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

Liliana Pereira Martins dos Santos

Summary: 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

Introduction

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 Internet of Things is considered to be the engine that is powering the 4th Industrial Revolution and is also, a challenge when it comes to personal data protection and privacy. 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.

The scope and extent of the protection granted to personal data and privacy by the new European legal framework, that for our purposes can be translated into knowing "how" (applicable regulations, legal basis for processing, legal requirements to consider, among others) and "where" (in which situations) 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.

While 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.

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 29ePrivacy Proposal), the entry into force of the future ePrivacy Regulation was delayed, therefore we will refer to the ePrivacy Proposal.

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

a) An Overview of the European Strategy for the Internet of Things

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.

---

[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.

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[5]. The first effort on this direction was COM (2007) 96 final, which had a focus on Radio Frequency Identification (RFID)[6], and already there we could see a reflex of the concerns that were risen with the matters of data security and data privacy.

On a later phase, the Commission published COM (2009) 278 final[7], contemplating an action plan for Europe concerning the IoT[8]. 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'"[9].

More recently, the Commission launched SWD (2015) 100 final, a DSM Strategy for Europe[10].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 paper also refers to the necessity of exploring innovations such as Cloud computing, Big Data tools and the IoT, considering them central to EU's competitiveness[11]. 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"[12], 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"[13].

b) 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 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.

---

[5]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), 48-49.

[6]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 microchip – 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".

[7]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.

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

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

[10]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.

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

[12]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.

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

In order to do so, we have identified two primary questions that should be answered to place both regulations into perspective, namely: what is the scope of both regulations and what are the contact points between both regulations?

Starting with our first question, aimed at understanding the scope of both regulations, 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, the 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*[14]*.*

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"[15]. 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.

The territorial scope is regulated in art. 3. 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.

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"*. Regarding the territorial scope, defined in art.3 of the ePrivacy Proposal, the regulation is to be 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).

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). 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[16].

---

[14] 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.

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

[16] 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.

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 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"*).

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

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.

The ePrivacy Proposal, is focused on protecting the right to respect for private life. The fundamental right to respect for private life is laid down in art. 7 of the Charter which 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). 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*. 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.

d) 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 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* [17].

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 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.

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[18];

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

[18] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223), 4. This conclusion is also supported by the Article 29 Data Protection Working Party, "IoT stakeholders aim

- 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, among others)[19];

-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.

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[20].

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

The IoT architecture layers, namely: application layer, network layer and perception layer are susceptible to several types of attacks that can compromise the security of IoT user's. The various possible attacks, vary according to the different architectural layers.

Therefore, a multi-layered security approach is required, taking also into consideration lifecycle issues: secure device (hardware); secure communications; secure cloud and secure lifecycle management. 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[21] of IoT, where potentially attacks[22] 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).

In our opinion, a good level of security in IoT can be achieved, considering: security on an organizational level, awareness from the IoT user, and a multi-layered security approach, considering the

---

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".

[19] Ibid.

[20] 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.

[21] As mentioned by Michael Whitman, Herbert Mattord, *Principles of Information Security*, (Course Technology Cengage Learning, 2011), 11, vulnerability is a weakness or failure in a system or protection mechanism that makes it permeable to attack or damage.

[22] 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.

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).

Privacy and Data Protection Challenges in the IoT

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[23]. 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. 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)[24].

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. 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[25], compliance with this principle also requires that the controller only retain 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.

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

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

[23] 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).

[24] 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.

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

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[26]), 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[27]. 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[28].*

Lawful grounds for processing in the IoT

When 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, if we come under the conclusion that the ECD that is being processed, does not qualified as personal data, the GDPR is not be part of the equation.

In practice, there are three relevant legal grounds in the GDPR that can be applied to the IoT context[29]:

- 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[30]);
- 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 theArticle 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*"[31].
- 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).

Applying the Principles Related to Personal Data Processing to the Internet of Things

The 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* "t*aken together, the principles enshrined in Article 6 of Directive 95/46/EC constitute a cornerstone of EU data protection law[32]".*

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, namely:

---

[26]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".

[27]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).

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

[29]Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, 14.

[30]Ibid.

[31]Ibid.

[32]Ibid, 16.

lawfulness, fairness and transparency - art.5 (1) a) GDPR; purpose limitation – art.5 (1) b) GDPR; data minimization– art.5 (1) c) GDPR; accuracy – art.5 (1) d) GDPR; storage limitation – art.5 (1) e) GDPR; integrity and confidentiality – art.5 (1) f) GDPR and accountability – art.5 (2) GDPR.

IoT products need to consider these principles in an early stage, especially when implementing privacy by design and privacy by default concerns. 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 referred 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.

Data Protection by Design and by Default: Engineering Privacy in the Internet of Things

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.

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), at least some of them (those who need to be insured on a system and/or device level).

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.

Data Protection Impact Assessments: A Common Requirement for the Internet of Things?

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 refers to the three main clusters where a DPIA “shall in particular be required”. 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 appearing 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*[33]. 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 theWP29 “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

[33]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.

DPIA. In our opinion, although not all IoT applications might require a DPIA, this assessment will still be the rule or common requirement for IoT applications[34].

"Who is Who": Controllers, Processors, Suppliers and Integrators

The stakeholders of the IoT ecosystem can be grouped in: data controllers, data processors, suppliers and integrators[35]. 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)[36].

The cloud service provider, 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[37].

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*"[38]. Therefore, in the IoT framework the privacy and data protection related obligations of the suppliers of hardware components (i.e. microcontrollers, single board computers[39], among others) and integrators would be regulated by means of a contract.

As for the device manufacturers, most of them usually qualify as data controllers, because 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*"[40], 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.

---

[34]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 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.

[35]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), 165-169.

[36]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.

[37]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.

[38]Ibid.

[39]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".

[40]Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223), 11.

Conclusions

In our research, 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.

Summarizing, to the full possible extent the answer to the first question (or questions):

- 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 two main requirements: DPIA, PbD;
- 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.