerson University – Privacy & Big Data Institute, April 2016, 4. The first principle states that the approach towards privacy should be proactive and not reactive, the second principle includes privacy concerns as default settings, the third principle states that privacy should be embedded into design, the fourth principle speaks of full functionality (positive sum, not zero sum), the fifth principle is related to end-to-end security (full lifecycle protection), the sixth principle is aimed at ensuring visibility and transparency, and the final and seventh principle is about the respect for the user and the need to keep it user-centric.

[218] Ann Cavoukian, op. cit.,6.

In its analysis the Forbrukerrådet, approaches the cases of tech giants Facebook and Google, and among several noteworthy remarks, points to the worrying fact that privacy intrusive default settings are being used, as is the case of the face recognition feature used by Facebook, where the privacy intrusive default settings are in fact being hidden from the user.

If the users want to change the settings to turn on face recognition, they have to click "Accept and Continue", and strangely if the users want to keep the face recognition feature turned off they have to choose the option "Manage Data Settings" and *actively turn the option off*[219].

The correct interpretation of privacy by default does not allow dark patterns to coexist with transparency, this means that users who do not wish more data to be processed should not have to search in the default settings to turn the option off[220].

The objectives of PbD should be addressed in a double perspective: integration of privacy in the organization and integration of privacy in the systems[221].

From a best practices point of view, engineering privacy in the IoT (in each IoT implementation), starts with the definition of the functional and operational requirements, the delimitation of the personal data that should be collected for the defined purpose(s) and a study of the potentially applicable PETs for the concrete case[222].

The topic of PbD, besides being intimately connected with the implementation of the principles that related to personal data processing, in our opinion is also supporting the effectiveness of the rights of the data subjects (chapter III of GDPR) for example, the rights to rectification (art.16 GDPR) and erasure (art.17 GDPR), considering the IoT background, need to be implemented on a system level, or as mentioned above, privacy needs to be integrated in the systems.

If, by hypothesis, an IoT deployment (where personal data is being processed) is thought from scratch without considering how can personal data from a specific individual be deleted if required, when such a granular requirement arises, the solution will either pass (if possible) by a manual deletion of the data and notification to all the parties that hold personal data of that individual to proceed with the deletion, or if it is not possible to do so, or to proceed with customization in due time, it can dwell into a situation of non-compliance with the right to erasure.

Furthermore, differently from PbD (as it was initially conceived by Ann Cavoukian) according to the GDPR both, "data protection by design" and "data protection by default" are "legal obligations" (under the GDPR both are placed under Section 1 of Chapter IV, regarding "General Obligations", in addition, the wording itself clearly leaves no doubt that we are in the realm of "legal obligations": *"the controller shall (…)"*).

The PbD framework, as initially proposed, remains a valid reference since it can support compliance with various legal requirements (e.g. the Fair Information Practice Principles or in our case the GDPR) through the mapping of the original principles to those (in case of the GDPR, more stringent) legal requirements.

[219] Norwegian Consumer Council (Forbrukerrådet), op. cit.,17.

[220] Ibid, 18.

[221] Antonio Kung, Frank Kargl, Santiago Suppan, Jorge Cuellar, Henrich C. Pohls, Adam Kapovits, Nicolas Notario McDonnell and Yod Samuel Martin, "A Privacy Engineering Framework for the Internet of Things", in *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer, 2017), 176.

[222] Ibid, 175.

4.6. Data Protection Impact Assessments: A Common Requirement for the Internet of Things?

The topic of the DPIA appears regulated in the GDPR under art.35. The Regulation does not provide an exhaustive list of the processing activities that should be subject to a DPIA (nor it could, due to the vast diversity of processing activities that could require one)[223], nevertheless it provides relevant guidance criteria that points out in the direction of the necessity or dismissal of a potential DPIA.

The general rule to determine if a DPIA is required can be found in art.35 (1) GDPR, therefore when a type of processing (in particular, one that uses new technologies) is likely to result in a *high risk* for the rights and freedoms of natural persons, the data controller prior to the beginning of the processing activity, should perform an assessment of the impact of the envisaged processing operations on the protection of personal data (DPIA).

In art. 35 (3) a), b) and c) the EU legislator makes reference to the three main clusters where a DPIA "shall in particular be required". These are processing operations that are "likely to result in high risks", namely:

- The cases of automated processing, including profiling, that constitute a basis for decisions producing legal effects concerning the natural person - art. 35 (3) a);
- Large scale processing of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10 - art. 35 (3) b), or;
- A systematic monitoring of a publicly accessible area on a large scale - art. 35 (3) c);

Although IoT is not part of the three main clusters mentioned in art.35 (3), according to the criteria carved out by the WP29, to provide a "more concrete" set of processing activities that due to their high-risk require a DPIA (considering the elements of Articles 35 (1) and 35 (3) (a) to c)), IoT is in fact appering as part of the nine identified criteria that should delimit the list to be adopted at the national level under article 35(4) and recitals 71, 75 and 91.

Particularly relevant for the IoT, is the identified criteria of *innovative use or application of new technological or organizational solutions*[224]. The IoT is the WP29 chosen example to embody this criteria, being considered that certain IoT applications could produce a significant impact on individuals' daily lives and privacy, and therefore require a DPIA.

As mentioned, by the WP29 "certain" IoT applications could trigger the DPIA due to their potential impact for the individuals' privacy, so in principle, not all IoT applications would have to be subject to a DPIA. In our opinion, altough not all IoT applications might require a DPIA, this assessment will still be the rule or common requirement for IoT applications[225].

[223] In the same direction, Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high-risk" for the purposes of Regulation 2016/679 (WP248 rev.01), Brussels, 04 October 2017, 9.

[224] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high-risk" for the purposes of Regulation 2016/679 (WP248 rev.01), 10.

[225] Also the French data protection authority (CNIL), recognizing the relevance of IoT for the topic of DPIAs, published recently a privacy impact assessment document oriented towards IoT devices, the document is laid out

There is undoubtly a differentation in terms of the possible dangers for privacy when we compare the different IoT applications, for example an IoT enabled refrigerator that monitors the stock and validity dates of our products is probably less invasive for our privacy than a wearable computing device, such as a medical tracker (that collects health related information).

However, the category of the collected data is only a piece of the bigger puzzle that is a processing operation, and "by default" IoT devices are meant to collect large amounts of data of their surrounding environments.

Our previous example, of the smart meters used to measure the consumption of water, electricity and gas is a good demonstration that the category of the data that is collected is only a part of the puzzle.

These meters pursue an informative purpose of measurement, to promote efficiency in our energy, water and gas spending's, but they also reveal important details about our lives, they can reveal that in a given period we are is absent, allowing potential robbers to safely gain access to our house. The damage here can also be extended to our property, belongings or even physical integrity.

The ability of IoT devices to collect large amounts of data from their surroundings (which include us) turns them into a desirable target. This ability connected with the security vulnerabilities analysed above should be enough to justify the need for a DPIA for most of the cases, since the processing is likely to result in a *high risk* for the rights and freedoms of natural persons.

4.7. "Who is Who": Controllers, Processors, Suppliers and Integrators

In section 2.2 we approached the notion of data controller and data processor, according to the GDPR. The "controller", which in light of art. 4 (7) GDPR, is the one who defines "why" and "how" personal data is processed, and the "processor", which according art. 4 (8) GDPR, processes personal data on behalf of the controller.

The logic inherent to GDPR tends to place the majority of the weight and obligations on the data controller. The data processor (art.28 and 29 GDPR), although with a lesser burden also has its share of duties under the GDPR.

For example, the processor has to maintain a record of all categories of processing activities carried out on behalf of a controller (art.30 (2) GDPR), to notify the controller without undue delay after becoming aware of a personal data breach (art.33 (2) GDPR), or to implement appropriate TOMs to ensure a level of security appropriate to the risk (art.32 GDPR).

Despite these definitions, it is not always easy determining "who is who" in a complex landscape such as the IoT, where as previously pointed several stakeholders coexist and tend to interact (e.g. the device manufacturer might not be the one who developed the software, the data processed by the device could be stored in a cloud from a third party, social platforms, data brokers, among others).

like a DPIA report, which is the deliverable of a DPIA - Commission Nationale Informatique & Libertes (CNIL), "Privacy Impact Assessment (PIA) – Application to IoT Devices", February, 2018.

This difficulty in determining “who is who” in the controller/processor dynamic (to which other realities, such as “joint controllership” can be added – art.26 GDPR[226]) is not circumscribed to the IoT. To help clarify the role of the data controller and of the data processor, the WP29 drafted an opinion on the concepts of “controller” and “processor”. In this opinion, among several grey areas, the role of telecom operators is analysed, being clarified that:

- If there is a transmission of a message (which contains personal data), by means of a telecommunications or electronic mail service, the purpose will be the transmission of such messages;
- In this case, the data controller (concerning the personal data contained in the message), will normally be the person from whom the message originates, and not the person that offers the transmission services;
- However, the person offering the transmission services, will normally take the role of data controller, regarding the additional processing of personal data deemed necessary to offer the services (the provider of telecommunications services is usually, only a data controller in the cases of traffic and billing data)[227].

This example sheds some light on the role of those whose main purpose is to provide a service. In our landscape, this would usually be the case for example, of the cloud service provider, who should be considered as a data processor (except regarding the additional processing of personal data necessary to offer the service), therefore processing data on behalf of a given data controller[228].

The IoT stakeholder framework, is composed of several intervenients as discussed above, of which cloud service providers are (usually) just a component. The stakeholders of the IoT ecosystem, can be grouped in: data controllers, data processors, suppliers and integrators[229]. The first two have to comply with the legal obligations set forth in the EU legal framework, while the last two do not (at least it does not result explicitly from the legal framework, but it should be a part of the legal obligations stipulated in supply and procurement contracts, conducted between these parties and the data controllers and processors)[230].

The integrators are those, “*(…) in charge of providing turnkey systems by bringing together component subsystems into a whole and ensure that those subsystems function together”,* while the suppliers are those who “(*…) provide component subsystems which are then integrated*”[231].

Therefore, in the IoT framework the privacy and data protection related obligations of the suppliers of hardware components (e.g. microcontrollers, single board computers [232], among others) and integrators would be regulated by means of a contract.

[226] Art. 26 (1) GDPR, clarifies that we have a joint controllership when two or more controllers jointly determine the purposes and means of processing.

[227] Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of “Controller” and “Processor” (WP169), Brussels, 16 February 2010, 11.

[228] On the same direction, although focused on the EU institutions and bodies, EDPS, “Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies”, Brussels, 16 March, 2018, 7.

[229] Kung, Kargl, Suppan, Cuellar, Pohls, Kapovits, McDonnell and Martin, op. cit., 165-169.

[230] Ibid. The authors argue that suppliers and integrators must include privacy engineering in their practice. Considering also that privacy engineering for suppliers has to be approached in a different manner, when compared with privacy engineering for data controllers, processors and integrators, since the suppliers as opposed to the other stakeholders groups, cannot be aware of the purposes for which data is collected.

[231] Ibid.

As for the device manufacturers, most of them usually qualify as data controllers, due to the fact that in most cases they do more than sell the physical device, they might have also "(…) *modified the "thing's" operating system or installed software determining its overall functionality*"[233], therefore collecting and processing personal data according to purposes and means they have determined.

The social platforms, are also usually considered as data controllers, since they automatically share aggregated data originated from the device, once the user has configurated this option in the standard default settings.

> *As this data is pushed by the user onto them, when it is processed by social networks for distinct purposes which they have determined themselves they then qualify as data controllers in their own right under EU law[234].*

Finally, the person who makes use of the IoT device (as mentioned previously, not only the owner of the device is in scope (or, is protected), also those who make use of the device are protected), qualifies as a data subject, according to the EU legal framework[235].

This "classification" of IoT stakeholders, according to their group (data controllers, data processors, suppliers and integrators) and to their role (e.g. device manufacturer, cloud service provider, social platforms) does not aim to be exhaustive, nor could it since each situation requires a case-by-case analysis, but merely to contribute to the topic by approaching the most common issues and difficulties.

5. Conclusions

As we explored in the course of our research, IoT is gradually taking its role as one of the "engines", powering the 4th Industrial Revolution (perhaps, not to a rhythm high enough to match the highest of expectations or the most optimistic forecasts).

However, IoT is undoubtedly, paving the way to make our connected world smarter, more efficient and sustainable, with solutions to improve cities (e.g. smart roads, smart parking, waste

[232]Anna Gerber, "Choosing the Best Hardware for Your Next IoT Project", (May 2017), https://www.ibm.com/developerworks/library/iot-lp101-best-hardware-devices-iot-project/index.html (accessed 22 July 2018), describes the role and functionality of the microcontrollers and single board computers: "A *microcontroller* is a SoC that provides data processing and storage capabilities. Microcontrollers contain a processor core (or cores), memory (RAM), and *erasable programmable read-only memory* (EPROM) for storing the custom programs that run on the microcontroller", while single board computers are "a step up from microcontrollers, because they allow you to attach peripheral devices like keyboards, mice, and screens, as well as offering more memory and processing power".

[233] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223), 11.

[234] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223), 12.

[235] In the same direction, Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223), 12, clarifying also that: "The processing of data in the IoT may also concern individuals who are neither subscribers nor actual users of the IoT. For instance, wearable devices like smart glasses are likely to collect data about other data subjects than the owner of the device. It is important to stress that this factor does not preclude EU law from applying to such situations. The application of EU data protection rules is not conditioned by the ownership of a device or terminal but by the processing of the personal data itself, whoever the individual concerned by this data is."

management), environmental sustainability (e.g. forest fire detection, air pollution, smart water solutions, such as river floods, chemical leakage detection in rivers), and our consumption habits (e.g. smart metering solutions, such as the smart grid), among several other innovations.

The potential of the IoT did not go unnoticed to the EU, that has created a European strategy for the IoT, from which we can derive the role that IoT is planned to have in the future of Europe's digitization (namely, in the implementation of the Digital Single Market).

Despite all the advantages and immense possibilities, present and future (e.g. the example of IoRT, which is considered to be the *next phase* in the development of IoT applications, combining AI, robotics, machine learning algorithms, and swarm technologies), the IoT is not trouble-free.

In fact, there are several privacy and data protection threats in the IoT that we clustered as below:

- The problem of identification and (partially) also the problem of localization and tracking in the IoT (as presented) – those problems can be directed to the threat of processing personal data without a valid legal ground and/or in disrespect of the individuals rights;
- All types of possible attacks (not just inventory attacks) that exploit IoT vulnerabilities and grant undue access to personal data of the users are a threat to privacy and personal data protection;
- The multiplicity of users that can share the same IoT devices;
- IoRT, and the discussions over the statute given to more sophisticated robots is a legal challenge for the IoT.

Apart from the privacy and data protection threats, also several security issues arise having the IoT as a background. There are typical vulnerabilities that can affect IoT, and those are important when addressing security concerns, since it is through them that an attacker can find an open door to compromise the device, and eventually access personal data.

Both realities (privacy and data protection threats and security issues) are intertwined, in fact it is common, that from a flaw in security, adverse consequences are felt by the user/data subject, if personal data is being processed.

We concluded, that in IoT a multi-layered security approach should be adopted, covering the following topics:

- Secure device (hardware);
- Secure communications;
- Secure cloud;
- Secure lifecycle management.

In line with the above (but, approaching the topic from the point of view of IoT's own singularities that we discussed previously), we observe that these singularities, in turn, may represent risks (to be mitigated or eliminated) for the data subjects/end-users.

These singularities that may bring risks for the rights and freedoms of the data subjects/end-users, have their root in IoT's connectivity (inherent predisposition for a contact and reception of information from the outside world at a very intense pace), that in turn, is oriented towards the collection of large amounts of data, which in the vast majority of situations, constitutes "personal data".

The new EU legal framework, the GDPR and the ePrivacy Proposal, aims to provide a robust and harmonized EU data protection regime, based on common standards, and able to provide the same data protection rights across the EU member States.

With our research, connecting the topics of IoT, privacy and personal data protection in the EU, we aimed to provide our contribution, towards the goal of understanding and addressing the potential effects of the identified risks that the IoT technology represents (or is foreseen to represent) for the protection of personal data and privacy, and ultimately for the data subjects/end-users.

In order to do so, we looked for the answers for two central and overall questions that were always addressed within the context of the IoT, namely:

- How (applicable regulations, legal basis for processing, legal requirements to consider; among others), and;
- Where (in which situations) is the new European legal framework regarding the protection of personal data and privacy applicable to the IoT.

In the course of our research we answered these questions to the full and possible extent, while having also built an adequate technical background to place the "IoT" topic into perspective. In turn, this approach provided a comprehensive overview of the status quo of personal data protection and privacy in Europe, when IoT is in the background.

Summarizing, to the full possible extent the answer to the first question (or questions), and not repeating obvious topics, duly mentioned so far (e.g. the applicable regulations), we can state that:

- The ePrivacy Proposal constitutes *lex specialis* in regards to the GDPR, complementing it in the cases that ECD qualifies as personal data (this means, according to point 1.2. of the Explanatory Memorandum of the proposal, that all the issues concerning the processing of personal data that are not specifically addressed by the ePrivacy Proposal are covered by the GDPR);
- Whenever we fall outside the restricted scope provided by the EU legislator that requires the exclusive applicability of the ePrivacy Proposal (rec.5 of the ePrivacy Proposal), and only then, it is possible to consider the legal grounds of the GDPR;
- Even on the above situation, it should be noticed that there is only a relevance for our topic if the second cumulative condition is not present (meaning: *the electronic service providers are not qualified as data controllers for that particular processing*), since the first condition must be present for the GDPR to be applicable - the data has to be personal data;
- Therefore, if we conclude, that the ECD that is being processed, does not qualified as personal data, the GDPR is not applicable;
- From the legal grounds present in the GDPR those that can be applied to the IoT context, are in practice three, namely: consent, performance of a contract, and legitimate interests, pursued by the controller or a third party;
- From those legal grounds, consent, is held to be the first and most reliable legal ground to be applied to the IoT landscape by the several stakeholders involved (e.g. device manufacturers, social or data platforms, device lenders or third party developers);

- The specific legal requirements to consider, apart from the ones that apply to all data controllers or data processors, can be grouped into the following main requirements: DPIA, PbD, compliance with the data protection principles, in particular due to IoT's ability to collect large amounts of data, with the data minimization principle (furthermore, as mentioned in section 3.2, there are also other non-legal requirements supporting the goal of protecting the user's privacy and personal data to consider, for example, the use of cryptographic techniques);
- These legal requirements stemming from the GDPR, are not tailored specifically for the IoT, and they apply to a variety of processing's involving personal data. However, due to their relevance and frequent applicability to the IoT, they find themselves in a position that allows their individualization from the remaining legal requirements.

Summarizing, the answer to the second question:

- The ePrivacy Proposal, is always applicable to the IoT (provided its scope of application is fulfilled), regardless the fact that personal data is being processed or not;
- GDPR, is applicable whenever personal data is processed (and the material and territorial scope of application is fulfilled);
- As stated above, the ePrivacy Proposal constitutes *lex specialis* in regards to the GDPR, complementing it in the cases that ECD qualifies as personal data. Therefore, this relationship model between both regulations, should be in the background when determining the applicability of the legal framework;
- The ePrivacy Proposal (*lex specialis*) may *particularize* or *complement* the GDPR;
- When the ePrivacy Proposal particularizes the general rules of GDPR, there is an underlying conflict between the rules of both regulations that cover the same topic on a distinct manner;
- When the ePrivacy Proposal complements the general rules of GDPR, there is no underlying conflict of rules, merely an additional rule that is to be applied.

While some minor aspects we addressed in the course of our research may change when the ePrivacy Regulation enters into force (for example, if the EU legislator takes into account some of the remarks made by both, the EDPS and the Article 29 Data Protection Working Party, concerning the topic of the end-user), the overall research and the conclusions that follow, maintain its full applicability.

References

Akimana, Béni-Tresor, Bonnaerens, Maxim, Van Wilder, Jonas, and Vuylsteker, Bjorn. “A Survey of Human-Robot Interaction in the Internet of Things”. December 2016, https://www.researchgate.net/publication/318722691_A_Survey_of_HumanRobot_Interaction_in_the_Internet_of_Things (accessed 24 February 2018).

Aleisa, Noura, Renaud, Karen. “Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion)”. Cornell University Library. September 2016. https://arxiv.org/abs/1611.03340 (accessed 05 May 2018).

Andress, Jason. The Basics of Information Security – Understanding the Fundamentals of InfoSec in Theory and Practice. Elsevier, 2011.

Ashton, Kevin. “That “Internet of Things” Thing”, in RFID Journal. June 2009. http://www.rfidjournal.com (accessed 21 April 2018).

Azurmendi, Ana. “Spain: The Right to be Forgotten”, in Privacy, Data Protection and Cybersecurity in Europe. Springer, 2017.

Article 29 Data Protection Working Party. Opinion 1/2010 on the Concepts of “Controller” and “Processor” (WP169). Brussels, 16 February 2010.

- Opinion 02/2013 on Apps on Smart Devices (WP202). Brussels, 27 February 2013.

- Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223). Brussels, 16 September 2014.

- Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (WP247). Brussels, 04 April 2017.

- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high-risk” for the purposes of Regulation 2016/679 (WP248 rev.01). Brussels, 04 October 2017.

Ballano Barcena, Mario, Wueest, Candid. ”Insecurity in the Internet of Things”. Symantec. March 2015. https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things-en.pdf (accessed 29 April 2018).

Bellotti, Victoria. “Design for Privacy in Multimedia Computing and Communications Environments”, in Technology and Privacy: The New Landscape. Cambridge/US: MIT Press, 1997.

Bilal, Muhammad. ”A Review of the Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D Printers”. Cornell University Library. June 2017. https://arxiv.org/abs/1708.04560 (accessed 29 April 2018).

Bulman, May. ”EU to Vote on Declaring Robots to Be “Electronic Persons””. Independent. January 2017. https://www.independent.co.uk/life-style/gadgets-and-tech/robots-eu-vote-electronic-persons-european-union-ai-artificial-intelligence-a7527106.html (accessed 25 April 2018).

Campbell, Peter. ” Driverless vehicles – Hackers have self-driving cars in their headlights”. Financial Times. March 2018. https://www.ft.com/content/6000981a-1e03-11e8-aaca-4574d7dabfb6 (accessed 28 April 2018).

CASAGRAS. Final Report. “RFID and the Inclusive Model for the Internet of Things”. EU Project Number 216803, 2009.

Castells, Manuel. The Power of Identity. The Information Age: Economy, Society, and Culture, Volume 2. Wiley-Blackwell, 2010.

Cavoukian, Ann. “Privacy by Design: Leadership, Methods, and Results”, in European Data Protection: Coming of Age. Springer, 2013.

Cavoukian, Ann, Popa, Claudiu. “Embedding Privacy Into What’s Next: Privacy by Design for the Internet of Things”. Ryerson University – Privacy & Big Data Institute, April 2016.

Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008).

Commission Nationale Informatique & Libertes (CNIL). “Privacy Impact Assessment (PIA) – Application to IoT Devices”. February, 2018.

Committee on National Security Systems. Committee on National Security Systems Glossary (CNSS). April 2015, 64 https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf (accessed 28 April 2018).

Communication from the Commission to the Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Radio Frequency Identification (RFID) in Europe: steps towards a policy framework. COM (2007) 96 final. Brussels, 15 March 2007.

- Internet of things – An action plan for Europe.COM (2009) 278 final. Brussels, 18 June 2009.

- A Digital Single Market Strategy for Europe. SWD (2015) 100 final. Brussels, 6 May 2015.

- Digitising European Industry – Reaping the full benefits of a Digital Single Market. SWD (2016) 110 final. Brussels, 19 April 2016.

Cuijpers, Colette, Koops, Bert-Jaap. "Smart Metering and Privacy in Europe: Lessons from the Dutch Case", in European Data Protection: Coming of Age. Springer, 2013.

Davis, Euan. "The Rise of the Smart Product Economy". Cognizant. May 2015. https://www.cognizant.com/InsightsWhitepapers/the-rise-of-the-smart-product-economy-codex1249.pdf (accessed 05 May 2018).

Directorate General for Internal Policies – Policy Department A: Economic and Scientific Policy, Mapping Smart Cities in the EU, European Union, 2014.

E. Agre, Philip. Technology and Privacy: The New Landscape. Cambridge/US: MIT Press, 1997.

EDPS. Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation). Brussels, 24 April 2017.

- "Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies". Brussels, 16 March, 2018.

Edson, Barb. "Azure IoT Technology helps NAV CANADA revolutionize air-traffic control". Microsoft Internet of Things. March 2016. https://blogs.microsoft.com/iot/2016/03/17/azure-iot-technology-helps-nav-canada-revolutionize-air-traffic-control/#JvuzE3WFYvjuqU6h.99 (accessed 28 April 2018).

E. Wright, Erin. "The Right to Privacy in Electronic Communications: Current Fourth Amendment and Statutory Protection in the Wake of Warshak v. United States", in I/S: A Journal for Law and Policy for the IS, 2007. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Wright.pdf (accessed 14 April 2018).

G. Boyce, Joseph, W. Jennings, Dan. Information Assurance – Managing Organizational IT Security Risks. Butterworth-Heineman, 2002.

Gerber, Anna. "Choosing the Best Hardware for Your Next IoT Project". May 2017. https://www.ibm.com/developerworks/library/iot-lp101-best-hardware-devices-iot-project/index.html (accessed 22 July 2018).

Gilchrist, Alasdair. IoT Security Issues. Walter de Gruyter Inc., Boston/Berlin, 2017.

H. Flaherty, David. “Controlling Surveillance: Can Privacy Protection Be Made Effective?” in Technology and Privacy: The New Landscape. Cambridge/US: MIT Press, 1997.

Hatton, Celia. ”China “social credit”: Beijing sets up huge system. October 2015. http://www.bbc.com/news/world-asia-china-34592186 (accessed 28 January 2018).

Helberger, Natali. “Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law”, in Digital Revolution: Challenges for Contract Law in Practice. Nomos, 2016.

Huertas Celdran, Alberto, Manuel Gil Perez, Manuel, Garcia Clemente, Felix, Martinez Perez, Gregorio. “Precise: Privacy-aware Recommender Based on Context Information for Cloud Service Environments”, in IEEE Communications Magazine. IEEE, 2014.

Hung, Mark. “Leading the IoT – Gartner Insights on How to Lead in a Connected World”. Gartner. 2017. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf (accessed 25 April 2018).

J. Solove, Daniel, Rotenberg, Marc, M. Schwartz, Paul. Privacy, Information and Technology. ASPEN PUBLISHERS, 2006.

Jeyanthi, N. “Internet of Things (IoT) as Interconnection of Threats (IoT)”, in Security and Privacy Internet of Things (IoTs) – Models, Algorithms, and Implementations. Taylor & Francis Group, LLC, 2016.

Julia Hilberg, Sontje. ” EU General Data Protection Regulation – What remains? What changes?” Deloitte. https://www2.deloitte.com/dl/en/pages/legal/articles/eu-datenschutzgrundverordnung.html (accessed 17 February 2018).

K. Mulligan, Deirdre. “Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act”, in The George Washington Law Review, 2004, 1590. http://scholarship.law.berkeley.edu/facpubs/2131/ (accessed 15 April 2018).

Karaboga, Murat, Matzner, Tobias, Obersteller, Hannah, Ochs, Carsten. “Is There a Right to Offline Alternatives in a Digital World”, in Data Protection and Privacy: (In)visibilities and Infrastructures. Springer, 2017.

Kobie, Nicole. “What is the internet of things?”. The Guardian. May 2015. https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google (accessed 21 April 2018).

Kung, Antonio, Kargl, Frank, Suppan, Santiago, Cuellar, Jorge, C. Pohls, Henrich, Kapovits, Adam, Notario McDonnell, Nicolas and Samuel Martin, Yod. "A Privacy Engineering Framework for the Internet of Things", in Data Protection and Privacy: (In)visibilities and Infrastructures. Springer, 2017.

L. Bellia, Patricia. "The Fourth Amendment and Emerging Communications Technologies", in IEEE SEC. & PRIVACY, 2006. http://ieeexplore.ieee.org/document/1637377/ (accessed 15 April 2018).

- "Surveillance Law Through Cyberlaw's Lens", in The George Washington Law Review, 2004, 1385 – 1386. http://scholarship.law.nd.edu/law_faculty_scholarship/766 (accessed 15 April 2018).

Liton, Melissa, "How much data comes from the Internet of Things?" (February, 2018), https://www.sumologic.com/blog/machine-data-analytics/iot-devices-data-volume/ (accessed 26 June 2018).

Lock, Tobias. The European Court of Justice and International Courts. Oxford University Press, 2015.

Madakam, Somayya, Date, Hema. "Security Mechanisms for Connectivity of Smart Devices in the Internet of Things", in Connectivity Frameworks for Smart Devices – Computer Communications and Networks. Springer, 2016.

Manyika, James, Chui, Michael, Bisson, Peter, Woetzel, Jonathan, Dobbs, Richard, Bughin, Jacques, Aharon, Dan. "The Internet of Things: Mapping the Value Beyond the Hype". McKinsey Global Institute.June2015.http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world (accessed 25 April 2018).

Mayer-Schönberger, Viktor. "Generational Development of Data Protection in Europe", in Technology and Privacy: The New Landscape. Cambridge/US: MIT Press, 1997.

Mayzaud, Anthéa, Badonnel, Rémi, Chrisment, Isabelle. "A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks", in Network and Service Management IEEE Transactions. IEEE, 2017.

McEwen, Adrien, Cassimally, Hakim. Designing the Internet of Things. Wiley, 2014.

Mendez, Diego, Papapanagiotou, Ioannis, Yang, Baijian. " Internet of Things: Survey on Security and Privacy". Cornell University Library. July 2017. https://arxiv.org/abs/1707.01879 (accessed 29 April 2018).

Meola, Andrew. ”How IoT and smart home automation will change the way we live”. Business Insider. December 2016. http://www.businessinsider.com/internet-of-things-smart-home-automation-2016-8 (accessed 25 April 2018).

Moorhead, Patrick. ”The Problem With Home Automation’s Internet of Things (IoT)”. Forbes. September 2013, https://www.forbes.com/sites/patrickmoorhead/2013/09/26/the-problem-with-home-automations iot/#217da6da70ec (accessed 25 April 2018).

Norwegian Consumer Council (Forbrukerrådet). ”Deceived by Design – How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy”. Forbrukerrådet. June 2018, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/ (accessed 05 July 2018).

O´Brien, Dick.” Internet Security Threat Report, ISTR Ransomware 2017 – An ISTR Special Report”. Symantec Corporation. July 2017. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf (accessed 29 October 2017).

Orrù, Elisa. “Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance”, in Data Protection and Privacy: (In)visibilities and Infrastructures. Springer, 2017.

Orwell, George. Nineteen Eighty-Four. Penguin Books, 2003.

Paar, Christof, Pelzl, Jan. Understanding Cryptography – A Textbook for Students and Practitioners. Springer, 2010.

Pagallo, Ugo, Durante, Massimo, Monteleone, Shara. “What is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT”, in Data Protection and Privacy: (In)visibilities and Infrastructures. Springer, 2017.

Prensky, Marc. “Digital Natives, Digital Immigrants Part 1”, in On the Horizon, Vol. 9 Issue: 5, doi: 10.1108/10748120110424816.

Proposal for a Directive of the European Parliament and of the Council, establishing the European Electronic Communications Code (Recast), COM (2016) 590 final/2, Brussels, 12 October 2016.

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) 10 final. Brussels, 10 January 2017.

Rodrigues Viana, Vítor. IDN Nação e Defesa, 133. Instituto da Defesa Nacional, 2012.

Rose, Karen, Eldridge, Scott, Chapin, Lyman. “The Internet of Things: An Overview – Understanding the Issues and Challenges of a More Connected World”, in Internet Society (October 2015). http://www.internetsociety.org (accessed 21 April 2018).

Ryerson University – Privacy by Design Centre of Excellence. ”Dr. Ann Cavoukian, Distinguished Expert in Residence”. https://www.ryerson.ca/pbdce/about/ann-cavoukian/ (accessed 05 July 2018).

S. Reverson, Derek. Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World. Georgetown University Press, 2012.

Schneier, Bruce. *“*Security and the Internet of Things*”*, in Schneier on Security (February 2017). https://www.schneier.com/blog/archives/2017/02/security_and_th.html (accessed 22 April 2018).

Schwab, Klaus. The Fourth Industrial Revolution. Portfolio Penguin, 2017.

Scully*,* Padraig.*”*Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers”.IoT Analytics GmbH. November 2016. https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/ (accessed 29 April 2018).

- ”5 Things to Know About IoT Security”. IoT Analytics GmbH. November 2017. https://iot-analytics.com/5-things-to-know-about-iot-security/ (accessed 29 April 2018).

Shrivastava, Gulshan, Kumar, Prabhat, Gupta, B. B., Bala, Suman, Dey, Nilanjan. Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, 2018.

Symantec DeepSight Adversary Intelligence Team*.* ”The Fourth Industrial Revolution – Opportunities and Challenges with the Internet of Things (IoT) and Why You Need Threat Intelligence”, Symantec Corporation. April 2018. https://www.symantec.com/blogs/expert-perspectives/fourth-industrial-revolution (accessed 28 April 2018).

Singh, Jatinder, Pasquier, Thomas, Bacon, Jean, Ko, Hajoon, Eyers, David. “Twenty Security Considerations for Cloud-supported Internet of Things”, in IEEE Internet of Things Journal*.* IEEE, 2016.

Solove, Daniel. The Digital Person – Technology and Privacy in the Information Age. New York University, 2004.

Sousa Pinheiro, Alexandre. Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional. AAFDL, 2015.

Spiser, Michael. Introduction to the Theory of Computation. Cengage Learning, 2013.

Suo, H., Wan, J., Zou, C., Liu, J. "Security in the Internet of Things: a Review", in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference. ICCSEE, 2012.

T. Tavani, Herman. Ethics and Technology – Controversies, Questions, and Strategies for Ethical Computing. John Wiley & Sons, Inc., 2011.

Tiainen, Minna. "Solving the Surveillance Problem: Media Debates About Unwanted Surveillance in Finland", in Privacy, Data Protection and Cybersecurity in Europe. Springer, 2016.

Van der Sloot, Bart. "Legal Fundamentalism: Is Data Protection Really a Fundamental Right?" in Data Protection and Privacy: (In)visibilities and Infrastructures. Springer, 2017.

Vermesan, Ovidiu, Friess, Peter. Internet of Things – From Research and Innovation to Market Deployment. River Publishers, 2014.

Vermesan, Ovidiu, Broring, Arne, Tragos, Elias, Serrano, Martin, Bacciu, Davide, Chessa, Stefano, Gallicchio, Claudio, Micheli, Alessio, Dragone, Mauro, Saffiotti, Alessandro, Simoens, Pieter, Cavallo, Filippo and Bahr, Roy. "Internet of Robotic Things – Converging Sensing/Actuating, Hyperconnectivity, Artificial Intelligence and IoT Platforms", in Cognitive Hyperconnected Digital Transformation - Internet of Things Intelligence Evolution. River Publishers, 2017.

Voigt, Paul, von dem Bussche, Axel. The EU General Data Protection Regulation (GDPR) - A Practical Guide. Springer, 2017.

Whitman, Michael, Mattord, Herbert. Principles of Information Security. Course Technology Cengage Learning, 2011.

Zanfir-Fortuna, Gabriela." Will the ePrivacy Reg overshadow GDPR in the age of IoT?" February 2017). https://iapp.org/news/a/will-the-eprivacy-reg-overshadow-the-gdpr-in-the-age-of-iot/ (accessed 13 May 2018).

Zhao, K., Ge, L. "A Survey on the Internet of Things Security", in Computational Intelligence and Security (CIS), 2013 9th International Conference. IEEE, 2013.

Ziegeldorf, Jan Henrik, Garcia Morchon, Oscar, Wehrle, Klaus. "Privacy in the internet of things: threats and challenges", in Secur. Commun. Netw. 7(12), 2014.

Cases

Griswold v. Connecticut, 381 U.S.479 (1965).

Katz v. United States, 389 U.S.347 (1967).

Case 43/71 Politi s.a.s. v Ministry for Finance of the Italian Republic (1971) ECR 1039.

United States v. Miller, 425 U.S. 435 (1976).

Oliver v. United States, 466 U.S. 170, 178 (1984).

United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996)

USA v. Steven Warshak, No. 08-4085 (6th Cir.2010).

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 (13 May 2014).