Global Campus Europe

University of Seville

European Master's Programme in Human Rights and Democratisation
A.Y. 2019/2020

The rise and consecration of the right to personal data protection within the European Union legal order

`

Author: Marvin THOMAR

Co-supervisors: Marta Bordignon
Angelica Bonfanti

Abstract

While we entrust our personal data to 'information and communications technology' (ICT) companies, the General Data Protection Regulation (GDPR) gives data subjects the possibility to control the dissemination of their personal data, in particular by requiring the ICT sector, to be more transparent regarding the processing of personal data. Moreover, with the influence of the European Convention on Human right (ECHR), the jurisprudence of the European Court of Justice (ECJ), the European Charter of Fundamental Rights and the adoption of the UN Guidelines Principles (UNGP), which came into force in 2011, the European Union gained sufficient legal backgrounds to develop a binding instrument which, in theory serves as a reference in the field of Data Protection. Yet, many factors hinder the proper implementation of this European instrument. Some are related to inconsistencies between EU Member States that have framed the right to protection of personal data within their domestic legal order, sometimes in different ways. Other are linked to the implementation of the principle of Transparency, which in many aspects is only partially respected by companies. Similarly, in some cases it is difficult for data subjects to enjoy the exercise of his or her rights notably due to the behavioral of companies, which will be discussed later in the thesis.

Global Campus Europe

Table of contents

Introduction

« When you say I don't care about the right to privacy because I have nothing to hide, that is no difference than saying 'I don't care about freedom of speech because I have nothing to say' or freedom of the press because I have nothing to write'. » Edward Snowden.

Nowadays, privacy is closely related to the personal data entrusted by users/customers to the 'Information and Communication Technology '(hereinafter 'ICT') corporations. Consequently, one of the negative effects of ICT corporations on Human Rights concerns the harvesting and the processing of personal data by ICT companies such as Amazon, Netflix, or Spotify. Indeed, after the collection stage, users have little insight and control over their own personal data. This possibility of ICT companies to breach human rights deserves to be examined in the light of the international legal framework on Business and Human Rights. Thus, in order to reduce the negative impact that such ICT corporations could have regarding Human Rights, in 2011, the Human Rights Council unanimously endorsed the UN Guiding Principles on Business and Human Rights (hereinafter 'UNGP'). It is aimed to help ICT companies to respect human rights into their own systems and cultures. In order to do so, ICT corporations must follow the guideline sets out by the UN Guideline Principles on Business and Human Rights, in particular, the one relating to the second pillar ''*the corporate responsibility to respect human rights* [1] ''. It means that ICT corporations'' *should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved''*[2]. In other words, addressing adverse human rights impacts requires taking adequate measures for their prevention, mitigation and, where appropriate, remediation. Moreover, some authors[3] argue that the recommendations enshrined by the UNGPs should be coordinated with the EU General Data Protection Regulation (hereinafter 'GDPR'), the European Court of Human Rights legal framework (hereinafter ECHR) and the Court of Justice of the European Union (hereinafter 'CJEU'). Thus, in order to meet their responsibility to respect human rights, business enterprises should have in place policies and

[1] UNGP 2011, s art 11-25

[2] UNGP 2011, s art 11

[3] Angelica Bonfanti, 'Introduction ICT Companies' Responsibility to Respect Human Rights : Remarks in the light of the EU General Data Protection Regulation' in Angelica Bonfanti (eds), Business *and Human Rights in Europe: International Law Challenges (Routledge 2018)*

processes appropriate to their size and circumstances, including: ''*(a) A policy commitment to meet their responsibility to respect human rights; (b) A human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights; (c) Processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute''*.[4]

Following the UNGPS, the European Commission adopted the ICT Sector Guide on implementing the UN Guiding Principles on Business and Human rights in 2011. It aimed to responsible ICT companies that have become increasingly active in recent years by affecting the enjoyment of human rights notably, through the misuse of the personal data from users. ICT sector is best described as a complex "ecosystem", with actors ranging from telecommunications services providers to large equipment manufacturers to small software or Web-based start-ups. In other words, it includes corporations that ''*provide telecommunication services/platforms for search, social networking, cloud computing and other web services, as well as device and component manufacturers*[5]''. ICT sector recognizes that it can both positively and negatively impact their staff, workers in their supply chain, customers, users or the communities around their operations.[6] Thus, in order to afford the maximum protection regarding the right to privacy and the processing of the personal data, the second pillar of the UNGPs, need to be coordinated with the GDPR and the ECHR[7] legal framework and the CJEU jurisprudence.

European Union has adopted a legally binding framework regarding online privacy, namely the General Data Protection Regulation (hereinafter 'GDPR'), which has been enforced on the 25 May 2018. The major update within the GDPR is that the processing of any EU citizens' information is now protected, regardless of whether the information processing is done within the EU or not, and regardless of where the retailer originates from. Any retailer around the globe that sells to an EU citizen is bound by law to protect private data. According to the article 4 of GDPR, 'personal data' means: «*any information*

[4] UNGP2011, s art 15

[5] Angelica Bonfanti, 'Introduction ICT Companies' Responsibility to Respect Human Rights : Remarks in the light of the EU General Data Protection Regulation' in Angelica Bonfanti (eds), Business *and Human Rights in Europe : International Law Challenges (Routledge 2018)*

[6] HRB and SHIFT, *ICT Sector Guide on implementing the UN Guiding Principles on Business and Human rights* (European Commission, 2011)

[7] European Convention on Human Rights 1953, s art 8. See also, Council of Europe, *STE N°108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Council of Europe, 1981)

relating to an identified or identifiable natural person ('data subject'); being an identifiable natural person the one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Moreover, processing according to the same article is, *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*».

Pursuant to the ECHR legal framework, domestic law must take appropriate safeguards to prevent any misuse of personal data as enshrined in article 8 of ECHR. In this sense, the Court has determined that ''*the need for such safeguards is all the greater where the protection of personal data undergoes automatic processing, the domestic law should ensure that such data are efficiently protected from misuse and abuse''*[8]. Thus, it can be coordinated with the first pillar of the UNGPs:'' *The state duty to protect human rights'*[9]''. This means that to ensure the enjoyment of individuals rights, states shall include in their domestic legal order appropriate steps to prevent, investigate, punish and redress abuses which occurred because of the actions of third parties, including business enterprises [10]. Moreover, in meeting their duty to protect, States should provide effective guidance to businesses on how to respect human rights throughout their operations.[11] Such guidance should indicate expected outcomes and share best practices[12].

Finally, the CJEU protects natural persons that have their data being processed. It is a fundamental right enshrined in the article 8 of the Charter of Fundamental Rights of the European Union. Article 16 of the Treaty on the Functioning of the European Union (Hereinafter TFEU) states that everyone has the right

[8] *Gardel v France* App no 16428/05 (ECHR, 17 December 2009)

[9] UNGP 2011, s art 1-10

[10] Ibid art 1

[11] Ibid art 3. See also, CNIL. *Guide for Processors* (edn 2017, CNIL 2017) or ICO. *'Guide to the GDPR* (1edn, ICO 2019) or AEPD. *Guide on personal data breach management and notification* (1edn, AEPD 2018)

[12] CNIL. *Guide for Processors* (edn 2017, CNIL 2017). See also, ICO. *'Guide to the GDPR* (1edn, ICO 2019) or AEPD. *Guide on personal data breach management and notification* (1edn, AEPD 2018)

to the protection of their personal data. Thus, the first data protection legislation used by the EU to respond to the personal data processing phenomenon was the 1995 Data Protection Directive[13]. However, at this time only 1% of the EU population was using Internet and Google had just launched its activities. Thus, the directive did not meet the amplitude of the phenomenon and appeared to be incompatible with the data processing phenomena. In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the European Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States[14]. Finally, in 2012, the European Commission made a proposal for a new Data Protection Regulation and in 2016, the GDPR was adopted and came into effect in 2018 replacing the Data Protection Directive 95/46/EC. In the same year, the European Commission adopted the Regulation[15] which repealed Regulation (EC) 45/2001, in order to bring into line with GDPR, the Union institutions bodies, offices and agencies regarding the protection of personal data. Yet, to protect personal data, EU authorities also have to address ‘’cookies’’. Indeed, they are an important tool that can give businesses a great deal of insight into their users’ online activity. Despite their importance, the regulations governing cookies are split between the GDPR[16] and the ePrivacy Directive[17]. The directive thus, leaves for EU member states the choice of means and form to implement the provisions of the directives in a timely manner. Consequently, the difference of means and form to implement such provisions led to the situation where, the protection of the users’ data doesn’t meet the same requirement everywhere within the EU.

Data protection is a contemporary issue for many countries all over the world since the value of the data has exceeded the value of the oil. The quantity of personal data processed each year continues to increase exponentially. Therefore, the ICT sector makes data easier to produce, edit, disseminate, and store, and all of this at an increasingly lower cost. This is the main reason why a company such as Facebook earns

[13] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

[14] Regulation (EU) 2016/679 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) [2016] OJ L 119/1

[15] Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data [2018] OJ L 295/39

[16] GDPR 2016, s recital 30

[17] Directive 2009/136/EC on the processing of personal data and the protection of privacy in the electronic communications sector [2009] OJ L337/11

its profit by harvesting and further processing the personal data of its users towards a third-party, rather than charging them with a subscription fee. Consequently, as we move around on the internet and in the real world, we are being continually tracked and profiled for the purpose of being targeted by advertising[18]. ICT corporations such as Facebook or Twitter justified that policy by stating that individuals are no longer actually interested in preserving their privacy[19] but, by opposition, are willing to share their own personal data with others. However, citizens do care about the data that has been collected and processed without their consent, especially for political purposes, since the Trump election and the successful pro-Brexit movement.

If some people are aware of the impact of their data with regards to their privacy, the majority are not. It is not so much the reasons why data is being used that is problematic, but the way it is processed. This way is destructive because it has been designed and used inappropriately. For instance, the CJEU has found that pre-ticked checkboxes does not constitute a valid consent to store cookies or accessing cookies stored on a website user's device, in a case which has considered the issue in light of the GDPR[20]. Indeed, where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. Consent is presumed to not be freely given if it does not allow for a separate consent to be given to different personal data processing operations. Although GDPR came into force, user find it difficult to express their rights with regards to their personal data. Firstly, reading privacy policies of ICT should not require a high level of reading ability. Secondly, regarding the legitimate interest of the Third-party tracking, the protection of the users' data doesn't meet the same requirement everywhere within the EU, notably in terms of the use of cookies. Indeed, it is the role of EU countries' data protection authorities to lay down the guidelines issued by the ePrivacy Directive. Consequently, the lack of consensus among the national's guidance, regarding the use of cookies, has undermined user's protected by the GDPR. Thirdly, regarding the right to obtain a copy of personal data, ICT do not appear to provide all the personal data undergoing processing such as advertising profiles and related data[21].

---

[18] Norwegian Consumer Council, *Out of control* (Forbrukerrådet, 2020)

[19] Gilian Bolsover, Elizabeth Dubois, Grant Blank, *A New privacy Paradox: Young People and Privacy on Social Networking Sites*. (Oxford Internet institute 2014)

[20] C-673/17 *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände* [2019] ECL I-801

[21] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD 2020)

Consequently, the thesis will investigate '' **Is GDPR implementation by EU Member States and EU-based companies effective in terms of personal data protection?''**

Basically, the methodology applied will be divided in to four main steps.

Firstly, this thesis will be focused on the legal framework of the personal data. It will be explained all the concept regarding personal data (Personal data, Processing, Data controller, Data processor, Data subject, Joint controllers). Thus, through the legal background of France, Germany, Spain and United Kingdom regarding their framework of data protection, the path that has led not only the states but also the European Community to enshrine the right to data protection as an autonomous right distinct from the right to privacy, and to set out the effects that this recognition of the protection of personal data has had within the EU legal order. The countries were chosen mainly because the research wanted to make a comparison between the evolution of the pioneers, namely France, Germany and Spain in the field of data protection, and those countries such as Spain and United Kingdom that were more reluctant to consider the opportunity of having a data protection within their domestic legal order .This comparison aims to highlight the differences that have emerged in the design of their national data protection and their impacts so far within the European Union.

Secondly, the thesis will address the concept of transparency as a pillar of the GDPR, mainly because it is now part of the principle relating to the processing of personal data and provides obligations for the ICT sector. In order to assess whether the provisions of the GDPR are being complied by the ICT sector, the thesis will use quantitative data that has been included in a report on privacy online[22]. It will confirm the hypothesis that Spotify UK, Amazon UK and Netflix UK do not comply with the GDPR in terms of transparency, in particular with regards to their privacy policies. These companies were chosen because they are leaders in their field and collect extremely important personal data in this respect. Thus, because of their economic interest, they have a wider impact on the enjoyment of human rights of the European population. The research reviewed the applicable privacy policies, cookie policies and other relevant notices, such as any advertising notices to assess how the companies are meeting their key transparency obligations under the GDPR. Thus, in order to assess the readability of privacy-related policies and notices, the research used an automated tool (Readable website, www.readable.com/) and the Flesch-Kincaid Reading Ease and the Flesch-Kincaid Grade Level formulas to gauge how easy or difficult they are to read. These tools have been used notably by Prof. Lorrie Faith Cranor who argued that the "*Flesch*

[22] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD 2020)

index has proven robust in many contexts and we do not immediately see any reason why privacy policies should be dramatically different from other types of textual analysis'' [23]. Finally, in the last part, the thesis will discuss of the impact of the legitimate interest on the transparency principle, which will give us a better insight to the effective implementation of the GDPR in terms of personal data protection.

In chapter 3, this thesis will be focused on the exercise of data subject rights as enshrined from Article 15 to Article 22 of GDPR. This chapter will be divided in two part. The first part, will discuss regular framework of the right of access to personal data, and will explain all the rights of data subjects and the relation between data subject rights and other human rights mechanisms, the enforcement of the rights of data subjects which implied some restrictions upon ICT sector. The second part, will outline the obstacles data subjects may face when they want to exercise their fundamental rights To support this argument, the thesis will refer to some case studies outlined by the report: TACD and European Union: *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD 2020).

[23] Aleecia M. McDonald, Robert W. Reeder Patrick Kelley, Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats* (Springer 2009)

Chapter 1: The Emergence of Personal Data Protection as a Fundamental Right of the European Union

I) The birth of Data protection in EU

This section will provide information necessary for a reader to understand in which ways UK, Germany, France and Spain have started regulating the processing of personal data. Indeed, by getting familiar with the roots of data protection into several countries and their positions with regard to the processing of personal data, it will be easier to understand the context of the development of Data Protection Law within EU legal order. Therefore, this section will explain the context of the adoption of Directive 95/46 and its impact on UK, Germany, France and Spain.

A) Example of UK, Germany, France and Spain

1) UK

The quest for a right to privacy in UK started right after the 1967 Nordic Conference. This conference was initiated by the International Commission of Jurist (Hereinafter ICJ), a non-governmental organization devoted to the promotion of human rights. This organization started to consider it necessary to define more accurately the concept of privacy. At this time, the right to privacy, ''*in the view of the participants to the Conference, had not only to be explicitly recognized in law, but also broadly configure in the light of technological developments, ensuring in particular the protection against interferences with correspondence, misuse of private communications, or disclosure of information received in circumstances of professional secrecy*[24]''. Shortly afterwards, British section of the ICJ called JUSTICE published its independent study, namely Privacy and the Law[25]. It laid down certain limitations and violations of the right to privacy of individuals that could be encountered, if we do not limit the impact of computerization. Since this report, the idea of privacy went from a theoretical concept to an actual

[24] Gloria Gonzàlez Fuster, *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1edn, Springer 2014) 42

[25] Littman, m., and P. F. Carter Rusk, Privacy *and the law* (1 edn, Stevens 1970). See also Gloria Gonzàlez Fuster, *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014)

development of the right to privacy. Indeed, in the absence of a general law, the common law had developed a case by case approach, where the right to privacy itself was not consecrated, but has many roots that can be found notably, within the law of confidentiality, or breach of confidence. According to another ICJ report[26], the protection granted was typically described as arising 'almost by accident, as an incidental effect of a variety of laws established for other purposes', unable to evolve towards a more general privacy protection. Finally, the recognition was definitely established, once JUSTICE drafted a Privacy Bill. Shortly afterwards in the UK, multiple privacy-related bills were adopted, such as a Data Surveillance Bill, and an unsuccessful Control of Personal Information Bill. Following the aftermath of the JUSTICE report and the adoption of successive Privacy Bill, a Committee of Privacy was appointed ''*to carry out a detailed examination of the subject of privacy*''[27]. It was decidedly focused on the use of computers for the processing of information, and more precisely their use in the private sector,'' *even if the subject had not been listed among its tasks*[28]''. In its final report, it set a series of principles to be taken into account by the data-processing industry and *'urged the industry to voluntarily adopt them as a code of good practice'*[29]. Finally, in 1973 UK joined the European Economic Community (Hereinafter EEC) and set up a Data Protection Committee that will later, lay down many contents of the first UK Data Protection Act. Indeed, the Data Protection Committee aimed at the adoption of legislation covering privacy issues from private sector, but also encouraged the setting up of an independent authority to ensure supervision, and ''*the mandatory registration of some computer users in order to process data*[30]''. Yet, it was only in 1984, after the Council of Europe approved a legally binding Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[31] that UK passed its first

---

[26] International Commission of Jurists (ICJ), *The protection of privacy* (ICJ, 1975) 414–602.

[27] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 43

[28] Ibid

[29] Ibid. See also, *Report of the committee on privacy (HC 1972-50-12)*

[30] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 43

[31] Council of Europe, *STE N°108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Council of Europe, 1981)

Data Protection Act[32]. Furthermore, with the enactment of a Human Rights Act 1998 that brought about the integration of Article 8 of the ECHR into UK law. It makes the protection of privacy in the UK definitely entered into a new phase. In fact, for many scholars[33] it has been described as a *"seismic shift'' or ''mini-revolution''*. UK was, therefore, ready to comply with the European Court on Human Rights and to create a general legal framework towards the right to Privacy. It was a rupture with the doctrine established by the Committee on Privacy on 1972, when it had the possibility to recognize the right of privacy, as a general right. At that time, the Committee was not interested in creating a legal framework of this particular right because that had not been the traditional way for England to protect the main democratic rights of citizens[34].

2) France, Germany and Spain

In the meantime, other countries such as France or Germany had already implemented article 8 of ECHR and have a broader definition of the concept of privacy which includes, in some cases, the regulation of the processing of personal data in order to enforce the legal protection of individuals. In fact, they can be considered as pioneers because 'their acts can be regarded as opening up a first period or wave of regulating activity, a wave starting in 1970 and ending in 1981 with the adoption of Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which subsequently became a main reference for all European legislators, influencing the drafting of later laws[35]. In the German Federal State of Hesse, the first legal instrument was developed on 9th November 1970. Its name was Datenschutz, which means data protection in German language. This data protection act aimed to regulate the processing of personal data stored within the Land's governmental files. It applied only to the public sector. Finally, it was rejected by the Bundestag[36] and it

[32] UK Data Protection Act 1984

[33] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 44

[34] *Report of the committee on privacy (HC 1972-50-12) 10*

[35] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1edn, Springer 2014) 56

[36] Ibid

was only in January 1977 that Germany finally enacted its first Federal Data Protection Law[37]. This Data Protection Law aimed at distinguishing data processed in the public and private sector. It focused mainly on data processing in the private sector by laying down specific rules to ensure the protection of personal data against misuse during their storage, transmission, modification or deletion. Concerning France, data protection started by the drafting of a legislative proposal[38] that encouraged the creation of both a Commission monitoring the use of computers (Comité de surveillance de l'informatique) and an ad-hoc Tribunal on computer-related issues (Tribunal de l'informatique). Despite the proposal was unsuccessful, it at least laid down the idea of regulating the processing of personal data, in order to reinforce the protection of data subject rights. Yet, it is only after a scandal caused by the publication that disclosed a project called S.A.F.A.R.I, which aimed to make collecting of personal data of individuals possible through a unique identifier that French government decided to launch the Commission informatique et libertés. The purpose of this commission was to determine the potential impact on human rights that computers may have[39]. Thus, the commission outlined that data related to the 'intimacy' of individual and family life, or racial, religious, political or similar information, was very relevant to understand the relation between computers and freedoms [40]. Finally, this report had the expected success, and France decided to adopt *la loi relative à l'informatique, aux fichier et aux libertés* ((Law on Computers, Files and Freedoms) of 6 January 1978[41]. The French law imposed a prohibition of collecting data without the will of the subject[42], and it also enshrined the right to access[43] and to rectify collected data[44]. Finally, it created a Commission Nationale Informatique et Libertés (Hereinafter CNIL)

[37] Ibid

[38] Proposition de loi tendant à la création d'un Comité de surveillance et d'un Tribunal de l'informatique 1970, SI /1454).

[39] Commission informatique et libertés. *Rapport de la Commission Informatique et Libertés* (La Documentation française 1975) P89

[40] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 61-65

[41] Loi relative à l'informatique, aux fichier et aux libertés *1978*

[42] Loi relative à l'informatique, aux fichier et aux libertés 1978, s art 26

[43] Loi relative à l'informatique, aux fichier et aux libertés *1978,* s art 34-40

[44] Loi relative à l'informatique, aux fichier et aux libertés 1978, s art 27

and empowered its monitoring and sanctioning powers[45]. In Spain, the regulation of processing personal data is enshrined in Article 18 of the Spanish Constitution[46]. In its third paragraph, the secrecy of communications, and, in its fourth and last paragraph, a mandate to limit the use of computers. However, many debates have arisen from the interpretation of this article. The recognition of a mandate to limit the use of computers in Article 18(4) was in any case accompanied by a recognition, among the constitutional provisions on principles of government and public administration, of a right for citizens to access public archives and registers, with the exception of those affecting the security and defense of the State, crime investigation, and the protection of the intimidad of individuals [47].

B) The development of Data Protection Law

1) The 1975 and 1976 Resolutions of the European Parliament

Around 1970, many events encourage the European Economic Community to take into account the emergence of personal data. Indeed, the commission of the European Communities *was concerned by the United States (US) companies' dominance within the European market of computer and data processing*[48]. Moreover, the public outcry which occurred in France, following the S.A.F.A.R.I S scandal, also had an impact in the European parliament. A French member of the European Parliament, Pierre Bernard Cousté, submitted an oral question to the Council on the subject of 'protecting the privacy of the Community's citizens. His questions concerned whether or not, the Council shall let the States Parties to take measures in protecting personal information alone, or shall the Council define privacy at the level of the European Community (Hereinafter EC) in order to ensure the same coherence along States parties.[49] As expected, many debates arose due to different national sensitivities of the time. For

[45] Loi relative à l'informatique, aux fichier et aux libertés 1978, s art 6

[46] Spanish Constitution 1978, s art 18 (3): ''*Secrecy of communications is guaranteed, particularly of postal, telegraphic and telephonic communications, except in the event of a court order to the contrary''*. See also, Spanish Constitution 1978 s art 18(4): ''*The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citiziens and the full exercise of their rights''*.

[47] Spanish Constitution 1978 s art 105(b)

[48] Commission of the European Communities. *Communication by the Commission of the European Communities concerning a Community policy for data processing* (EU Commission 1973) p 63/73

[49] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 113

instance, some deputies would argue that the Council shall urge member States to adopt ‘*’data protection laws, while others would argue that ‘a right to privacy’ should be defined at the level of the European Community*’’ [50].As a result, the European Parliament decided to prepare a report on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing[51]. Based on this report, the European Parliament adopted a resolution[52] which aimed to consider the necessity of the adoption of a Directive on ‘*individual freedom and data processing’’*[53]. In this sense, the European Parliament made a compromise toward those who argued that States should be granted a margin of appreciation for the implementation of provisions to protect personal data, and those who wanted to associate the rules of the processing of personal data with the right of privacy, through a definition proposed at the EC level. Yet, *neither the Commission nor the Council undertook any particular action in direct response to the European Parliament’s 1975 Resolution*[54]. It is the reason why a year later, the European Parliament adopted a second Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing[55], which aimed to request the Commission to start working on the drafting of EC legislation in order to avoid the adoption of conflicting national laws between Member States. The Commission moved forward and 20 years later, under the influence of the Council of Europe.[56] it adopted many proposals related to the protection of personal data such as the Proposal for a Council Directive[57]. Moreover, it

[50] Ibid

[51] European Parliament.: *report on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing* (European Parliament,1975)

[52] Resolution of the European Parliament *on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing* [1975] OJ C60/48.

[53] Ibid.

[54] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 116

[55] Resolution of the European Parliament of 8 April 1976 on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing [1976] OJ C100/27

[56] Council of Europe, *108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Council of Europe, 1981)

[57] Proposal for a Council Directive *concerning the protection of individuals in relation to the processing of personal data* (SYN 287). The proposal was transmitted to the Council on 27 July 1990, and to the European Parliament on 3 october 1990. See also, Proposal for a Council Directive *concerning the protection of personal data and privacy in the context of public*

also requested for a mandate to negotiate with the Council of Europe in order to adhere to [58] and more generally, to be part as member of the European Convention on Human Rights.

2) The ambitious Directive 95/46

Following the proposal for a Council Directive that became Directive 95/46/EC with some additional amendments[59], it was approved on 24 October 1995 [60] Although the Directive was expected by many Member States to address and consecrate the protection of personal data, it finally did not use the opportunity to do so. Directive 95/46 EC emphasizes the protection of individuals with regard to the processing of personal data. The purpose of this Directive is to oblige Member States to protect not personal data itself, but rather the rights and freedom of natural persons, and in particular their right to privacy, with respect to the processing of personal data[61]. Moreover, Directive 95/46 also aimed at ensuring and at the same time forbidding any restrictions of the free flow of personal data between Member State[62]. Thus, at the time of writing, the European Commission is still trying to make a compromise between the necessity of protecting and harmonizing the right to privacy along European Union [63] and encouraging the European market by supporting the free flow of personal data which consequently, and in some regards, would undermine data subject rights. It is for this reason that ECJ [64]

digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks (SYN 288).

[58] Recommendation for a Council Decision on the opening of negotiations with a view to the accession of the European Communities to the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data. See also, Gloria Gonzàlez Fuster. The emergence of Personal Data Protection as a Fundamental Right of the EU. 2014. Springer.

[59] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 125

[60] Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] OJ L281

[61] Directive 95/46/EC 1995, s art 1(1)

[62] Directive 95/46/EC 1995, s art 1(2)

[63] Directive 95/46/EC 1995, s Recital 10

[64] Joint Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others [2003]* ECR I-4989

reinforced the linkage between the directive and Article 8 of the ECHR. In Rundfunk[65], ECJ considered that although, directive 95/46 had been adopted using as legal basis an internal market provision, did not mean that it was only applicable when where directly at stake internal market issues. In this case, the question was whether or not, authorities could disclose data about employees, and on the applicability of Community Law in this context. Thus, ECJ interpreted the scope of this directive as the same way as Article 8 of the ECHR, by accepting certain interferences from authorities, unless it is in accordance with the law, pursues one or more of the legitimate aims specified in article 8(2)[66] of the European Convention on Human Rights. The ground on which such interferences can be justified is under conditions of being "necessary in a democratic society, in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". As the ECHR as affirmed many times, it is for the respondent Government to demonstrate that the interference pursued a legitimate aim[67], and in order to determine whether a particular infringement upon Article 8 is "necessary in a democratic society", the Court balances the interests of the Member State against the right of the applicant. When determining whether an interference was "necessary" the Court will consider the margin of appreciation left to the State authorities, but it is a duty of the respondent State to demonstrate the existence of a pressing social need behind the interference[68]. Indeed, the association between Article 8 of ECHR and the scope of the Directive 95/46/EC, has been commonly accepted among Member States in the view of limiting the scope of the rights and obligations set out by the Directive, notably in case of national security or for the prevention, investigation, detection and prosecution of crime[69]. The scope of this Directive can be regarded as the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing

[65] Ibid

[66] *Rundfunk* § 76

[67] *Mozer v. The Republic of Moldova and Russia* App no 11138/10 (ECHR, 23 February 2016)

[68] *Piechowicz v. Poland* App no 20071/07 (ECHR, 17 April 2012) § 212. See also, *Campanelli v. Italy* App no 25358/12 (24 January 2017) § 179-184.

[69] Directive 95/46/EC 1995, s art 13(1)

system or are intended to form part of a filing system[70] . In this sense, it went beyond the scope of Convention 108, which only covered automated data processing[71]. Furthermore, Directive 95/46 laid down some details regarding the concept of personal data that will be reutilized for the GDPR, 20 years later. Personal data, according to article 2(a) of Directive 95/46 EC is defined as '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'*. It also describes in its article 6: the 'principles related to data quality' which includes that data must: be processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in incompatible ways; adequate, relevant and not excessive in relation to the purposes of processing; accurate and, where necessary, kept up to date; and stored in a form permitting identification of data subjects only as long as necessary for the purposes of the processing. Regarding data subject rights and notably, the concept of consent, the Directive exposed conditions and rules to make data processing legitimate. It started with the necessity that data subject has unambiguously given his consent' to the processing[72]. Moreover, it described the to '*information be given to the data subject'*[73] and has afforded some rights for data subject, such as the right to access data[74], the right to object to some data processing practices[75] as well as a right not to be subject to some automated decisions[76]. Concerning the transfer of personal data to third countries, a prohibition of such transfer had been put in place, if the third countries would not have *'an adequate level of protection'*[77]. Yet, in order to preserve the economic area of the European Market, some exceptions have been set out in its Article 26. Finally,

[70] Directive 95/46/EC 1995, s art 3(1)

[71] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 136

[72] Directive 95/46/EC 1995, s art 7

[73] Directive 95/46/EC 1995, s art 10

[74] Directive 95/46/EC 1995, s art 12

[75] Directive 95/46/EC 1995, s art 14

[76] Directive 95/46/EC 1995, s art 15

[77] Directive 95/46/EC 1995, s art 25

all of these provisions within Directive 95/46/EC have to be protected by an independent supervisory authority, which will be in charge of monitoring the application of the implementing provisions[78]. It means that each Member State has to obtain at least one independent supervisory authority, and gives to this independent authority; *investigative powers, effective powers of intervention and the power to engage in legal proceedings*[79], as well as the possibility to hear claims from individuals[80]. This involvement of an independent authority is for a purpose of reducing the conflicts of national laws between the Member States, most notably by encouraging cooperation among all of the independent supervisory authorities.

Indeed, one of the benefits of adopting a Directive is the fact that it provides a period of time for States to implement its provisions. Once Directive 95/46/EC was adopted within the European Union, Member States had 3 years to adapt their national legislation to its content. While UK still did not have the right to privacy incorporated explicitly in the UK legal system[81], with the adoption of the Directive and the Human Rights Act in 1998, it was obliged to apply the rights set out in the ECHR, including Article 8 of the ECHR on the right to respect for private life, generally perceived as a key step for the protection of privacy in the UK[82]. Shortly afterwards, certain tensions arose between UK and the European Commission, which were in regard to the idea that privacy was being used to mould restrictively the scope of application of the transposing instrument [83]. Most of the claims were referring to the restrictive reading of the notion of personal data applied by UK. In Spain, the lack of instrument available to develop the mandate to legislate of Article 18(4) of Spanish Constitution was put to an end in 1992, when Spain adopted the Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LoRTAD). This law had already taken into account the proposal of the European Commission in 1990 and had ratified Convention 108 in 1984. In this regard, it tried to distinguish the term *'intimidad' from the term 'privacidad' by arguing that, whereas 'intimidad' was concerned with*

[78] Directive 95/46/EC 1995, s art 28

[79] Ibid

[80] Ibid

[81] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 149

[82] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 149

[83] Ibid

the sphere in which are developed the most reserved dimensions of a person's life, 'privacidad' referred to a wider spectrum of dimensions, facets that were possibly irrelevant separately, but that together draw up a picture of the individuals' personality that they are entitled to be kept concealed[84]. Eventually, Spain implemented Directive 95/46/EC in 1999, with *the Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)* and chose not to deal with the constitutional framing of personal data protection: contrary to the 1992 LORTAD[85].

Regarding Germany, as said before[86], it had its own data protection law provisions since 1970, namely the Federal Data Protection Act. Germany as a state solely had to review it, once in 2001, in order to comply with the European Commission[87]. Facing a pressure for not having transposed Directive 95/46/EC, France reported this issue to the European Commission arguing that its 1978 loi informatique et libertés appeared to be somehow consistent with Directive 95/46/EC. Yet, after announcing its intentions to do a review on it, as Germany previously did, Directive 95/46/EC was transposed in French Law in 2006 [88].

II) The recognition of the protection of Personal Data as a Fundamental Right

Early in 2000, many EU Members States encouraged the adoption of a Fundamental Right of the protection of personal data at the EU level. After many steps of the EU community towards this objective, it would be materialized with the inscription of a right to protection of Personal Data in the Charter, enacted by the ratification of the Lisbon Treaty in 2009. Thus, this recognition had led, first to many recommendations toward ICT companies in order to encourage them to protect Personal Data, and

---

[84] LORTAD 1992, s § 1 of preamble.

[85] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 151

[86] SEE chapter 1 (A) (2)' Comparison with other country in EU'

[87] European Commission, "*Report on the implementation of The Hague Programme for 2007: Follow-up of the implmentation of legal instruments in the fields of Justice, Freedom and Security at national level*", (European Commission, 2007)

[88] Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés 2004

then to the adoption of the GDPR which obliges ICT to comply with the regulation. Moreover, the possibility for the civil society and public authorities to bring ICT companies that are not in compliance with the protection of data, before the court, empowered data subject rights.

A) Steps towards the creation of a new right

1) The adoption of the right to protection of Personal Data in the Charter of Fundamental Rights of the European Union

It is true to say that henceforth, every EU Member State has, within their legal order, laws on the protection of personal data. More often, these laws are regarded as being of constitutional or equivalent importance. Yet, some differences have arisen between EU members in their ways of conceiving this framing. While some states, considerate that the fundamental rights dimension signals a connection with rights already protected by national instruments[89]. Eventually for others, the right to personal data was enshrined in their legal domestic orders, but not always named as the right of personal data[90]. In those States, the interplay between personal data protection laws and fundamental rights is characterized in terms of personal data being incorporated and associated to serve the right to privacy. Germany and Spain refer themselves to the first category. In Germany, the recognition of personal data as a fundamental right began in 1983, after the German Federal Constitutional Court abandoned the doctrine suggesting that the protection of personal data should be considered and associated under the content of preexisting Fundamental Rights[91]. Instead, the Court decided to associate the notion of self-determination which assumes, a dimension of the free development of personality according to which subjects need to have the capacity to decide autonomously and take free decisions[92], and the necessity to protect personal data, arguing that ''*that individuals would not act with total freedom if they did not know which data about them were being processed* [93]''. From there, the court developed and defined the

[89] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 174-184

[90] Ibid p 174

[91] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 174-184

[92] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 174-184

[93] Ibid

core elements of the new rights, emphasizing *that the use of personal data must respect a strict limitation of purpose, and that uses incompatible with the purpose of the original collection are to be forbidden*[94]. In Spain, the Constitutional mandate to legislate of Article 18(4) of Spanish Constitution, regarding the regulation of the use of computer, was fulfilled by LoRTAD, and it was eventually read by the Spanish Constitutional Court as a fundamental right[95]. It is only after a ruling that occurred in 1993, where a citizen requested access to its data but had been refused the access by public administration[96], that the Spanish Constitutional Court addressed more specifically the interpretation of Article 18(4) of Spanish Constitution. It associated the exercise of the control of personal data as a positive freedom for individuals and have deemed that although personal data are now an electronic archive, it still needs to be considered as belonging to the sphere of intimidad. This fundamental right was definitely consolidated in 2000, after a ruling of the Spanish Constitutional Court[97]. During the judgment, the Constitutional Court put forward the core elements of the right, described its boundaries and explicitly referred to it as the derecho fundamental a la protección de datos[98](‘fundamental right to data protection). On contrary, France had a different approach on the protection of personal data. The law applying is still the 1978 loi informatique et liberté, although it was amended two times (2004 and 2006), it does not recognize the protection of personal data as a separate fundamental right, to the great displeasure of CNIL that argued ‘‘*none of currently constitutionally protected French rights and freedoms appears to encompass the whole scope of the envisaged right to personal data protection’’*[99]. Concerning UK, it enacted the Human Right Act in 2000, which encompassed many provisions set out in the Convention 108 or Directive 95/46/EC, but privacy has still not been considered as a constitutional right. Therefore, the concept of privacy was limited and could not reach the next step, which is the recognition of the right to informational self-determination, as done by Germany. These differences between the terminologies

---

[94] Ibid

[95] Ibid

[96] Ibid

[97] STC 292/2000, *de 30 de noviembre de 2000 del Tribunal Constitucional (recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Perso*

[98] STC 292/2000 § 5.

[99] CNIL. *Press conference Présentation du 32ème Rapport d’activité 2011* (La documentation Française, 2012)

in legislations led to inconsistency regarding the protection of personal data among the EU members States, and can explain the Cambridge Analytica Scandal, where in UK, millions of users found their personal data exploited by a third party, without their consent. Indeed, where, privacy has not been a constitutional right, the value attributed to consent is seen differently. This may explain the position of treating consent as one of the many alternatives rather than giving it a primary status.

Foreseeing that such a situation could arise, the EC Member States decided to hold a meeting in Cologne in 1999, with an aim to create a 'Charter of fundamental rights of the EU'. Firstly, it was to give more visibility to EU citizens about Fundamental Rights applying within EU. Secondly, by consecrating and listing Fundamental Rights, it was a way to consolidate them at the EU level[100]. Yet, during the draft, disputes and tensions arose to the question whether or not, the draft shall lay down new rights as Fundamental Rights. Some country, such as UK or France expressed the idea that they did not want the creation of any new rights, particularly regarding the protection of personal data, because it was not the purpose of the drafting of the EU Charter[101], and a reference to data protection under the respect for private life was more than enough[102]. Other, such as Germany or Spain that have already establishing a fundamental right to the protection of personal data, and with the help of an international cooperation, namely the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (Group composed of representatives of the data protection authorities of member States) , they manifested their support for the inclusion in the upcoming catalogue of a right to the protection of personal data[103]. Thus, the establishing of the protection of personal data in Article 8 of the Charter, as an autonomous right distinct from privacy was not easily accepted by all EU Member States, considering that some of them were afraid of this right becoming restrictive for them because of the Charter 's potential binding nature in the future. For many scholars, it was uncertain whether the final text would generate enough consensus among member States in order to be adopted as a legally binding text[104].

---

[100] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 192. See also, European Council Conclusions concerning the Cologne EuropeanCouncil. (European Council, 1999) §44

[101] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 193

[102] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 197

[103] Ibid

[104] Ibid p 195

Thus, it is in this context that the drafting of the Charter started being written by representatives of the heads of State and Government, the President of the European Commission, Members of the European Parliament and national Members of the Parliament[105]. Unfortunately, only a minority of Member States recognized, after the signature of the Charter in 2000, protection of personal data as a fundamental right. This Charter, without being a binding instrument, did not in any case constitute a common constitutional tradition among them[106],and it is for this reason that the protection of personal data at the EU level, will be encouraged by the ECJ and by the Lisbon treaty[107].

2) The manifestation in the Case Law of the EU Court of Justice before the adoption of the Lisbon Treaty

Before the proclamation of the EU Charter, personal data was considered mainly within the light of the right to respect for private life. Afterwards, with the adoption of the EU Charter, this approach shifted to the point of considering personal data separately from privacy. Originally, the right to protection of personal data was first invoked by General Advocates in their Opinions[108], and it was later also referred to by the Court of First Instance[109] and by the ECJ in 2006.[110] At this time it stressed the Charter's linkages with previously existing sources for the identification of EU fundamental rights but did not consecrate the existence of a right to personal data protection. It did change with the Promusicae[111] case. For the first time, ECJ recognized the right to personal data protection. The case was about the applicability of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. Thus, the court argued that this directive sets out in its

---

[105] Ibid p 194

[106] Ibid p 206

[107] Ibid

[108] C-340/99 *TNT Traco SpA v Poste Italiane SpA [*2001] *ECR* I-*04109*, Opinions of Advocate General Alber, § 94 (in reference to Article 36 of the Charter)

[109] Joined Cases T-377/00, T-379/00, T-380/00, T-260/01 and T-272/01 *Philip Morris International and Others v Commission SpA* [2003] ECR II- *00001*, §122.

[110] C-540/03 *Parliament v Council* [2006] ECR I-*05769*

[111] C-275/06 *Productores de Música España (Promusicae)* [2008*] ECR I-0027,* § 64

preamble, stressing the importance of Articles 7 and 8 as safeguards of its applicability. Moreover, ECJ considered that Article 7 of the Charter ‘‘*substantially reproduces*’’ Article 8 of the ECHR, whereas Article 8 of the Charter ‘’*expressly proclaims the right to protection of personal data*’’. The Court thus innovatively used the EU Charter as a direct source for the identification of a fundamental right[112]. It was confirmed during the ruling of Rijkeboer in 2009. In his opinion for the case[113], Advocate General Ruiz-Jarabo Colomer had argued (mentioning Rundfunk) that ‘’ *the fundamental right to privacy, as a general principle of Community law, had found legislative expression in Directive 95/46/EC, which refers to the provisions of which were codified in Article 8 of the Charter[114]*’’.

Finally, with the adoption and ratification of the Lisbon Treaty which came into force on 1 December 2009, the Charter is able to impose its Fundamental Rights within the EU legal order. Indeed, Lisbon Treaty describes the three major modes of integration of fundamental rights in the EU legal order. In this sense, it consecrated the right to protection of data protection by granting to the EU Charter the same legal value as the EU Treaties[115]. Therefore, the Lisbon Treaty confirms the doctrine of ECJ regarding the right to data protection. Moreover, it enshrined this right, in article 16 (1) of the Treaty on the Functioning of the European Union (hereinafter TFEU), in the same term as Article 8(1) of the Charter and provides a a new legal basis for the European Parliament and the Council to lay down rules on personal data for data processing falling under EU law[116], and recalls that compliance with these rules shall be subject to control by an independent authority. Thus, the Lisbon Treaty allows European Parliament and the Council, for instance, to adopt data protection rules to replace Directive 95/46/EC without any need to ground them in a legal basis on the establishment of the single market [117].

---

[112] Promusicae § 64. See also: Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 206

[113] C-553/07 *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* [2008] ECR I- 03889, Opinion of Advocate General Ruiz-Jarabo Colomer

[114] Ibid § 8.

[115] TFEU 2008, s art 6(1)

[116] TFEU 2008, s art 16(2)

[117] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 206

B) Effect of the right of personal Data within EU legal order`

1) The adoption of the GDPR

Shortly after, the communication of EU Commission expressed the need for having a better EU legal framework regarding data protection. In 2012, EU commission announced a proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data[118]. This proposal aimed to be directly applicable in all Member States[119] and contained a right to be forgotten, a right to data portability, a general obligation to notify data breaches, and an existence of data protection officers in charge of reducing the impact of such data upon individuals. It is the translation of Article 16(2) of the Treaty on the Functioning of the European Union (Hereinafter TFEU) including, a right to the protection of personal data not mentioned in conjunction with the right to privacy, or as an element of privacy, but in place of the right to privacy[120], and the fact that in the EU Charter, data protection provisions (Article 8) are separated from the provision devoted to the right to respect for private life (Article 7). It made clear for the EU Commission, the necessity to abandon the provisions of the Convention 108, which had been consolidated by Directive 95/46/EC, according to which the protection of personal data serves fundamental rights and freedoms in general, but in particular privacy[121].

This new legal approach led to the adoption of the GDPR and the necessity to explain some concepts such as ‘’controller’’, ‘’processor’’ and ‘’ joint controllership’’, which in line with the new regulation are the key to understanding the rules that protect personal data. The GDPR defines the ‘controller’, as the “*natural or legal person, public authority or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (...)*”[122]. It implied five elements. The first one is related to the type of actors that can be controllers, and it covers any organizational

[118] European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. 2012

[119] Ibid p 8

[120] Gloria Gonzàlez Fuster. *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1 edn, Springer 2014) 243

[121] Ibid p 248

[122] GDPR 2016, s article 4(7)

entity. The second element concerns the factual influence that the controller has over the processing operation, by virtue of an exercise of decision-making power[123]. The third element relates to the determination of the purposes and means of the processing operation. ''*The identification of the 'why' and the 'how' of a processing operation can be regarded as the decisive factor for an entity to assume the role of 'controller' within the meaning of data protection law*[124]''. Indeed, during the processing of personal data, *the controller is the one deciding on the purpose ('why') and on the means to carry out such processing operation ('how')* [125]. Furthermore, Article 4(7) of the GDPR sets out the possibility for the purpose and means of a specific processing operation to be determined by more than one actor. This specification makes it explicitly clear that the concept of controllership does not necessarily refer to one single entity but can also involve multiple parties playing a role in a processing operation[126]. As a result, and as confirmed by the CJEU, each of the actors involved have obligations under data protection law [127]. Finally, any processing of personal data requires for one or a set of processing operation, fall under the responsibility of the controller[128]. Regarding the processor, it concerns natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller[129]. Thus, the role of a processor is to process personal data on behalf of the data controller. In other words, the processor is serving the controller's interest in carrying out a specific task and shall follow the instructions set out by the controller, at least with regards to the purpose and the essential elements of the means[130]. Yet, the processor should not be regarded as the controllers' subordinate but as the one that

---

[123] GDPR 2016- 1/2010 Opinion *on the concepts of "controller" and "processor"* [2010] 9. See also, Regulation 2018/1725 *Guidelines on the concept of controller, processor and joint controllership under EU regulation*. [European Commission, 2019]

[124] Ibid

[125] Ibid

[126] Ibid

[127] Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] ECLI -388, §29

[128] Regulation 2018/1725 *Guidelines on the concept of controller, processor and joint controllership under EU regulation*. [European Commission, 2019] 12-14

[129] GDPR 2016, s art 4(8). See also, Directive 95/46 1995, s art 2

[130] Regulation 2018/1725 *Guidelines on the concept of controller, processor and joint controllership under EU regulation*. [European Commission, 2019] 7-9

can share liability, in case of data breaches, or if the processor is found to have acted beyond the instructions and mandate given by the controller[131]. Finally, GDPR added a new category of actors, irrespective of the concept of 'controller' or 'processor'; 'the joint controllers'. It is the situation were two or more controllers determine the purposes and means of the processing[132], implying that each controller is aware of the general purpose and essential elements of the means of processing and determine together the means to carry out a processing operation[133]. However, being aware of the purposes and means of the processing without having access to personal data, is still, according to the ECJ regarded, as a joint controller [134]. Moreover, being considered as a joint controller is still at some regards, not a right for a controller to have access to personal data[135].

To conclude, at the time of the adoption of Directive 95/46/EC, only 1% of the EU population was using Internet, and Google had just launched its activities. Thus, the directive did not meet the amplitude of the phenomenon and appeared to be incompatible with data processing phenomena. This is the reason why the GDPR has a broader scope; it includes more binding standards and provides significant fines. For example, it requires that "*prior to giving consent, the data subject shall be informed thereof*''[136], and gives more rights to individuals when it comes to the access and dissemination of their own data. Thus, consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations[137]. Pursuant to Article 5 of the GDPR, the processing must satisfy the criteria of ''*lawfulness, fairness and transparency, purpose limitation and data minimization*''. However, it is not so much the data that is being used that is problematic, but the way it is processed. This way is destructive because it had been biased, designed and used inappropriately. For instance, the ECJ has found that pre-ticked checkboxes do not constitute valid consent to store cookies

[131] Ibid

[132] GDPR 2016, s art 26

[133] Regulation 2018/1725 *Guidelines on the concept of controller, processor and joint controllership under EU regulation*. [European Commission, 2019] 23

[134] Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] ECL I -388, §38

[135] Case C-25/17 *Jehovan todistajat* [2018] ECL I- 551, §69 and §75. This has been reiterated in Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2019] ECL I- 629, §. 69

[136] GDPR 2016, s art 7 (3)

[137] GDPR 2016, s recital 42

or accessing cookies stored on a website user's device, in the case which has considered the issue in light of the GDPR[138]. Therefore, the major update within the GDPR is that the processing of any EU citizens' information is now protected, regardless of whether the information processing is done within the EU or not, and regardless of where the retailer originates from. Any retailer around the globe that sells to an EU citizen is bound by law to protect private data. Indeed, where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation[139]. Thus, the data subject must be granted the enjoyment of the rights to have access to its personal data, through a transparency process. It requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used[140]. Moreover, data subject' rights implies a better control of the data of users from ICT companies, and the clarification of their responsibilities, in case of breaches. Indeed, breaches of the GDPR are subject to substantial fines, up to 4% of the annual global turnover for certain infringements.

2) The implementation of obligations for the private sector

Following the implementation of the Directive 95/46/EC and Lisbon Treaty within EU legal order, the consecration of the right to data protection, and the development of Internet, which has associated personal data with a great value in the last two decades, discussions were engaged at international level for the adoption of an instrument, targeting responsible ICT companies that have become increasingly active in recent years, by affecting the enjoyment of human rights notably, through the misuse of the personal data from users. This instrument, the UNGP, led to the adoption of the Guide on the implementations of the UNGP by EU Commission in 2011. The objective of this Guide is to enhance the balance between States duty' (Protection against human rights abuses) and the responsibility of ICT sector to implement provisions set out in the UNGP. In other words, ICT companies are expected, from setting out their commitment to respect human rights, to identifying and addressing their human rights

[138] C-673/17 *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände* [2019] ECL I-801

[139] GDPR 2016, s art 5

[140] GDPR 2016, s recital 39 . See also GDPR 2016, s art 12

risks, to providing remedy where actual harms occur[141]. At this regard, the guide sets some approaches that ICT corporations can put in place in order to avoid breaching the right to protection of personal data. The Guide recommended within ICT companies, to integrate individuals who are responsible for human rights, in the process of decision making, with staff responsible for the activities that may have an impact of the right to data protection[142]. For instance, in the case of high-risk contexts or severe impacts on data protection, it proposed *to involve relevant staff from across the business in discussions with affected stakeholders on how to address such impacts*[143]. Furthermore, it urged ICT to develop systems for protecting personal information stating that from a human rights due diligence perspective, *ICT should consider a range of issues in determining whether their systems adequately protect individual' personal information[144], and for responding to requests related to personal data*[145]. Although, the Guide is not a legally binding document, it translates the expectations of the UNGP to the specifics of the business sector.

More precisely, the UNGP also has many common grounds with the GDPR, notably through its three pillars; the State duty to protect human rights, the corporate responsibility to respect human rights, and the access to remedy. Regarding the first pillar, States must take appropriate steps to prevent any breaches of personal data in their domestic legal order[146]. In this sense, the GDPR carved out the possibility of each supervisory authority to advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing[147]. Moreover, GDPR translated the meaning of Article 2 of the UNGP which considers that ''*States should set out*

---

[141] HRB and SHIFT, *ICT Sector Guide on implementing the UN Guiding Principles on Business and Human rights* (European Commission, 2011) P 44

[142] Ibid

[143] Ibid

[144] Ibid

[145] Ibid

[146] UNGP 2011, s art 1

[147] UNGP 2011, s art 57

clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations''. Indeed, the GDPR sets out that each supervisory authority needs to promote the awareness of controllers and processors of their obligations under this Regulation[148]. This obligation has been met by many data protection authorities that have issued many guidance for controllers or processors[149], either for the private or public sector. The second pillar meets the provisions of the GDPR in a number of aspects. Firstly, in order to adverse human rights impacts[150] resulting of breach of personal data, GDPR expects controllers and processors to communicate of the breaches to the supervisory authority, not later than 72 hours after having become aware of it[151]. It also expects that ''*any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered*''[152]. Secondly, both the UNGP[153] and the GDPR require companies to seek to avoid, prevent or mitigate adverse human rights from their operations, products or services. Indeed, GDPR carves out that companies which are using, in particular, new technologies for processing personal data, to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data[154]. Furthermore, both controllers and processors shall provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject[155]. It has to recall that such obligations are applying to all companies[156] that are processing personal data ''*wholly or partly by automated means and to the processing other than by automated*

[148] GDPR 2016, s art 57(d)

[149] CNIL. *Guide for Processors* (edn 2017, CNIL 2017). See also, ICO. *'Guide to the GDPR* (1edn, ICO 2019) or AEPD. *Guide on personal data breach management and notification* (1edn, AEPD 2018)

[150] UNGP 2011, s art 11

[151] GDPR 2016, s art 33

[152] GDPR 2016, s art 82

[153] UNGP 2011, s art 13

[154] GDPR 2016, s art 35

[155] GDPR 2016, s art 24 and 28

[156] UNGP 2011, s art 14

means of personal data which form part of a filing system or are intended to form part of a filing system[157]''. Finally, in order to fulfill their responsibility to respect human rights[158], the UNGP and GDPR suggested a policy commitment. Indeed, the GDPR expects from data controllers and processors, the adoption of a code of conduct aiming at contributing to the proper application of the Regulation, but also expects from them to identify, prevent, mitigate and account for how they address their impacts on human rights, notably due to the risks that are presented by processing personal data, in particular from ''*accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed*[159]''. Concerning the access to remedies, as part of its duty, each supervisory authority must allow data subjects to have the right to lodge a complaint with a supervisory authority[160]. Moreover, every data subject has the right to an effective judicial remedy, either against a supervisory authority[161], or against a controller or processor[162].

3) The manifestation in the Case Law of the EU Court of Justice after the adoption of the Lisbon Treaty

Following the adoption of the Lisbon Treaty, the Charter and, more precisely, Article 8 of the Charter relating to the right of data protection, this right acquired a legally binding status. In the meantime, the ECJ continues to follow the jurisprudence of Promusicae and Rijkeboer' judgments which consider the right to data protection as an EU fundamental rights. Thus, in the case law of tele2 Telecommunication[163], the necessity to balance fundamental rights between copyright and EU data protection was brought to the foreground. The decision did not preclude the possibility for Member States to integrate within their own territory, an Internet Service Provider that assigns an IP address to its clients, as well as it accepts

[157] GDPR 2016, s art 2

[158] UNGP 2011, s art 15

[159] GDPR 2016, s art 32 (2)

[160] GDPR 2016, s art 77

[161] GDPR 2016, s art 78

[162] GDPR 2016, s art 79

[163] C-557/07 *Lsg-Gesellschaft zur wahrnehmung von leistungsschutzrechten Gmbh v. Tele2 Telecommuication GMBH* [2009] ECL I-107

the disclosure of personal traffic data from the Internet Service Provider to private third parties for the purposes of civil proceedings for alleged infringements of exclusive rights protected by copyright. Yet, the judgement held as well that, under the principle of proportionality, temporary IP address must not be stored the purpose of civil litigations in copyright infringement cases. Thus, the Court of justice expects EU member States to make a balance between provisions set out in the directive and EU fundamental rights. This necessity of proportionality will be reminded by the Court in a famous decision[164]. It was asked to the Court to invalidate Directive 2004/24, which requires telephone communications service providers to retain traffic and location data for a period specified by national law to prevent, detect, investigate and prosecute crime and safeguard security. Two interferences from the Member State Party have been raised by the court. First of all, the fact that an electronic communications services or public communications retain data relating to a person's private life constitutes an interference with Article 7 of the Charter. Secondly, the Directive is an infringement of Article 8 of the Charter because it provides for processing of personal data. According to the Court, the fight against serious crime and terrorism does not, in itself, justify the necessity of the retention measure without imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees effective to protect their personal data against the risk of abuse[165]. In other words, the Directive was incompatible with the Charter because of the Directive's lack of safeguards regarding how telecommunications data would be kept, managed, and accessed. Following the ECJ's ruling in Digital Rights Ireland, two other cases[166] were brought before the ECJ in order to clarify the interpretation of the Directive 2002/58 regarding the processing of personal data and the protection of privacy in the light of Articles 7 and 8 of the Charter. While the scope of this Directive should not apply in *''any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law*[167]'', the Court stated that a legislative measure which provides national authorities with the right to require from providers of electronic communication services access to data, falls within the scope

[164] C-293/12 and C-594-12 *Digital Rights Ireland LTD v. Ireland* [2014] ECL I- 238
[165] Ibid §51-58

[166] Joined cases C-203/15 *Tele2 Sverige AB c. Postoch telestyrelsen* and C-698/15 *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis* [2016] ECL I- 970

[167] Directive 2002/58/EC, s art 1(3)

of the Directive[168]. However, the ECJ held that the general and indiscriminate retention of all traffic and location data is in contradiction with Articles 7 and 8 of the Charter. Such interference could only be permitted if the objective was to counter serious crime[169]. Indeed, the ECJ considered that the limitations upon the respect for private and family life and the right to data protection have to be proportionate, necessary to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms[170]. Finally, the ECJ sets out guideline to Member States if they want to retain data from individuals, ''*as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime*''[171]. Concerning the transfers of personal data to third country, the rule set out by the Directive 2000/520 led to an agreement between the US-UE, so called *''the Safe Harbor Decision''*. It concerns the transfer of personal data between these two countries. Usually, such transfers can be put in place only if the third country ensures an adequate level of protection. The problem was that the principles of safe harbor scheme applied only to self-certified US organizations receiving personal data from the European Union, but not for the U.S. public authorities. Moreover, since the revelation of Snowden, the law and practice of the United States did not offer adequate protection against surveillance by public authorities of the data transferred to that country. For all the above reasons, the ECJ did not validate the Safe Harbor Decision. Few years later, in presence of the same actors of the latest proceedings[172] and despite the adoption of the GDPR, the European Court of Justice reminded supervisory authorities within the EU of the obligations of having an adequate level of protection to allow the transfer of personal data to a third-country, and in particular the role of each authority concerning the illegal dissemination of personal data

[168] Joined cases C-203/15 *Tele2 Sverige AB c. Postoch telestyrelsen* and C-698/15 *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis* [2016] ECL I- 970, §78

[169] Ibid § 102

[170] Directive 2002/58, s recital 11

[171] Joined cases C-203/15 *Tele2 Sverige AB c. Postoch telestyrelsen* and C-698/15 *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis* [2016] ECL I- 970, §120

[172] Case C-311/18. *Data Protection Commissioner v Facebook Ireland and Maximillian Shrems* [2020] ECL I- 559 (''Invalidation of the EU-US Data Protection Shield'')

used by the ICT sector. As stated in its first decision regarding the transfer of personal to third country, the ECJ decided to invalidate the privacy shield.

Chapter 2: Transparency as a pillar of GDPR.

I) The concept of transparency according to the GDPR

Transparency under GDPR implies the obligation for controllers to provide an amount of information to data subjects in order for not being prosecuted. In other words, transparency plays a key role in protecting personal data by setting out some requirements to data controllers. As a result, the burden of the proof is upon data controllers that have to demonstrate their compliance with GDPR, notably the respect of requirements under the transparency principle. However, in certain cases, transparency has exceptions which can lead to the possibility for ICT sector not to provide information to data subject and more generally, to restrain data subject's rights.

A) The role of the transparency to protect Personal Data

1) Transparency and the principle of accountability and fairness

In this sense, transparency under GDPR has an impact on "the provision of information to data subjects related to fair processing; how data controllers communicate with data subjects in relation to their rights under the GDPR; and how data controllers facilitate the exercise by data subjects of their rights[173] ". Transparency is not a new concept; it has already been alluded by previous Data Protection Law[174]. Yet, the main change now is the transparency, enshrined into the principles related to processing of personal data[175], while before it was not[176]. It implies a link between the principle of fairness and the new principle of accountability[177]. Following Article 24 and Article 5 of GDPR, the controller shall be able to demonstrate that personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject[178]. Therefore, the principle of accountability requires transparency of processing

[173] Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017] 5

[174] Directive 95/46/EC 1995, s recital 58

[175] GDPR 2016, s art 5

[176] Directive 95/46/EC, s art 6 (a)

[177] GDPR 2016, art 5(a)

[178] Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017] 5

operations in order that data controllers are able to demonstrate compliance with their obligations under the GDPR[179].

Finally, it is important to recall that transparency is now an integral part of the principles relating to processing of personal data. It is a principle which is covered by Article 12 of GDPR and interpreted by recital 39. The latter provides a definition of the meaning and effect of transparency's principle in the context of data processing: "It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed…"

2) Transparency and the right to be informed

The right to be informed is derived from rules laid down by the principle of transparency. Indeed, GDPR requires that "the controller shall take appropriate measures to provide any information or communications relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language[180]". It reflects the individual's right to be informed[181] about the use of their personal data, in order for them to exercise a degree of control over it. Among information required by GDPR, it creates a distinction between the obligations of the controllers when personal data are collected from the data subject, and when personal data have not been obtained from the latter. In the first category, data subject has the right to have information at the time when their personal data have been obtained, including information about the purposes of processing, the legal basis that entitled organization to process such data, the period for which the personal data will be stored, and the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the

[179] Ibid

[180] GDPR 2016, s art 12

[181] Ibid article 13 and 14

right to withdraw consent at any time[182]. Furthermore, Article 13(1)(f) sets out the conditions when data controller intends to transfer personal data to a third country or international organization, data subject has the right to be informed and controller shall incorporate appropriate or suitable safeguards and the means by which to obtain a copy of personal data or where they have been made available[183].When personal data have not been obtained by the data subject, GDPR requires same obligations for controllers of the first category, but emphasizes the responsibility of controller to know "from which source the personal data originate, and if applicable, whether it came from publicly accessible sources[184]", and to provide information when the legitimate interest is applied by the controller itself or a third party. Finally, regarding how data controllers facilitate the exercise of data subjects' rights, it has been partly set out by the second part of Article 14. The controller shall provide the information within a reasonable period of time after obtaining the personal data, but at the latest within one month. Thus, transparency applies throughout the life cycle of processing. Indeed, "at the start of the data processing cycle, when the personal data is being collected either from the data subject or otherwise obtained throughout the whole processing period, when communicating with data subjects about their rights; at specific points while processing is ongoing, for example when data breaches occur or in the case of material changes to the processing[185]", and at the end of the processing, with the existence of the right to request from the controller access to and rectification or erasure of personal data[186].

.

B) Exception of the transparency rules

1) Exemption of Article 13 and 14 of GDPR

Regarding the exceptions within the obligation to provide information, it has to be distinguished whether or not personal data have been collected directly from data subject. In the case where personal data were obtained from the data subject, Article 13 of GDPR sets out only one exception; if the data subject already has the information regarding the processing of its personal data, data controller does not need

[182] Ibid Article 13 (2) (c)

[183] Ibid Article 13(1)(f)

[184] Ibid Article 14 (2)(f)

[185] Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017] 6

[186] GDPR 2016, s art 14 (2)(c)

to provide further information[187]. Yet, it implies the principle of accountability as said above, the controller has the burden of proof to demonstrate that data subject already has the information, and "how and when data subject received it and that no changes have since occurred to that information that would render it out of date[188]". On the contrary, if personal data were not obtained from data subject; in addition to the circumstances where the data subject already has the information, Article 14 carves out a broader set of exceptions notably, if "the provision of such information proves impossible or would involve a disproportionate effort [189],where providing the information required under Article 14.1 would make the achievement of the objectives of the processing impossible or seriously impair them[190]", or in case where the Union or EU member States already provide measures to protect the data subject's legitimate interest[191], and finally, when personal data must remain confidential for the obligation of professional secrecy[192]

First of all, the situation where it ''proves impossible'' to provide information to data subject, seems complicated to apply for the data controller. According to the Working Party, "if a data controller seeks to rely on this exemption it must demonstrate the factors that actually prevent it from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so[193]". Regarding the provision of information that would involve a disproportionate effort, recital 62 refers to it and considered in this regard that " the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration" when assessing the disproportionate effort arguing by controller with regard to Article 14. In other words, to justify a disproportionate effort, controller has to already have put safeguards in place to ensure the protection of personnel data. If it is considered as inadequate, controller' liability should be engaged. Furthermore, concerning the purposes of the processing that may infringe the

[187] GDPR, s art 13(4)

[188] Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017] 24

[189] Article 14(5) (b) of GDPR

[190] Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017] 25

[191] GDPR 2016, s art 14(5)(c)

[192] GDPR 2016, s art 15(d)

[193] Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017] 26

obligations to provide information to the data subject. Firstly, the data controller has to demonstrate that *"the provision of the information set out in Article 14(1) alone would nullify the objectives of the processing"*. Secondly, this exemption has to be tempered because Article 14(5)(b) pre-supposed that the processing has to respect, in all circumstances, provisions set out by Article 5 of GDPR, namely personal data shall be processed lawfully, fairly and in a transparent manner. Finally, in case where the Union or EU member States already provide measures to protect the data subject's legitimate interest, and when personal data must remain confidential for the obligation of professional secrecy, the Working Party considered for the first case that *"this exemption is conditional upon the law in question providing "appropriate measures to protect the data subject's legitimate interests"*. Such a law must directly address the data controller and the obtaining or disclosure in question should be mandatory upon the data controller. Accordingly, the data controller must be able to demonstrate ''*how the law in question applies to them and requires them to either obtain or disclose the personal data in question*''[194]and, it should make it clear to data subjects that '' *it obtains or discloses personal data in accordance with the law in question, unless there is a legal prohibition preventing the data controller from doing so*'' [195]. In the second case, the Working Party considers that if a data controller wants to rely on the exemption set out in article 14.5(d), it has to demonstrate that information processed and collected fall under the obligation of professional secrecy which prohibits the data controller "*from providing all of the information set out in Articles 14.1, 14.2 and 14.4 to the data subject*.[196]"

2) Restrictions on data subject rights in regard with the transparency principle

Under GDPR, it is possible to restrict the scope of data subject rights in relation to transparency. Indeed, Article 23 sets out that " *the Union or Member States to which the data controller or processor is subject may (be restricted) by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22*". Furthermore, the same Article continues by stating that such restrictions shall "respect the essence of the fundamental rights and freedoms and (shall be)

[194] Ibid p 29

[195] Ibid

[196] Ibid

necessary and proportionate". Thus, it is clear that if data controllers rely on this exemption for not complying with the set of articles provided by the GDPR, it must be demonstrated firstly, how the national provisions apply to them, and afterwards, as stated in Article 23(2)(h) and also by the Working Party, "*data controllers shall inform data subjects that they are relying on such a national legislative restriction to the transparency obligation unless doing so would be prejudicial to the purpose of the restriction*[197]".

II) Failing to respect transparency: some case studies

This section will discuss how companies such as, Spotify, Amazon and Netflix are complying with Articles 12, 13 and 14 of GDPR which require ICT companies to provide information to data subject. In this sense, the thesis will analyze their privacy policies from different perspectives, firstly under the scope of readability and then, under the obligations of ICT companies to provide information about the use of personal data and rights.

A) The lack of readability to read privacy policies of Amazon, Spotify and Netflix

1) The necessity to implement 'appropriate measures' to meet transparency obligations

More often, to have access to information relating to personal data, the form and manner in which the information required under Articles 13 and 14 should be provided to the data subject, are referred to as a data protection notice, privacy notice, privacy policy, privacy statement or fair processing notice [198]. Indeed, GDPR does not provide any information rather that the controller shall take *''appropriate measures''* in relation to the provision of the required information for transparency purposes[199]. It means, according to the EU guideline initiated by the EU Data Protection Authorities that "*the data controller should take into account all of the circumstances of the data collection and processing when deciding upon the appropriate modality and format of the information provision. In particular, appropriate*

[197] Ibid

[198] Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017] 14

[199] Ibid. See also, GDPR 2016, s art 13(1)(f) and art 14(1)(f)

measures will need to be assessed in light of the product/ service user experience[200]". In other words, the EU Data Protection Authorities consider that "appropriate measures'' to be assessed, should result from feedback of experiences from costumers and users and not only from the side of ICT companies. It is again a manifestation of the principle of accountability because data controller has to demonstrate with its format and modality of providing information that personal data are protected by "appropriate measures in a concise, transparent, intelligible and easily accessible form, using clear and plain language[201]". Thus, one of the possibilities to test whether or not, the format and modality of providing information is adequate, with the readability expected by the users and the GDPR, is to use tools like test of readability or accessibility. Indeed, EU Data Protection Authority recognizes the role of readability testing and advised that if organizations "are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/notices/ policies etc., they can test these, for example, through mechanisms such as user panels, readability testing[202]" . It is indisputably clear that the collected personal data give an idea of the audience on the platform, therefore, ICT companies should use such data to determine what that audience would likely understand in a clear and plain language.

2) Weak score of the readability

Nevertheless, it has to be noted that it is not the cases of Amazon UK, Netflix UK and Spotify UK. Indeed, according to the report made this year in partnership with the European Union, reflecting the readability of the privacy policies issues by these companies, "it *would take between 17-21 minutes each to read the main privacy policies/notices of the three companies*[203]". It is not what should be interpreted as ''concise or easy' to understand. More precisely, the Flesh-Kincaid Readability formula[204] considers that on a scale of 0 to 100, a score of 30-49 is considered difficult to read. All of these companies had scores between 35-47, meaning they are all difficult to read. It has to be recalled that such modality and

[200] Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017] 14

[201] GDPR 2016, s art 12(1)

[202] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) p 13

[203] Ibid p 14

[204] '*Readability Formulas website'*, www.readabilityformulas.com/flesch-reading-ease-readability-formula.php

format to provide information to data subject does not meet the requirement neither of the guidelines carved out by the EU data protection authorities which had suggested that "*the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to [individuals]*[205]" , nor the GDPR in general. A table incorporated within the report summarizes all these data collected. For the relevance of the thesis, only the data in relation with companies based in UK shall be taken into account. Moreover, since this report, Spotify Privacy has updated only its Privacy Policy, and the latter has a score of 34.9, which unfortunately, is still considered as difficult to read.

Here the data collected, as followed:

Company	Document Type (sign up)	Number of Words	Time to Read	Flesch-Kincaid Reading Ease
Amazon UK	Privacy Notice	3863	17.10	40.4
	Cookie Notice	419	1.51	47.7
	Interest-Based Ads notice	527	2.20	39.4
	Conditions of Use & Sale	6459	27.31	44.5
Amazon US	Privacy Notice	2671	11.52	46.2
	Conditions of Use	3391	15.04	39.6
Netflix UK	Privacy Statement	4285	19.02	35.0
	Terms of Use	2267	10.04	45.9
Netflix US	Privacy Notice	3999	17.46	35.6
	Terms of Use	4057	18.01	40.9
Spotify UK	Privacy Policy	4738	21.03	43.2
	Terms and Conditions of Use	8457	37.35	35.6
	Cookie Policy (access to site)	1860	8.16	43.6
Spotify US	Privacy Policy	4728	21.0	43.3
	Terms and Conditions of Use	7469	33.11	36.2

Table 1: A Flesch Reading Ease score of 30-49 is considered difficult to read

In addition to the poor level of readability issued by the Flesh Reading, regarding policies and notices that were analyzed, the report highlighted the fact that the path to finding essential information, which led to the access of key choices and rights of personal data, should be easy and accessible for consumers to be used.

[205] Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017] 5

B) The assessment of information provided about the use of personal data and rights

1) The lack of clarity concerning information to exercise data subject rights

As explained above, it is true that Amazon, Netflix and Spotify have failed the test of readability which means that their privacy policies/notices are too difficult to be understood by users or consumers. Yet, it has to be noted that such tests are recommended but not mandatory. It is the lack of enforcement of Article 12 of GDPR, which requires ICT companies to clearly set out the personal data that they have processed, in an accessible way and using plain language. More specifically, privacy policies of Amazon and Spotify are organized under separate headings which describe what personal information is collected[206]. However, in practice, the use of long sentences and structures make it hard for consumers to understand and to read their privacy policies. Moreover, "individuals must also still seek out further specific details of purposes, and how to exercise their rights, including the right to access their personal information. This does not help people make informed decisions about the use of their personal data or exercise their rights easily[207]". Regarding the specific detail of purposes, both of the companies within their privacy policies, intend to explain the purposes of processing under distinct headings, yet, once inside these headings, they describe the purposes in a generic way[208]. For instance, Spotify[209] refers every time to ''legitimate interest''[210] as a legal basis to justify the process of individual's personal data, without providing any further information. Amazon is more problematic, since it neither explains the specific purpose for which personal data is used, nor on what legal basis it is under the GDPR[211]. This lack of information led individuals to take decisions, without having the sufficient knowledge of the personal data at stake. Indeed, it prevents "*individuals from making informed decisions about the use of their personal data and understanding the implications of such use*[212] ". Netflix also updated its Privacy

[206] TACD and European Union, Privacy *in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) p 14

[207] Ibid

[208] Ibid

[209] Spotify. Privacy Policy. See section ''What we use your personal data for''.2020

[210] Ibid

[211] Amazon UK. ''*Privacy Notice*''. Entitled at "For What Purposes Does Amazon Europe Process Your Personal Information? (Amazon UK,2019)

[212] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) p 14

statement[213], after the report was released, but unfortunately it is still a situation whereby individuals must search for information about specific matters such as the purposes of processing, user's rights, and access to data.

2) Information not clear about the processing of personal data

Regarding the purposes and legal basis for data collection, as being said above, legitimate interest is used many times to justify the collection of personal data. Yet, it is not the only one used for these companies to process personal data. In this sense, Spotify's privacy policy in its section entitled 'what do we use your personal data for', says it uses personal data for many different purposes. One of these purposes is to provide and personalize the Spotify Service which means the personalization of located content advertising on or outside of Spotify, including for third party products[214]. The other purpose is to collect information about an individual's interactions with the Spotify Service such as *"the date and time of any requests you make, songs you have listened to, playlists you create, video content you've watched [and] URL information, cookie data, your IP address, the types of devices you are using to access or connect to the Spotify Service, unique device IDs, device attributes."*[215] Spotify supports its argument by stating that the processing of such data is necessary for the performance of a contract and its legitimate interests. However, as noticed in the report based partly on Spotify UK[216], "Spotify does not notify individuals of the right to object to the processing of personal data or provide a means for individuals to object, and *"questions whether the company is meeting its obligations under the GDPR"*. Regarding Amazon, as explained above, it did not provide any information about the legal basis which justifies the processing of personal data. Netflix does the same but in an ambiguous way; it is still not possible to understand its Privacy Statement, and more specifically: what will be the legal basis for the processing and, which kind of data are used, which are the specific purposes for doing so. Furthermore, sometimes it considers that personal information may be processed for *''other purposes described in the Use of Information section of this Privacy Statement"*, but such purposes are not expressly defined in

[213] Netflix. *Privacy Statement* (Netflix, 2020)
[214] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) 15

[215] Ibid

[216] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) 15-17

the statement.[217] Thus, it appears that all are in contractions with the European Data Protection Board (EDPB) which has clarified that data controllers shall inform about the purposes of their processing, in a way that it is detailed enough in order to avoid any confusion as to what the legal basis is [218] . It is true to say that each company strives to collect data from individuals behavioral, from the first visit on their websites and throughout of their further online activity. From this, it is unclear what legal basis do companies rely on for these purposes under GDPR, for example, for the performance of a contract or the companies' legitimate interests[219]. The European Data Protection Board (Hereinafter EDPB) confirms the approach of considering as a general rule that using the processing of personal data for behavioral advertising is not necessary for the performance of a contract for online services. [220]

III) The regular framework of legitimate interest

In this section, it will be explained the condition to use legitimate interest as a legal basis for the processing of personal data and then, the thesis will expose how legitimate interest is used as tool for digital marketing.

A) Legitimate interest as a legal basis for processing

1) The legitimate interests of data controller

The assessment of the accountability and lawfulness of processing based on legitimate interest as legal basis, will result of the ability of ICT companies to demonstrate that each processing of personal data was necessary for the purposes of the legitimate interests[221] i.e. the processing represent a real and present interest ,and was complying with the principles of processing personal data, specially the one

[217] Ibid 14

[218] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) 15-16. See also, Regulation 2016/679 *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects''* [European Commission, 2019]

[219] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) 15-16

[220] Regulation 2016/679 *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects''* [European Commission, 2019] §57

[221] GDPR 2016, s art 6 (1) (f)

regarding transparency[222].Indeed, GDPR expects that when the processing is based on the ground of legitimate interest, it should be clear to the users the legitimate interest pursued by the controller or by a third party [223]. Moreover, article 6(1) (f) carves out that it is prohibited to process personal data on the basis of legitimate interest, "where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". During the discussions prior to the adoption of the GDPR, a list was drafted to outline which kind of fundamental rights and freedoms of the data subject can be overridden by the interest of the data controller[224]. These lists have been found in provisions and recitals of GDPR. They provide the way forward to asset the balance between the rights and freedoms of the data subject and the interest of the data controller. Thus, for instance, when it is necessary to fight the fraud or for direct marketing purposes, the processing of personal can be justified on the ground of legitimate interest[225]. Moreover, data controller has to take into account the reasonable expectation, at the time and in the context of the collection, of data subject regarding the processing of its personal data. Further processing based on the same legal basis, where data subject does not expect them, could override the interest of data controller and not be considered as a legitimate interest.[226] Furthermore, a legitimate interest can be regarded when controller is transferring personal data within the group of undertaking for internal administrative purposes[227]. Ditto for the purposes of ensuring network and information[228] or security, notably in case of data sharing for reducing the threats to public authority[229] or " if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[230] ". Finally, the concept of interest needs to be distinguished from the concept of purpose

[222] Ibid art 5

[223] Ibid art 14(2) A

[224] Directive 95/46/EC *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'* [European Commission, 2014] Section III.3.1 P25-26

[225] GDPR 2016, s recital 47

[226] Ibid

[227] Ibid recital 48

[228] Ibid recital 49

[229] Ibid recital 50

[230] Ibid

as mentioned in Article 6(f) of GDPR. Purpose in data protection means that data controller is aiming to process personal data on the ground of a specific reason. An interest here, is broader and can be the result from a benefit that the controller obtains from the processing[231]. It has to be clearly articulated in order to asset if the interest and fundamental rights of the data subject can be overridden by the interests of data controller. In other words, according to the Information Commissioner's Office which is the data protection authority in UK, this test can be broken down into three elements.: *"(1) Purpose test: are you pursuing a legitimate interest? (2) Necessity test: is the processing necessary for that purpose? (3) Balancing test: do the individual's interests override the legitimate interest?''*[232]. First of all, when pursuing a legitimate interest, controllers have to identify which interests can apply in order to justify the fundamental rights that they want to exercise. It can be the freedom of the arts and sciences[233], the right to liberty and security[234], or the freedom to conduct a business [235] . Afterwards, the processing needs to be necessary for the exercise of the fundamental right chosen. The balancing test require the data controller to asset the impact that such processing will have upon data subject. It needs to be taken into account, emotional states of data subject "*that may result from a data subject losing control over personal information or realizing that it has been or may be misused or compromised, – for example through exposure on the internet*[236] ".

2) Interests of the data subject

GDPR requires to data controller to take into account the interests or fundamental rights and freedoms of the data subject which require protection of personal data, when processing personal data for the purposes of legitimate interest[237]. These fundamental rights are those enshrined in the Charter. Thus,

[231] Directive 95/46/EC *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'* [European Commission, 2014] Section III.3.1 P25-26

[232] ICO. *'Guide to the GDPR'*(ICO, 2018) 77-83

[233] Charter 2001, s art 13

[234] Ibid art 6

[235] Ibid art 16

[236] Directive 95/46/EC *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'* [European Commission, 2014] Section III.3.4. P38

[237] GDPR 2016, s art Article 6(f)

when data controller aims to process personal data under legal basis of the legitimate interest, it has to take into the interests but also the fundamental rights and freedom of the data subject. The' interests 'of data subject in the sense of GDPR include all the relevant interest that may have data subject. Moreover, in opposition with 'the legitimate interest' that has been laid down in the provisions and recitals of GDPR, data subject interests under the scope of GDPR therefore, applies *"a wider scope to the protection of individuals' interests and rights*[238] *"*.Indeed, interferences cannot be tolerated if it overrides the interests and rights of data subject. For example, *" an individual who may have perpetrated theft in a supermarket could still see his interests prevailing against the publication of his picture and private address on the walls of the supermarket and/or on the Internet by the owner of the shop*[239]" . Finally, in case if the third party or the data controller wish to process personal data of data subject, the latter should be entitled to object to the processing of its personal data[240]. The data controller can still go beyond this restriction, yet it has to demonstrate that its own interest overrides the rights and fundamental freedoms of data subject[241].Finally regarding the transfers of personal data under the legal basis of legitimate interest, the assessment between the interest of data controller and the fundamental rights and freedom of data subject has still to be carry on by the data controller which in case of complaint, would have to demonstrate its compliance under GDPR.

B) Legitimate interest as tool for digital marketing

First of all, the GDPR allows the use of legitimate interest to serve digital marketing purposes[242].Using as legal basis, the legitimate interest which allows companies themselves to asset the balance between their legitimate interest and the rights and freedoms of data subjects, seems to make it inevitable that personal data will end up into the database of hundreds of companies that individuals have never heard of[243]. Indeed, the legitimate interest pursued by the data controller or the third party can be controversial,

[238] Article 29 Data Protection Working Party '*Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'*2014. See Section III.3.3. P30

[239] Ibid

[240] GDPR 2016, s recital 69

[241] Ibid

[242] GDPR 2016, s recital 47

[243] Ibid

notably when the interest is based on "*the economic interest of a company to learn as much as possible about its potential customers so that it can better target advertisement about its products or services.*"[244]This flexibility offered to business-oriented supporter to have the possibility of processing personal data under the broader definition of legitimate interest, and make them responsible of the balance between their interest and those from data subject, removes a degree of legal certainty. Indeed, the consumers do not want to be targeted but feel powerless. It is due to the fact that it is beginning to become the responsibility of users to check whether the balancing test carried out by the data controller is lawful and comply with all the principles of personal data processing and if appropriate safeguards have been put in place in order to protect personal data[245]. In addition, GDPR expects data controller to assess "all the circumstances surrounding the data transfer and should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data"[246].While under the principle of transparency, data controller shall justify the data involved in the processing under the legal basis of legitimate interest. It is the lack of information provided by the third party or data controllers, regarding the personal data involved under the basis of legitimate interest that makes the spread of data out of control.

[244] Article 29 Data Protection Working Party '*Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'*.2014. See Section III.3.1. P30

[245] GDPR 2016, s recital 50

[246] Ibid recital 113

Chapter 3: The rights of Data Subjects

I) The EU legal framework of the rights of data subject

A) What are the data subject' rights?

All the data subject rights enshrined in GDPR are derived from the obligation to transparently process personal data, which applies to the necessity of providing certain information to data subject rights.

1) The right of access

The right of access to data is the translation of Article 8 of the Charter of Fundamental Rights which states: "everyone has the right of access to data which has been collected concerning him or her". This right of access has been materialized by the right to obtain a copy of personal data, as it helps individuals to understand how and why ICT sector is using user's data, and to check if it is doing it lawfully[247]. In practice, individuals have the right to have the information that confirms that an entity is processing their personal data, a copy of personal data and other supplementary information, which will depend on, whether or not, personal data have been collected from data subject[248]. Regarding the content of the copy of data, GDPR does not require to make information legible. Usually, it takes the format of coded information. In other words, the additional information provided to response to a request has to be understood by an average person, children included. However, controllers are not required to ensure that information included within the copy will be understood by the particular individual making the request[249]. Finally, a request can be made to any part of the organizations and does not have to be to a specific person or a contact point. Moreover, the request does not have to include the phrase 'subject access request' or Article 15 of the GDPR, as long as it is clear that the individual is asking for his/her own personal data[250].

2) The right of rectification

[247] ICO. *'Guide to the GDPR* (1edn, ICO 2019) 51-60. See also, GDPR, s art 15

[248] See Chapter 2 I.A(2) '' Transparency and the right to be informed'', See also GDPR, s art 13 and 14 GDPR.

[249] ICO. *'Guide to the GDPR* (1edn, ICO 2019) 90-98. See also, GDPR, s art 15

[250] Ibid

The GDPR also includes a right of rectification in order to let individuals, in case of inaccurate personal data, rectify the mistake. It is the result of Article 16 and Article 5(1)(d) which concern the accuracy principle, whereby, controller has to take steps to ensure that the personal data were accurate, when obtained. This right imposes a specific obligation to reconsider the accuracy upon request. As for the right of access, the request can be verbal or in writing, it does not need to have the mention of 'request for rectification'. As long as the individual has challenged the accuracy of their data and has asked the controller to take steps to complete data held about them that is incomplete, this will be a valid request under Article 16. The fact that this right can be evoked verbally presents a challenge for any employees that could receive a valid verbal request. It is for this reason that GDPR encourages the controller to provide means for requests to be made electronically, especially where personal data are processed by electronic means.

3) The right to object

The right to object found its provisions under Article 21 of GDPR. It gives individuals the right to object to the processing of their personal data at any time. It is a preventive measure which allows individuals to ensure that their personal data will not be processed by the controller. The objection can have different features. It can be in relation to the processing of personal data concerning him or her[251], or where personal data are processed for direct marketing purposes[252]. In case of the latter, the personal data shall no longer be processed for such purposes[253]. Moreover, the controller has to inform at the latest, at the time of the first communication, the legitimate grounds used for the processing[254]. Finally, in the context where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject shall have the right to object to processing of personal data concerning him or her[255]. Again, in this case GDPR does not specify how to make a valid objection[256], therefore, it can be made either verbally or in writing. Individuals do not need to have to include the mention of 'objection to processing' as long as the condition stated above applied.

[251] GDPR 2016, s art 21 (1)

[252] Ibid (2)

[253] Ibid (3)

[254] Ibid (4)

[255] Ibid (6)

[256] ICO. '*Guide to the GDPR* (1edn, ICO 2019) 147-156

4) The right to erasure

The right to erasure also knows as 'the right to be forgotten' is applied under Article 17 of GDPR. This Article suggests that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay[257]. More specifically, it lays down obligations of controllers to erase personal data without undue delay where one of the following grounds applies: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed[258], the consent has been removed and there is no other legal ground for the processing[259], personal data have been unlawful processed[260]. Finally, individual can make an objection verbally or in writing.

5) The right to restrict processing

This right can be linked to the right to rectification and the right to object. It is Article 18 of the GDPR that considers, under certain circumstances, the possibility of restraining access from personal data. It means that individuals can limit how a company is using their data[261], and also it can be an alternative to requesting the erasure of personal data[262]. Moreover, if the request concerns the accuracy of the personal data, or the legitimate interest pursued by the controller or the third-party does not override those of the data subject, the data subject shall have the right to obtain from the controller restriction of processing[263]. In most of cases, the restriction of individual personal data is not definitive, but it will be put in place for a certain period of time[264]. Like the other rights, GDPR does not specify how to make a valid

[257] GDPR 2016, s art 21(1)

[258] Ibid article 17 (1)(a)

[259] Ibid art (1)(b)

[260] Ibid art (1) (d and e)

[261] Ibid art 18 (1) (d)

[262] Ibid art 18(1)(b)

[263] Ibid, art 18(1)

[264] ICO. *'Guide to the GDPR* (1edn, ICO 2019) 125-133. See also, GDPR 2016, s art 18(3)

objection[265], therefore it can be made either verbally or in writing. Individuals do not need to have to include the mention of 'request for restriction', as long as the condition stated above applied.

6) The right to data portability

The right to data portability is the right which entitles individuals to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmits this data directly to another controller[266]. In other words, it mainly applies when the lawful basis for processing is the consent, or because of the performance of the contract, or if the company is carrying out the processing by automated means[267]. Moreover, it provides the data subject the right to have the personal data transmitted directly from one controller to another[268], and to receive a copy of personal data. Yet, this right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[269]. Data portability only applies to personal data. According to the ICO, "*this means that it does not apply to genuinely anonymous data. However, pseudonymous data that can be clearly linked back to an individual (eg where that individual provides the respective identifier) is within scope of the right*"[270]. In case when personal data belongs to different individuals and were included in the data portability, controller has to asset whether or not, such transmissions of data would adversely affect the rights and freedoms of the third party. As similar to other provisions, GDPR does not specify how individuals shall exercise data portability rights. Therefore, it means the request can be made verbally or in writing and does not need to have the mention of 'request for data portability', or reference to Article 20 of GDPR, as long as one of the conditions listed above applies.

7) The right related to automated decision-making including profiling

Profiling is now defined by GDPR under Article 4(4) and recital 71 of GDPR which consider the possibility of "the use of personal data to evaluate certain personal aspects relating to a natural person,

---

[265] Ibid

[266] GDPR 2016, s art 20(1)

[267] GDPR 2016, s art 20(1) of GDPR

[268] GDPR 2016, s art 20(2)

[269] GDPR 2016, s art 20 (3)

[270] ICO. '*Guide to the GDPR* (1edn, ICO 2019) 133-146

in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement." Whereas, automated decision-making is the process of making a decision by automated means without any human involvement. These decisions can have factual data as basis, as well as on digitally created profiles or inferred data. For example, an online decision to award a loan[271]. Yet, by opposition it can also be beneficial for individual in many sectors, including healthcare, education, financial services and marketing. They can lead to quicker and more consistent decisions, particularly in cases where a very large volume of data needs to be analysed and decisions taken very quickly[272]. Thus, the right related to automated decision-making gives the opportunity to the data subject not to be part of a decision based solely on automated processing, including profiling.

8) The right to be informed

See chapter 2, I(A) (2) Transparency and the right to be informed.

9) The relation between data subject rights and others human rights mechanisms.

All these data subject rights are new since the adoption of the GDPR. Often, these rights let the possibility of data subject to have an insight regarding practices of companies toward its personal data and, where appropriate, allow users to restrict the access to it. In any case, it is ICT sector that has to demonstrate its compliance with the request submitted by data subject. In case of when an issue arises between data subject and companies, *"every data subject shall have the right to lodge a complaint with a supervisory authority*[273] "or for any entity contesting the claim of data subject, including the supervisory authority itself [274]. It can be regarded as the translation of UNGP, regarding the access to remedy notably when it comes to the EU member States to ensure that "*through judicial, administrative, legislative or other appropriate means, that when such abuses occur within their territory and/or*

[271] ICO. *'Guide to the GDPR* (1edn, ICO 2019) 156-162

[272] Ibid

[273] GDPR 2016, s art 77

[274] Ibid art 78

jurisdiction those affected have access to effective remedy"[275]. Moreover, GDPR as UNGP carve out the possibility of having appropriate non-judicial grievance mechanisms, alongside judicial mechanisms[276]. As non-judicial grievance mechanisms, it may be mediation-based, adjudicative or follow other culturally appropriate and rights-compatible processes. It seems that GDPR is being shaped in order to respect the UNGP and the EU Charter in order to improve the respect and accountability of ICT sector, particularly by ensuring the respect and enforcement of Article 8 of the EU Charter that states: (1)Everyone has the right to the protection of personal data concerning him or her; (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority.

B) The enforcement of the rights of data subject

1) Time limits for complying with the rights of data subjects

Under the principle of transparency granted by the GDPR, controller has to provide information on action taken upon a request of a data subject without undue delay and in any event within one month from the receipt of the request[277]. This time limit concerns all the rights of data subject. However, if the request is complex or if the same individual fill in other requests to the same controller, GDPR accepts the possibility of extending this period by additional two months[278]. In this sense, if the controller wants to comply with GDPR, it has to notify to the data subject any extension within one month[279], and explain why this extension is necessary. By opposition, if the controller does not accept the request of personal data made by an individual, the controller shall inform this individual without delay and "at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy[280]". Furthermore, in most

[275] GDPR 2016, s art 25

[276] Ibid art 78 and 79

[277] Ibid art 12 (3)

[278] Ibid

[279] Ibid

[280] GDPR 2016, s art 12(4)

cases, the request has to be provided for free of charge[281]. This period of time for complying to requests sent by data subject is an asset for the enforcement of data subject. It emphasizes the principle of accountability by setting out obligations of companies. Therefore, with the limit of storage of personal data, they shall be considered as keys for the enforcement of data subject rights.

2) Limit of storage of personal data

Limiting the storage of personal data is one of the principles of the processing of personal data. It is linked to the right of restriction and accuracy laid down in Article 5(1)(c) and Article 5(d) of the GDPR. The combination of these articles has an impact on the obligation of the data controller to limit the retention of personal data. Firstly, organizations shall erase any personal data that are inaccurate and no longer needed for the purposes for which they are processed[282]. Secondly, it is mandatory for them to review personal data that they have been collecting, in order to permit the identification of data subject that no longer has a purpose to be kept[283]. Furthermore, the principle of accountability makes some effects as well. Indeed, it is data controller that has the burden of proof to demonstrate that either, such data were erased because of their irrelevance with the ongoing processing or are still necessary for the purposes for which the personal data are processed. Finally, the only condition that allows personal data to be kept for longer, while the purposes of the processing terminated, it is for archiving purposes in public interest, for scientific or historical research aims or statistical purposes in accordance with Article 89(1). In other words, when applying the provisions of Article 5(1)(e), it is possible to continue to process personal data, even if it is not for the purposes for which personal data are processed (eg. for the public interest). Yet, in this case, safeguards should be applied to data subject, notably the anonymization or pseudonymization[284]. Indeed, they will alter in a way that is no longer permits identification of the data subject.

II) Restrictions of the rights of data subject

[281] Ibid art 12(5)

[282] Ibid art 5(1)(d)

[283] Ibid art 5(1) (e)

[284] Ibid art 89

Data subject rights are not absolute rights, they can be undermined if the request is considered as unfounded or excessive, or due to the legitimate interest. In practice, there are other difficulties to exercise data subject right, notably to obtain a copy of personal data.

A) Reasons to restrict the rights of data subject

1) Unfounded and excessive requests

Article 12(5) of GDPR carves out the possibility for data controllers to be exempted of responding to subject access requests, notably when such requests are manifestly unfounded or excessive. According to ICO, a request can be manifested unfounded if the individual clearly has no intention to exercise its right of access. For example, an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organization; or the request is intended to cause disruption[285], or to make unsubstantiated accusations against the organization or its employees[286], or to target a particular employee. The key is to consider whether or not individuals have a clear intention to exercise their rights. The onus is on the controller to demonstrate that, taking into account the context in which the request is made, it is clearly and obviously unfounded. Concerning a request that can be considered as excessive, it is the situation where an individual repeats the substance of previous requests, and a reasonable interval has not elapsed; or it overlaps with other requests that are considered as excessive because of the fact that doing so would constitute a disproportionate effort to comply with the timeline established by GDPR[287]. At any cases, it is the controller that has to demonstrate its compliance with GDPR and mainly on which legal basis or circumstances, it found the request of the data subject unfounded or excessive[288]. ICO reiterates that each request must be considered on a case-by-case basis. Indeed, a request should not be considered excessive merely because it is particularly broad or burdensome. In this case, the controller may ask for clarification, but is always obliged to make a "reasonable" search for the information. However, in certain cases, the cooperation of the data subject and the provision of additional information

[285] ICO. *'Guide to the GDPR* (1edn, ICO 2019) 107

[286] Ibid

[287] GDPR 2016, s art 12(5)

[288] Ibid

may be necessary for the controller to carry out this reasonable search. In its guidance released, the ICO informs data subject about what to expect when making access requests, and which organizations they can address when dealing with data subjects[289]. A controller has two options for processing a request that it considers falling under the two categories mentioned above: (1) the controller may refuse to process the request. In this case, the controller shall inform the data subject of the reasons for the refusal of the request, and of his or her right to lodge a complaint with the national data protection authorities where the damage occurred, in order to seek judicial remedy. Furthermore, (2) a controller may decide to respond to a request even if he considers it manifestly unfounded or excessive. In this case, the controller is allowed to make the execution of the request subject to the receipt of "reasonable compensation" from the data subject. The controller must be able to justify the level of the fees requested and these fees must be based on the administrative costs related to the execution of the request. If the fee request is reasonable, the time limit for replying to the request is suspended until the data subject has paid the requested fee.

2) Legitimate interest

As being said in chapter 2[290], legitimate interest is the most flexible way to process personal data. Under Article 6(f) of GDPR, it means that a processing is considered lawful, only if it is based on legitimate interest. In most the cases, it is used by companies to process personal data. However, in terms of responding to data subject requests, it is unclear whether or not data subject can have a copy from all the personal data that have transited under legitimate interest. It gives the possibility of ICT sector to transfer some of the data collected from data subject to a third party, if safeguards have been put in place[291]. Lately, the ECJ[292] considered that transfer of personal data between US and EU could not happen because of the fact that surveillance tools deployed in the United States are incompatible with the protection of personal data guaranteed to Europeans by the GDPR. Furthermore, the ECJ emphasizes the role that data protection authorities should have when such violations occur. They are obliged to suspend or forbid any transfer of personal data when appropriate safeguards have not been put in place. Thus, it is still

[289] ICO. *'Guide to the GDPR* (1edn, ICO 2019) 98-110

[290] See Chapter 2, III) A) 1) The regular framework of the legitimate interest

[291] GDPR 2016, s art 45

[292] C-498/16 *Shrems v. Facebook Ireland Limited* [2005] ECL I-37

unclear if under the term of appropriate safeguards whether or not data subject can have a copy from all the personal data that have transited under legitimate interest and have been collected by the third party. Moreover, the right to erasure and the right to restriction of processing can be undermined, at least for a period of time, notably when the data controller is pursuing a legitimate interest that override the protection afforded to personal data[293]. Thus, because of the legitimate interest, it may be possible for the controller not to comply with the request until the purpose of the processing is still overridden the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. The assessment is carries out by the data controller and under the principle of accountability, actually it is the data controller that shall demonstrate its compliance with GDPR.

B) Example: Practical difficulties for obtaining a copy of its data

1) Obstacle of the enjoyment of the data subject rights

Nowadays, the enjoyment of data subject rights remains an issue because of the fact that ICT sector is making the exercise of such rights difficult, notably the exercise of the right to request access. Amazon EU was found to refer to the right to request access to personal data only in a footnote to a section in its privacy notice called *'What choices do I have'*. The notice does not contain any reference to the right to obtain a copy of personal data. According to the researchers[294], "*it is not easy to exercise the right of access: individuals either have to read through a long privacy notice (itself hidden in very small print at the very bottom of the site) to get information about this right, or try to find it through the 'Help & Customer Service' section"*. After several click-throughs and drop-down menus with multiple choices people are finally led to a way to request 'all your data' via email'. Amazon replied within one month which is positive in regard to GDPR, but researchers did not contend that Amazon EU supplied all the data which it is likely to hold. Indeed, when it has been asked to Amazon, if that was all the data Amazon processes about them and if that were only those, they were entitled to under the GDPR? It replied that the organization has provided to the researchers all the data that was stored about them with the timeline determined by the GDPR legislation[295]. Yet, in the light of Article 15(3) of the GDPR, it seems that the

[293] GDPR 2016, s art 17(1)(C) and art 18 (1) (d)

[294] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) 28

[295] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) 28

company is not fully complying with the provision set in GDPR. Indeed, Amazon has provided a copy of personal data but only concerning the ones stored, while it has remained silent concerning the undergoing processing of personal data[296].

Regarding Netflix, the researchers found difficult to request their personal data. Indeed, Netflix refused to process the request of access, arguing the necessity for any individual to justify their identity by providing proof of identity. First of all, it is true that GDPR allows companies, in case of reasonable doubts, to ask individuals additional information to confirm the identity of the data subject[297]. In this case, the researchers provided Netflix with the last four digits of a prepaid debit card, plus mobile number registered at the time of opening the Netflix account. All of these elements should be taken into account when assessing the justification of proof of identity. Indeed, GDPR has stated that insofar the identification of individuals is important for protecting personal data against unauthorised disclosures, the identification requirements and process should be proportionate and not act as a barrier to such an important right[298]. Having, as a policy, the requirement to disclose personal data only after the issuing of a government ID with data and birth included, while other proofs of identity have been released, can be considered as a barrier to exercise the right of access. Regarding Spotify, it let individuals to have only access to a copy of data under the right to portability[299]. It was silent on the right to obtain a copy of the personal data undergoing processing as required by the article 15 of GDPR.

2) The applicability of the data retention

As discussed in paragraph I.B.2 of this chapter, GDPR prohibits organizations from keeping personal data longer than is needed for a lawful purpose. Furthermore, as information provided, they must justify the retention of personal data[300]. Based on the research conducted, none of the investigated companies appear to comply with the obligation to set out the "period for which ... personal data will be retained."[301].

---

[296] Ibid

[297] GDPR, s art 12(6)

[298] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) 29-30. See also, GDPR 2016, s recital 63

[299] Spotify, *Privacy Policy,* (Spotify 2020) See section related to 'What we use your personal data for''.

[300] GDPR 2016, see art 12(2)(a)

[301] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) 31

All three are ambiguous and use generic statements to the effect that they may keep data for as long as it is required or permitted by law. They variously invoke continued use of services, tax or accounting purposes, billing or records and fulfilling 'purposes described' in their privacy notices. None of the companies specify the periods for which they will keep personal data. Moreover, successful access requests made to Amazon EU, Netflix EU, Spotify EU for copies of access personal data revealed that the companies may keep certain behavioral data from the moment an individual opens an account. Spotify, for example, clearly states in its privacy notice that it will retain the personal data "for as long as you are a user of the Spotify. For example, we keep your playlists, song library, and account information"[302]. To conclude, all of these 3 companies make it impossible to determine the specific purposes why they can store personal data.

[302] Spotify, *Privacy Policy*, (Spotify 2020) See section related to' Data retention and deletion'

Conclusion: Recommendations to improve the GDPR

GDPR has indeed strengthened the protection of personal data, in particular by laying down obligations of companies to make the processing of personal data more transparent. Although transparency is the cornerstone of GDPR, it still needs to be better enforced in order to be fully implemented. Data controllers must indeed take responsibility for the dissemination of personal data, notably in the design of their system in charge of processing personal data. Thus, to be better enforced, GDPR needs to increase the liability of data controllers, in particular by applying more strictly the transparency rules and by giving priority to the protection of privacy by design. Furthermore, it is also necessary to strengthen the rights of data subjects. This is why the thesis argues for the need to reduce the dissemination of personal data and to protect more personal data, in general.

Nowadays, the ICT sector uses privacy policy to comply with the requirement of providing information as set out by Article 12, 13, and 14 of GDPR. Yet, it seems that the compliance of these articles is insufficient, notably because the information provided is not very readable. As a result, this places the user in a vulnerable position due to his/her lack of understanding of big data's subtle. Indeed, many authors criticize the fact that longer sentences and words are harder to be understood than shorter ones[303]. Moreover, GDPR set outs that for any processing of personal data, ''*the data controller shall provide any information due to the processing of the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language* »[304]. Thus, it is clear that the use in privacy policies of longer words and sentences should not be understood as a concise, transparent, intelligible, and easily accessible form, using plain language. Indeed, the EU data protection authority carves out what should be interpreted by the understanding "concise, transparent, intelligible and easily accessible, using clear and plain language". First of all, a "concise and transparent" manner means that data controllers must present the information effectively and succinctly in order to avoid information fatigue. This information should be clearly distinguished from other non-privacy related information such as contractual provisions.[305] Secondly, information is only intelligible if it can be understood by the intended audience.

[303] Singh, R. I., Sumeeth, M. and Miller, *A User-Centric Evaluation of the Readability of Privacy Policies in Popular Web Sites* (Springer 2011) 501-514

[304] GDPR, s art 12

[305] Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017] 7-15

Thus, the data controller must know the composition of his/her target audience and ensure the level of understanding of the average member[306]. Thirdly, 'easily accessible' means that the data subject must not seek to find information on the processing of his/her personal data. Data controllers must signpost the user in order to make the information apparent[307]. Finally, the need "for clear and plain language" means that the information should be provided in the simplest possible way, avoiding complex sentence and language structures. The information must be concrete and definitive; it should not be formulated in abstract or ambivalent terms, nor should it leave any room for different interpretations. In particular, the objectives and legal basis for the processing of personal data must be clear[308]. The readability of privacy policy plays a role in assessing the compliance of ICT sector towards the principle of transparency. Indeed, EU Data Protection Authorities recognize the role of readability testing and advised that if organizations "*are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/notices/ policies, etc., they can test these, for example, through mechanisms such as user panels, readability testing"*[309]. Thus, in order to increase compliance in the ICT sector, a readability threshold should be determined. It will have two effects. Firstly, it will increase confidence among consumers/users, mainly because the more readable information is, the more users will entrust their personal data to businesses. In addition, it will set a standard for all businesses and make the transparency requirement more understandable for businesses themselves, but also consumers/users. Indeed, companies will use this standard to revise their privacy policies to make them more readable. Users will have more transparent information and will be able to exercise their rights more easily. This standard can be seen as a readability mark that all companies must meet in order to comply with the GDPR.

A new idea has emerged to protect personal data as enshrined by GDPR. It is 'the data protection by design'. It was internationally accepted at the 32nd International Conference of Data Protection and Privacy Commissioners, held in Jerusalem in 2010, with the adoption of the "Resolution on Privacy by Design"[310]. This resolution aimed at recognizing the need to include, within ICT Sector, privacy

[306] Ibid

[307] Ibid

[308] Ibid

[309] TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD, 2020) 13

[310] AEPD, *A guide to Privacy by Design* (1edn, AEPD 2019) 5

principles that are conceived and designed in line with EU data protection from the outset. Furthermore, the resolution also invited Data Protection Authorities to actively work on and promote the inclusion of 'privacy by design' in policies and legislation on data protection within their respective States[311]. Besides, the GDPR also includes within its provisions the possibility of considering privacy requirements from the first stages of product and service design into data protection regulations[312]. Indeed, it offers to individuals the guarantee to integrate their rights and freedom relating to the processing of their personal data from the early development stages of systems and products.[313] Thus, it can be understood as the need to consider privacy and the principle of data protection from the inception of any type of processing. Moreover, it incorporates personal data protection throughout the life of an object and it involves not only the application of measures for privacy protection in the early stages of the project ,but also to consider all the business processes and practices that process associated data, thus achieving true governance of personal data management by organizations[314]. In any case, such 'privacy design' will enforce GDPR rules. Firstly, the privacy by design allows any system or process or infrastructure to provide all information needed to data subject rights in order to demonstrate diligence and accountability before the data protection authority, and it is designed from the beginning by identifying possible risks to the rights and freedoms of the data subjects and minimizing them before they can cause actual damage[315]. Rather than imposing an unreasonable burden upon data subjects to monitor their own data through company practices, the privacy by design neutralizes or minimises risks instead of corrective measures to resolve security incidents once they have occurred[316]. The inaction of users must not imply a reduction in the protection offered by GDPR or a breach of personal data. Secondly, "privacy by design" will give the user the highest possible level of privacy because personal data are protected in any system, application, product, or service. Establishing a default setting that guarantees all rights and freedoms of data subjects will ensure that the privacy of individuals is protected to the maximum extent possible. Thus, if the subject does not modify the setting, their privacy is

---

[311] Ibid

[312] GDPR 2016, s art 25

[313] AEPD, *A guide to Privacy by Design* (1edn, AEPD 2019) 5

[314] Ibid p6

[315] Ibid

[316] Ibid

guaranteed and must remain intact, as it is integrated into the system and constitutes the default setting[317]. Thirdly, privacy, and more specifically, the protection of personal data needs to be embedded into the design of a system that aims to collect personal data. It needs to include all systems, applications products, and services, as well as the business practices and processes of an organization. It can be summarized as a *"privacy design thinking"* perspective[318]. Fourthly, privacy by design can be used to reach an optimal balance between the legitimate interest of companies and the rights and freedoms of users. This is the reason why it is important to integrate such design at every stage of data processing in order to analyze each case and take appropriates measures, such as early pseudonymization or anonymization techniques or the safe and guaranteed destruction of the information at the end of its life cycle[319].

Nowadays, it is difficult for data subjects to limit or prevent the massive tracking and data sharing going on within ICT sector. There are only a few alternatives for users to prevent tracking in web browsers. Yet, most of them are not effective because those "barriers" still allow data collection and tracking[320]. Due to the complexity and the overarching lack of transparency, consumers are more or less powerless to prevent the harms that the system facilitates or makes possible[321]. Indeed, by notably using as legal basis the legitimate interest which allows companies themselves to assess the balance between their legitimate interest and the rights and freedoms of data subjects, it seems to make it inevitable that personal data will end up into the database of hundreds of companies that individuals have never heard of[322]. As demonstrated by the cases of Amazon, Netflix, and Spotify, consumers/users need to spend an unreasonable time to read and to understand privacy policies. Moreover, it is often impossible to know which data are linked to the legal basis used by ICT sector, or which personal data may be used and shared[323]. In this sense, there are number of individual and collective harmful effects can be pointed

[317] I AEPD, *A guide to Privacy by Design* (1edn, AEPD 2019) 7

[318] Ibid p8

[319] Ibid p9

[320] Øyvind H. Kaldestad. Forbrukerräde. *Out of control*. 2020. P179

[321] Ibid

[322] Ibid

[323] Ibid. See also TACD and European Union: *Privacy in the EU and US: Consumer experiences across three global platforms*. 2020

out[324]. Individual harm can happen when it affects a particular consumer, and such collection of data from the latter will produce a negative effect, such as being excluded from certain services or receiving higher prices for products or services. Collective harm arises from the indirect effects on society or groups of consumers as a whole. For example, if online surveillance has the effect of dissuading individuals from looking for information online, this creates collective harm to society over time because public debate may become less informed[325]. All of these harmful effects upon consumers/users have been outlined in many recent studies[326]. For instance, consumers are particularly concerned about their location being tracked. For example, a 2018 study showed that 75-80% of respondents felt vulnerable when their location data were shared[327]. Similarly, 69% of respondents agreed with the statement "It should become more difficult to store personal data that can be used for creating digital profiles", while only 11% disagreed[328]. The unlimited spread of personal data occurring across ICT sector may lead to harm to individuals, to impact on their trust in the digital economy and in the democratic institutions[329]. Finally, it seems relevant to arguing if the effects of the spread of personal data is a price worth paying to have personalized content and advertising[330].

As being said above, the unlimited spread of personal data mainly based on legitimate interest undermines the enjoyment of data subjects' rights. Yet, even though since the adoption of GDPR, each EU member state has a national data protection authority whose aim to enforce the GDPR and can put fines to companies that are not complying with the regulation[331], regardless of its size. Actually,

---

[324] Øyvind H. Kaldestad. Forbrukerräde. *Out of control*. 2020. P179

[325] Øyvind H. Kaldestad. Forbrukerräde. *Out of control*. 2020. P43

[326] Ibid

[327] Ibid. See also "Privacy and Location Data: Global Consumer Study March 2018", HERE Technologies - https://www.here.com/sites/g/files/odxslz166/files/2019-02/HERE%20Technologies%20Privacy%20and%20Location%20Data%20Global%20Consumer%20Study%20March%202018%20-%20Reviewed.pdf

[328] Øyvind H. Kaldestad. Forbrukerräde. *Out of control*. 2020. P43. See also, "Nordmenn og deling av persondata", Norwegian Computing Center - https://www.nr.no/sites/default/files/files/NR-Rapport_Nordmenn-og-deling-av-persondata_ALerT2019.pdf. P63

[329] Øyvind H. Kaldestad. Forbrukerräde. *Out of control*. 2020. P180

[330] Ibid. For more information on how the adtech industry is influencing the internet as a whole, see "Targeted Advertising Is Ruining the Internet and Breaking the World", Dr. Nathalie Maréchal https://www.vice.com/en_us/article/xwjden/targeted-advertising- is-ruining-the-internet-and-breaking-the-world

[331] Article 83 of GDPR

investigations need to lead to concrete actions if systematic violations do not cease[332]. As pointed out by the German Data Ethics Commission, data protection authorities need to fill a legal vacuum, in particular, due to a significant lack of enforcement measures against large multinational companies that systematically break the law. Furthermore, in its latest decision, the EU Court of Justice recalls the obligations of the supervisory authorities of each EU Member State, and in particular the role of each authority concerning the illegal dissemination of personal data used by the ICT sector[333]. It is indisputable that in order to ensure the protection of consumers/users' personal data and to reduce the inconsistencies among supervisory authorities, transnational cooperation must be improved notably regarding the use of cookies and other internet-tracking technologies, which rely on the consent of the users. GDPR defines consent as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*[334]". While French, UK, and German authorities highlight that a user continuing to browse a website does not amount to that user's consent. The Spanish authority however understands that users may grant consent to the use of cookies by means of a clear and affirmative action such as, for example, clicking a button or link or scrolling[335]. Another divergence is about the applicability of 'cookies walls. These types of cookies are used by websites to deny access to users if they do not consent to all cookies and trackers present on this site. In France and Germany, cookies walls are prohibited because the user would suffer adverse consequences if they refuse to accept their presences[336]. In other words, cookies walls are considered as a sort of barrier that puts the user in a "take it or leave it" situation, where the user must choose whether to allow marketing cookies or similar tracking technologies or be denied access to the website. Spain and UK have a different approach, ICO notes that consent that is forced via a cookie wall is "unlikely to be valid." However, it also notes that GDPR must be balanced against other rights, including freedom of expression and freedom to conduct a business[337]. Concerning Spain, the data protection authority considers that as

[332] Norwegian Consumer Council, *Out of control* (Forbrukerrådet, 2020) 180

[333] Case C-311/18. *Data Protection Commissioner v Facebook Ireland and Maximillian Shrems* [2020] ECL I- 559 (''Invalidation of the EU-US Data Protection Shield '')

[334] GDPR 2016, s art 4(11)

[335] Gabriel Voisin, Ruth Boardman, *ICO, CNIL, German and Spanish DPA revised cookies guidelines: Convergence and divergence* (IAPP 2020)

[336] Ibid.
[337] Ibid

possible to use cookies wall, as long as the user is informed about it, and unless the denial from the user will lead to the situation where the data subject could not be able to exercise a legal right[338].

Besides, the European Union needs to adopt further additional protections regarding personal data in order to fight the tracking of consumer behavior on online platforms. For example, by modernizing the ePrivacy Directive which among other things, regulate how companies can access information on consumers end devices[339]. Consequently, the adoption of a strong Regulation on Privacy and Electronic Communications which would include the concept of privacy by design, combined with effective enforcement, will particularise and complement the GDPR by protecting consumers from online tracking and profiling[340].

[338] Norwegian Consumer Council, *Out of control* (Forbrukerrådet, 2020) 181

[339] Ibid

[340] Ibid

Global Campus Europe

BIBLIOGRAPHY

BOOOK

Hildebrandt, Gutwirth, *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008)

Gonzàlez Fuster, *The emergence of Personal Data Protection as a Fundamental Right of the EU* (1edn, Springer 2014)

Orla, *The foundation of EU data protection law* (Oxford University Press 2015)

Guidelines

Human Rights Council, *the UN Guidelines Principles* (United Nations 2011)

HRB and SHIFT, *ICT Sector Guide on implementing the UN Guiding Principles on Business and Human rights* [European Commission, 2011]

CNIL, *Guide for Processors* [CNIL 2017]

CNIL, *Guide sécurité des Données Personnelles* [CNIL 2018]

CNIL, *Analyse d'impact relative à la protection des données* [CNIL 2018]

Regulation 2016/679 *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects''* [European Commission, 2019]

Regulation 2016/679 *Guidelines on transparency under Regulation 2016/679* [European Commission, 2017

AEPD, *A guide to Privacy by Design* [AEPD 2019]

AEPD, *A guide on the use of cookies* [AEPD 2019] Directive 95/46/EC *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'* [European Commission, 2014]

Directive 95/46/EC *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'* [European Commission, 2014]

ICO. *'Guide to the GDPR* [ICO 2019]

DSK, *Guidelines for Telemedia Providers [*DSK 2019]

Law

Regulation (EU) 2016/679 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) [2016] OJ L 119/1

Directive 2009/136/EC on the processing of personal data and the protection of privacy in the electronic communications sector [2009] OJ L337/11

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

UK Data Protection Act 2018

Loi relative à l'informatique, aux fichier et aux libertés 1978

Spanish Constitution 1978

Report

Norwegian Consumer Council, *Out of control* (Forbrukerrådet, 2020)

TACD and European Union, *Privacy in the EU and US: Consumer experiences across three global platforms* (TACD 2020)

Gabriel Voisin, Ruth Boardman, *ICO, CNIL, German and Spanish DPA revised cookies guidelines: Convergence and divergence* (IAPP 2020)