UiO : Faculty of Law
University of Oslo

The data privacy regime for legal persons in the electronic communications sector according to Directive 2002/58/EC

Candidate number: 8024

Submission deadline: December 1, 2014

Number of words: 15,765

Contents

1 Introduction

Law is a creation of humanity for humanity. However, the extreme complexity of human relations has made it necessary to invent non-human legal fictions,[1] which have included the subjects of rights and duties similar to those of human beings, which has been very useful in the improved regulation of the relations between natural persons, particularly in the field of commerce. Perhaps the most significant of these legal fictions is the invention of the legal person or corporation,[2] which, despite its physical absence in the real world, has had even greater relevance in the global economy than human beings have had. Despite the important role of legal persons, the modern world, principally through another fiction that yields tangible results—that is, cyberspace—has witnessed new dilemmas with regard to law and to the consideration of legal persons as subjects of rights. One of these quandaries has concerned whether legal persons should be recognized as subjects of rights with regard to data privacy when their data are processed by electronic means. This dilemma emerged in the mid-1990s with the advent of the Internet as a publically accessible technological tool, and it continues today, despite the fact that some laws first included legal persons as subjects of protection more than a decade ago.

In fact, even though Directive 2002/58/EC (e-Privacy Directive or EPD), which, unlike Directive 95/46/EC (Data Protection Directive or DPD), recognizes certain prerogatives for legal persons concerning data privacy, was enacted more than ten years ago (July 12, 2002), scholarship on the topic of data privacy rights for legal persons has accepted that this matter has been poorly addressed.[3] Moreover, some courts, such as the European Court of Human Rights (ECtHR), have affirmed that "case-law on the protection of data and information systems is limited."[4] Thus, these issues—that is, data privacy for legal persons and data privacy in the digital context—continue to require innovation. Our purpose in this paper is to discuss the data privacy regime for legal persons in the electronic communications sector according to the

[1] See Knauer (2010), pp 1, 3, 9, 17, 18 and 38

[2] Schane (1987), p 563

[3] Bygrave (2014), p v

[4] Bernh v Norway, p 40

EPD and to attempt to clarify how this regime was established and what potential benefits and risks may now be facing the information society.

Our main aim is to discuss the regime established by the EPD for legal persons and then to reflect on various points concerning these juristic entities in the field of data privacy, particularly as it relates to the digital context. This aim arose principally because we detected that the controversy over whether legal persons should be considered data subjects, and thus be protected under data privacy rules, continues even today although the EPD, which included legal persons as subjects of protection, was enacted more than ten years ago. Nevertheless, perhaps because of the polemic point of whether legal persons should be data subjects for data privacy purposes, this regime of protection raises questions that could represent severe challenges and uncertainties for legal persons, as well as for providers of electronic communications services. Hence, our objective is to discuss these issues and attempt to define a better perspective on the EPD, which would be comprehensible enough to allow us to form an opinion about the sufficiency of the dispositions facing the information society.

This paper is particularly important from the perspective of the providers of electronic communications services regarding their subscribers' legal persons (as we have mentioned above, scholars and judges have said little about their prerogative to data privacy in a digital context). Indeed, we consider that those providers are major subjects that must obey the national legislations that European Union (EU) Member States enact based on the EPD. However, this paper focuses only on the data privacy regime for legal persons established by the EPD without referring to any national legislation in particular because our purpose is to discuss the main reference of rules on electronic privacy for legal persons in the EU, which is the EPD, and because a discussion of national legislations that have implemented this directive is beyond the limits of this paper.

Lastly, it is important to mention that we acknowledge the current proposal for a "New EU framework for protection of trade secrets," which mainly "aims at making it easier for national courts to deal with the misappropriation of confidential business information, remove the trade secret infringing products from the market and make it easier for victims to receive compensation for illegal actions."[5] Nevertheless, we do not address this proposal in this paper

[5] Council of the European Union (2014-2)

because, first, it is still a legal draft and is neither definitive nor in effect; second, our focus is on the data privacy regime for legal persons when their personal data is processed by electronic means. However, because this current proposal is related to the protection of undisclosed know-how and business information against their unlawful acquisition, use and disclosure, we consider that it concerns intellectual property law, commercial law, and civil law.[6] Third, the scope of this paper is limited and the comments on this draft may well lead to a separate paper. Nevertheless, the proposal of this new directive demonstrates that businesses—most of which are incorporated legal persons—also deserve attention regarding their privy information because EU lawmakers are worried about their protection.

1.1 Questions and problems considered

The main question addressed in this paper concerns whether the data privacy regime established in the EPD for legal persons is adequate. Accordingly, we will consider the role of diverse dispositions related to legal persons in the EPD, and we will discuss these dispositions with the purpose of revealing their potential benefits or risks for the electronic communications sector in the EU and for the information society.

We consider six issues in order to question the adequacy of the EPD regarding legal persons.

First, the EPD employs at least three concepts such that each appears to refer to something different. These concepts are privacy, personal data protection, and legitimate interest. A question then arises concerning whether there is any difference between these concepts, which are very important for the conception of data privacy. A related question concerns the consequences that could delimit the data privacy regime for legal persons (mainly because the controversy over whether legal persons are subjects of privacy continues).

Second, the absence of the recognition of legal persons within the Data Privacy Directive, which is the benchmark of the EPD, leaves doubt regarding the recognition of legal entities in this directive. However, another question concerns the point at which legal persons are recognized within the EPD and whether it is possible to discuss real rights holders or not.

[6] See Council of the European Union (2014), pp 2, 3, 9, 10, 11, 17, 25, 26 and 39

Third, the scope of the EPD regarding legal persons was established in order to protect these entities with regard to the processing of their personal data. This protection exists when the entities comply with two cumulative criteria: acting in the electronic communications sector and doing so under the role of subscribers. There is then a limitation stipulating, not only the sector in which the data privacy is recognized for legal persons (namely, the electronic communications sector) but also, with respect to this restricted sector, data privacy for legal persons is only recognized when they are acting as subscribers. We estimate that these kinds of constraints could result in complications in implementing the law, while also providing weak protection for legal persons in the e-communications sector.

Fourth, though the EPD provides for the protection of the legitimate interests of subscribers who are legal persons, these legitimate interests are not clarified in the EPD. Thus, they remain undetermined concepts, which could represent nebulous points for the implementation of the Directive and obstruct harmonic legislation in the EU because of the liberty that Member States could take in embodying the concept within their national legislations.

Fifth, two more potential risks to harmonization in the EU exist. Indeed, although article 1(1) of the EPD states that "This Directive provides for the harmonization of the national provisions required to ensure an equivalent level of protection," articles 12(4) and 13(5) establish that the European lawmaker may leave to the discretion of the Member States the protection of the legitimate interests of legal persons that are subscribers, with regard to their entry into public directories and their protection against unsolicited communications transmitted by electronic means. Hence, this legislative discretion of Member States appears a source of non-uniform regulation that could oppose the main objective of harmonization of the EPD, and it could thwart the general purpose of legal harmonization in the EU, at least with regard to topics that we consider relevant with respect to personal data processing in the electronic communications sector and to ensuring the free movement of such data in the EU.

Sixth, considering that the EPD was enacted with the purpose of adapting and complementing the DPD with respect to the e-communications sector, there is a close relationship between both Directives (i.e., the EPD and the DPD). The latter Directive mainly refers to the former. Hence, taking into account the disposition in the DPD (articles 1(1) and 2(a)), whose content refers only to natural persons, and the statement in recital (12) of the EPD, which states that Member States are not obliged to extend the DPD provision to the protection of the

legitimate interests of legal persons, it has complicated the EPD's application to legal persons in certain cases that involve or refer to the DPD dispositions. Thus, the certainty of data privacy protection for such legal persons is questionable.

1.2 Overview of chapters

This paper is divided into seven chapters. In the first chapter, in addition to this brief description of the paper's contents, we present some preliminary points in which we give a very broad idea about this work on the dilemmas posed by cyberspace with regard to law and to the consideration of legal persons as subjects of data privacy rights. In the section on questions and problems considered, we pose the primary and secondary research questions, as well as the problems that we will tackle. Lastly, in this first chapter, we provide a brief description of the method that we use to approach the topic.

In the second chapter, we review the conceptual references, that is, the benchmarks against which the subsequent topics may be compared or assessed. Specifically, in this second chapter, we present a broad perspective on the main points that a law should cover in order to be adequate regarding the context of this study, namely, the EU and cyberspace. Moreover, we discuss the concept of data privacy in order to explain that we prefer this label because it synthesizes the ideas of privacy and data protection.

In the third chapter, in order to gain a better perspective on our principal legal point of departure—the EPD—we discuss its background, scope, and aim (which could be relevant to understanding the real influence of the Directive on the data protection regime of legal persons in the electronic communications sector). We then address the concepts included in the EPD regarding data privacy (which could be very useful in determining whether any definition best suits legal persons, which are our main subject). Finally, we explore the manner in which it recognizes legal persons.

In the fourth chapter, we analyze the two main requisites that a legal person must meet to be considered a subject of protection, according to the EPD. Our main purpose is to discover the situation that legal persons face with regard to the EPD and to determine the existence of any barrier to their access to protection regarding their data privacy.

In the fifth chapter, we discuss the rules that are considered the most controversial for legal persons in the EPD. This part considers evidence that certain provisions of the EPD actually hinder the adequate data privacy protection of legal persons, both in the EU and in a digital context.

Lastly, the sixth and the seventh chapter provide, respectively, our conclusion and the list of references that we consulted.

1.3 Method

This paper focuses on the data privacy regime established by the EPD with regard to legal persons. Hence, our main source of reference is the EPD itself. We will also consider related doctrines and cases, if they exist. It is noteworthy that these cases could refer to the right to privacy stated in article 8 of the European Convention on Human Rights (ECHR), which, although different from the EPD, is related to it regarding the issue of privacy.

We write this paper from a *lege lata* perspective of the EPD. Namely, we discuss the state of the current law, attempt to detect its potential advantages, and its potential risks. Finally, we dare to give an opinion about whether the EPD is sufficient with respect to the regime it has established for legal persons or not.

2 Conceptual references

Given that our main research question concerns whether the data privacy regime established in the EPD is adequate[7] and that we assume a *lege lata* approach to discussing the current state of the EPD,[8] we should state a point of reference that both helps us to answer the research questions and complies with our approach. Thus, in this chapter, we look at the concept of *adequacy*, exploring diverse perspectives with the purpose of clarifying the implications of this concept regarding the EU directive that established a regime of data privacy, which is extremely relevant in the information society.

Additionally, we consider that the group of dispositions concerning the protection of the fundamental right to privacy in the new circumstances of the information society has been denominated as privacy law (mainly in the United States of America (US)) and as data protection law

[7] *Supra*, section 1.1

[8] *Supra*, section 1.3

(mainly in the EU), which are the most influential legislations worldwide regarding this subject. In this chapter, we explain the reasons that we chose the label of data privacy for this paper.

2.1 Adequacy concept concerning an EU directive for the information society

The Merriam-Webster Dictionary defines *adequacy* as "the quality or state of being adequate,"[9] and it lists various synonyms that could be useful to an understanding of the concept: "acceptability, sufficiency, satisfactoriness."[10] Regarding the adjective *adequate*, the same dictionary states that it means "enough for some need or requirement"[11] and that its synonyms are "acceptable, all right, decent, fairish, fine, good, OK (or okay), passable, respectable, satisfactory, serviceable, tolerable."[12] From a semantic perspective, the concept of *adequacy* implies an idea concerning the minimum elements necessary to comply with a certain purpose. That is, it signifies a situation in which the circumstances are sufficient to reach a certain condition. It could also be understood that less than the minimum of elements would represent the failure to accomplish the certain purpose, while more than the minimum of elements would imply the superior fulfillment of the purpose.

We can also state that the concept of *adequacy* is adaptable to the desired purpose. Namely, *adequacy* depends on the desired objective according to which the elements minimally required to consider the desire fulfilled should be analyzed. Thus, to know what is adequate with respect to a certain situation, it is necessary to propose an ideal target, based on which the minimum circumstances to consider the ideal achieved are established.

From a legal perspective, Black's Law Dictionary states that *adequacy* signifies "being legally able to complete a requirement."[13] With respect to *adequate*, the same dictionary establishes that it means "sufficient; proportionate; equally efficient."[14] As we can see, there are no exact, legal definitions of *adequacy* and of *adequate* law. This is perhaps because, as stated above, the concept of *adequacy* is functional; that is, it describes the sufficiency of something

[9] "Adequacy" in the *Merriam-Webster Dictionary*

[10] *Idem*

[11] "Adequate" in the *Merriam-Webster Dictionary*

[12] *Idem*

[13] "Adequacy" in *Black's Law Dictionary*

[14] "Adequate" in *Black's Law Dictionary*

in relation to the desired aim, through that which is described as adequate or not. Accordingly, to clarify the legal concept of *adequacy*, it is necessary to have at least a broad idea about what the goal of law is. Similarly, it is necessary to establish the target of a certain legal issue in order to clarify whether its specific circumstances are *adequate*.

Hence, in reference to the goal of the law in a very broad sense, we can say that "law's purpose is to order society by influencing humans to behave in socially desirable ways."[15] Given this target, the concept of *adequacy* could be extremely broad, and its treatment is beyond the scope of this paper. What we can say considering this extensive objective is simply that a law is adequate if it is able to influence its subjects to behave in the way that lawmakers envisioned as the minimum suitable behavior in achieving a desirable reality, according to the particular circumstances of a community.

In order to build a strong point of reference for this paper and to obtain a narrower definition of *adequacy*, we tackle the characteristics that we consider the minimum for an EU directive to be adequate. After that, we discuss the features of a law that is adequate for the information society, which we think is the quintessential objective, which current lawmakers should have in mind when enacting data privacy laws.

The EU is a political-economic integration that operates by means of a system of supranational independent institutions and intergovernmental negotiated decisions by the member states.[16] Moreover, in addition to the Euro zone, it is considered the major model of economic integration in the world,[17] and the main target of its legislation policy is coherence. That is, EU legislation should promote the construction of a single market.[18] To accomplish this goal, its legislation is based partly on a system of directives the mission of which is to foster legal harmonization among the Member States.

This means that the EU directives provide a benchmark on which the Member States must base and enact their legislation. These individual legislations should be consistent with one another in order to be considered adequate to promote the single market that the EU

---

[15] Reed (2012), p 179

[16] Gabel (2014)

[17] Burges (2013)

[18] Walden (2013), p 144

claims to be. Accordingly, we consider that a directive should have two principal features in order to be adequate: clarity and impartiality.

Indeed, given that the EU is a group of countries with different cultures, EU directives should be clear to all of nations and thus enable implementation for everyone. It follows that an important characteristic of an EU directive is having content that is understandable in the same way by all Member States. This can be difficult to achieve because the different languages in the EU represent a challenge in communication, especially when certain expressions do not have equivalences or are multivalent across languages.

Similarly, the different cultures within each Member State can also represent a challenge because law is influenced by culture. Hence, each country has what is called a legal tradition.[19] Thus, a EU directive should be not only clear in the sense mentioned above but also impartial. Namely, it should defer to the legal tradition of each Member State, which means respecting the legal features of each Member State without giving preference to or fostering certain legal traditions over others.

With respect to cyberspace (i.e., "the 'location' in which people [interact] with each other while using the Internet"[20]), the processing of personal data—which is the focus of this paper although cyberspace can involve many other issues—is not a new activity. Instead, it has been always present in human interaction, but since the emergence of the welfare State, it has had a major role in governmental agencies. Nevertheless, in recent years, personal data have come to play a very significant role in our information society, such that they have even been called "the new oil."[21] Consequently, legislation on data privacy has been criticized for not being adequate for the context of cyberspace.[22]

Hence, it has been argued that the law should be revisited, with the aim of adjusting its suitability to cyberspace. Accordingly, we believe that there is a twofold perspective on analyzing the law as a suitable influence on cyberspace. These two perspectives are related to the creation and the structure of law, on the one hand, and to the content of law, on the other hand.

---

[19] Carozza (2014)

[20] Busell (2013)

[21] Bygrave (2014), p 4

[22] See, for instance, Reed (2012), pp 130 *et seq*

With regard to the creation and the structure of law, which we identify as the external aspects of law, and without considering the law's content, it has been stated that with respect to cyberspace, lawmakers must take into account that users are not influenced by the enforcement of law. Such enforcement is almost impossible to achieve through coercive, traditional means. However, users obey the law because they respect it, and this respect depends on three aspects: the consideration by users that lawmakers have authority over them; the consideration by users that the aims of these lawmakers are also desirable to them; and the consideration by users that compliance to the law is likely to achieve these aims. In summary, lawmakers should develop a persuasive process that convinces cyberspace actors that they have the authority to regulate certain activities in cyberspace.[23] This is relevant for both legal persons and the providers of electronic communications services. Because they are legal fictions, those who create and operate such services are flesh-and-blood individuals who are directly influenced by law.

Concerning the content of law, the cyberspace environment has highlighted the importance of certain characteristics that must exist in a law for it to be considered adequate. These features can be summarized in the idea that since "the scope of a lawmaker to impose its will on cyberspace actors is extremely limited, so that by and large laws work (if at all) in cyberspace because actors accept their normative force and thus obey them,"[24] a law should be understandable; that is, it should be a meaningful law. To create such a law, lawmakers should avoid making overly complex, contradictory, and precise laws.[25] Indeed, it has been suggested that "a law whose text makes its normative aims clear, in as simple a manner as is possible, is more likely to be respected than one which attempt to impose a multitude of precisely defined obligations whose connection with the law's aims is obscure."[26]

Thus, in legal terms and according to the circumstances of the information society, the concept of *adequacy* represents a very simplified law that is easily understandable by its recipients and that reflects the present social norms, which are highly influenced by the cyberspace

---

[23] Reed (2012), pp 68, 178, 179 and 188

[24] *Ibid*, p 129

[25] *Ibid*, p 129 *et seq*

[26] *Ibid*, p 149

usage.[27] Hence, such a law is respected and followed by users, which in our context are primarily the providers of electronic communications services and secondarily the users and subscribers of those services.

Consequently, the concept of *adequacy*, with regard to an EU directive facing the information society, relates to two things. First, it implies a clear and deferential legal rule, the content of which can be understood in the same way by all of the Member States, and it respects the legal features of each Member State, without giving preference to or fostering certain legal traditions. Second, it refers to a legal rule that reflects the present social norms—one that recognizes and respects even new uses and customs, as dictated by netizens, and that is simple enough for its recipients to grasp its meaning easily. In these two ways, a law can achieve respect and observance by users, who in our case are mainly the individuals that conform to and operate the providers of electronic communications services. It can also conform to the processing and protection of the personal data of legal persons because those individuals must to comply with the national legislations enacted by EU Member States, based on the EPD.

2.2 Data privacy

The concept of data privacy traditionally refers to "a body of law that is specifically aimed at regulating the processing of data on individual natural/physical persons,"[28] although it has sparked a discussion concerning whether it could include the processing of data for legal persons. We believe that this concept of data privacy does include juristic persons because, as is the case in this paper, the EPD considers legal persons to be subject to any protection. Thus, in a certain regard, an EU rule has already surpassed the aforementioned discussion and recognized legal persons as subjects of protection.

The primary purpose of this legal body is to safeguard the privacy-related interests of data subjects, particularly with regard to data about and from them being processed by others.[29] This makes the key role of this subject matter more understandable with regard to the

[27] Reed (2014), p 169

[28] Bygrave (2014), p xxv

[29] *Ibid*, pp xxv and 1

information society: that is, through technology, it is possible to process, in a very broad sense, extensive amounts of data about and from any person.

In fact, as more and more data are collected, created, compiled, and stored through information and communication technology, the ability of persons decreases, with regard to knowing how to control the dissemination of such data. Thus, data privacy law aspires to empower the subjects of data with the ability to recognize their own rights, to determine the data that are being held, to know how their data are being processed, to correct their data if they are wrong, and most importantly, to decide whether their data can be collected or not.[30] Consequently, we can see that this discipline of law revolves around the concept of personal data, which complicates the matter, since this concept, as scholars have stated,[31] is pragmatic and depends largely on the circumstances of each particular case.

As we have previously stated, this area of law is also known under other names, such as data protection law (which is a common name in Europe) and privacy law (which is a common name in the US and other non-European countries). However, the term data privacy has been increasingly used, because it is considered to provide a more suitable description of the law's content. Moreover, it reflects not only the notion of information control (which is implicit in the data protection concept) but also a broad idea of personal integrity, which can be understood from the concept of privacy. Finally, the term data privacy synthesizes both European and non-European perspectives.[32]

Finally, although the need to tackle the meaning of the concept of privacy seems obvious, we are not going to do so in this paper for two reasons: first, the purpose of this paper is not to answer the question of what privacy signifies; second, answering this question is not an easy task because it could require a great amount of deep reflection.[33]

---

[30] Edwards (2009), p 451

[31] *Ibid*, p 458

[32] Bygrave (2014), pp xxv, 28 and 29

[33] Raab (2014), p 39

3 The e-Privacy Directive

This part briefly introduces the EPD. First, we describe the origin of the EPD and discuss its purpose of aligning law with the new trends of the information society, mainly the electronic communications sector, which was previously considered a telecommunications issue. Second, we briefly discuss the scope and aim of the EPD in order to clarify the main purpose of this Directive with respect to legal persons. Third, we discuss the contents of the EPD with regard to the concepts of both data privacy and the protection of personal data such that they could generate various uncertainties and difficulties in the implementation of their dispositions. Fourth, we seek to explain the EPD's inclusion of legal persons as data subjects, albeit in an uncertain manner and to show that DPD establishes the dispositions that are directed only to natural persons.

3.1 Background

On December 15, 1997, Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector was enacted. However, as soon as it was adopted, it was already out of date because, from the middle of the 1990s, the Internet and electronic communications were already in frequent use. Hence, because EU lawmakers wanted to remove the uncertainty of whether Directive 97/66/EC also applied to the Internet and e-mail, they decided to repeal this Directive and adopt a new one, which included the then-new issues surrounding the Internet and electronic communications.[34]

In reality, it was thought that the successful development of information society services—which, since the middle of 1990s had been an established fact with clear and great potential—was largely dependent on the confidence of users that their privacy and information would not be put at risk. Thus, a legal framework was needed to protect the rights of natural persons, as well as the legitimate interests of governments and legal persons.[35]

Hence, the proposal of the EPD was included in a larger package of telecommunications directives aimed at strengthening competition within the EU electronic communication market. The main purpose of EU lawmakers was to improve privacy rights for individuals,

[34] Debusseré (2005), pp 72-73

[35] *Ibid*, p 72

while paying attention to the legitimate interests of legal persons by extending the protections for telecommunications, which were already in place, to a technology-neutral category of electronic communications.[36]

Therefore, the EPD, which was enacted on July 12, 2002, "forms part of the 'Telecoms Package', a new legislative framework designed to regulate the electronic communications sector and amend the existing regulations governing the telecommunications sector."[37] It is important to note that this "Telecoms Package" included four additional directives concerning general frameworks, access and interconnection, authorization and licensing, and universal services. Moreover, this package was amended in December 2009 by two directives concerning better law making and citizens' rights, as well as by the establishment of the Body of European Regulators for Electronic Communications (BEREC).[38]

3.2 Scope and aim

Article 1 of the EPD establishes the scope and aim of the Directive. The first paragraph of this provision clearly states the aim of the EPD, as follows: it "provides for the harmonization of the national provisions required to ensure an equivalent level of protection of… the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector." However, the scope of the Directive requires deeper analysis.

The main reference to the scope of the EPD occurs in the second paragraph of article 1. This disposition states that the EPD particularizes and complements the DPD regarding the aim established in the previous paragraph, while providing for the protection of the legitimate interests of legal persons when they play the role of subscribers in the electronic communications sector. Thus, the first reflection is that "The [EPD] is mainly directed towards online privacy, while the [DPD] applies broadly to privacy practices, not limited to Internet activities."[39] This perspective is useful in understanding why it was necessary to adapt the DPD and

---

[36] Bakar Munir (2004), pp 732-733

[37] "Data protection in the electronic communications sector" in *EUR-Lex*

[38] *Idem*

[39] Baumer (2004), p 402

to repeal the Telecommunications Directive, as we explained in the previous section. Specifically, this change occurred because it was necessary to bring law to the then (i.e., the beginning of the 21st century) newcomer cyberspace environment.

Hence, we can summarize the EPD by saying that it requires Member States to guarantee the confidentiality of electronic communications. Specifically, article 5 states that Member States shall prohibit listening, taping, storing, or other kinds of interception or surveillance of communications. Moreover, according to article 6, communications service providers are obligated to delete all traffic data no longer required for the provision of communications services. Nevertheless, "Member States are permitted to restrict the scope of this protection to safeguard national security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offences."[40]

The EPD is understandable because information and communication technologies—mainly Internet and electronic messaging services—require specific measures to secure that users have a right to privacy. Thus, "the [EPD] contains provisions that are crucial to ensuring that users can trust the services and technologies they use for communicating electronically."[41] Hence, the relevance of the EPD to the information society appears to be obvious because through electronic means, the risk of dissemination and abuse of personal data increases considerably,[42] which makes data privacy a paramount aim. Rules, such as the EPD, help to secure legal security and protection in the information society.

It has been recognized that among the different dispositions of the EPD, the main ones apply to spam (i.e., unsolicited communications, regulated by article 13), which state a regime of users' prior consent ("opt-in"), and to the installation of cookies (article 5(3)), which similarly follow the general principle of users' previous consent.[43] However, despite the importance of these rules in the cyberspace environment, which we discuss later,[44] with regard to spam, the EPD in article 13(5) excludes the application of its dispositions to legal persons.

---

[40] Bakar Munir (2004), p 731

[41] "Data protection in the electronic communications sector" in *EUR-Lex*

[42] Bernh v Norway, para 59

[43] "Data protection in the electronic communications sector" in *EUR-Lex*

[44] *Infra*, chapter 5

Moreover, with regard to cookies, article 5(3) defers to the DPD to regulate the consent needed to permit their installation. Thus, it is uncertain whether this protection encompasses legal persons or not because the DPD recognizes only natural persons as data subjects.

With regard to this controversy between the EPD and the DPD and the attempt to find a solution, it has been stated that the EPD concerns the regulation of two specific categories of data: location data and traffic data. That is, it concerns any data processed for the purpose of the conveyance of communications through an electronic communications network or the billing thereof. Moreover, both categories are defined without reference to the concept of personal data used in the DPD to fix the scope of application of data protection legislation.[45] Thus, it appears that even though the EPD, as its main scope and aim, has to particularize and complement the DPD, it is necessary to take some care with its scope, which could differ from that of the DPD.

Lastly, from the very beginning, it has been stated that the effects of the aim and scope of the EPD are unclear and that it is necessary to wait until the implementation of the EPD in the Member States to gain a better perspective.[46] If this is true, the problem now is that the analysis of each regulation in each Member State would be a very broad exercise, which is beyond the scope of this paper. However, the EPD's aim and scope are consistent with cyberspace challenges, mainly because we consider that this Directive maintains the principle of technological neutrality, which favors its application, despite the passage of time and the advent of technological advances. Regarding its dispositions about unsolicited communications and cookies, they are not applicable to legal persons, which in itself could be a negative aspect.[47]

3.3 The mix of concepts and the restricted concept of the data privacy of legal persons

Because the EPD uses the concepts of both privacy and personal data protection, we will determine whether there is any relation or difference between them, according to the text of the EPD. We will then discuss how the EPD states a distinction between the employments of these

[45] Poullet (2010), p 10

[46] Crichard (2003), p 303

[47] See *infra*, sections 5.1 and 5.2

concepts according to the kind of subject to which the law relates: that is, natural persons or legal persons. Finally, we will determine whether it is possible to derive a concept of data privacy for legal persons, based on the different approaches contained in the EPD.

The first reference in the EPD, which includes the concepts of both privacy and personal data protection, which we think is relevant to understanding their interaction, is recital (5). Recital (5) first states that "New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user." This extract could be understood to mean that privacy and personal data, if they can be so related, are different concepts and, consequently, refer to different things.

The above idea can be confirmed through the last portion of the same recital (5) of the EPD, which establishes that "These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk." Hence, we estimate that while the concept of personal data refers to somebody's close information (e.g., name, address, purchasing preferences, medical records, financial statements, etc.), which could be manageable through cyberspace, the concept of privacy relates to a situation of freedom from disturbance or interference.[48] Thus, personal data protection affects the level of privacy. Thus, although it may be true that the two concepts—personal data and privacy—cannot be differentiated, they are, at least, strongly related.

We could provide other examples of how the EPD treats the concepts of privacy and personal data as dissimilar but deeply related. Indeed, we have the case of recital (6), which states that "Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy." As we can see, the conjunction "and" clearly denotes that the two concepts are different. Moreover, recital (46) suggests the same idea by establishing that "The protection of the personal data and the

[48] We are not attempting to define the concept of privacy; instead, we are only trying to discuss its interaction with the concept of personal data. Moreover, as stated in the last part of section 2.2, the definition of privacy is outside the scope of this paper, largely because that definition could warrant a separate dissertation.

privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service…."

Therefore, we can confirm that when they enacted the EPD, lawmakers had in mind a distinction between personal data and privacy. We consider this differentiation to be consistent with the nature of each concept because, as stated above, while the concept of personal data implies information from somebody, the concept of privacy is broader, denoting the whole situation of a person free from any disturbance or disruption. Thus, in the case of personal data, the protection of personal data could mean, in part, the respect for privacy.

However, our question here is related to the convenience of this level of detail in the EPD, mainly because this kind of differentiation between the concepts of privacy and personal data is unlikely to be understandable to ordinary people, who are most likely not specialists in data privacy topics and who have to comply the national legislation which EU Member States enact to implement the EPD (and who, in the case of this paper, would mainly be individuals who are in charge of the processing of personal data within companies related to electronic communications services, and who, although it can be argued that they should have some knowledge about data privacy, are not necessarily lawyers specializing in this field. In addition, the law must be understandable to any individual, not just specialists).[49] Actually, this kind of confusion of concepts is even more remarkable in the case of legal persons because the EPD not only gives the idea that privacy and personal data are different but also gives the impression that the legitimate interests of legal persons, which are protected by the EPD, are different from privacy and personal data. Thus, a question arises concerning the meaning of those legitimate interests.

Indeed, recital (8) and articles 1(1) and 1(2) of the EPD establish privacy, personal data, and the legitimate interests of legal persons as three different concepts. The first states that "Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the electronic communication sector, should be harmonized…" The second notes, "This Directive provides for the harmonization of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confiden-

[49] See *supra*, last part of section 2.1

tiality, with respect to the processing of personal data in the electronic communication sector…" Finally, the third refers to the second, stating that "The provisions of this Directive particularize and complement Directive 95/46/EC [Data Protection Directive or DPD] for the purposes mentioned in paragraph 1. Moreover, they provide for the protection of the legitimate interests of subscribers who are legal persons."

Therefore, it appears that the EPD includes these three concepts as different notions and even assigns them different targets: that is, some are related to natural persons and others are related to legal persons. Therefore, it is advisable to explore these definitions further. In the following, we will discuss how the EPD allocates these concepts depending on whether a person is natural or legal.

Regarding natural persons, the EPD establishes its broadest object of protection, which is, as stated in its article 1(1), the protection of rights to privacy and confidentiality concerning the processing of personal data in the e-communications sector, as well as the assurance of the free movement of such data and of e-communication equipment and services in the community. These rights are the principal reference in understanding the object of protection in relation to legal persons: namely, their legitimate interests as subscribers of the e-communications sector. After all, as we stated above, these legitimate interests are recognized by the EPD as different from (though allied with) privacy and personal data protection.

With regard to the EPD, EU lawmakers have recognized several rights of individuals, which are deeply related to the main entitlements of privacy and data protection. Some of these rights concern the security of processing (article 4), the confidentiality of communications (article 5), the removal or making-anonymous of traffic data (article 6), the reception of non-itemized billing (article 7), the restriction of calling and connected line identification (article 8), the difference between location data and traffic data (article 9), automatic call forwarding (article 11), and so on. These rights obviously tend to safeguard personal data and ultimately (and as the main target) the privacy of natural persons. This is based on the assumption that the latter (i.e., privacy) is intimately tied to the protection of dignity and honor,

which, in Europe, is also often perceived as valuable to society in general, and to the maintenance of civility, pluralism, and democracy in particular.[50]

This broad concept of protection seems to benefit natural persons. Nevertheless, its large scope complicates the identification of the prerogatives for legal persons because throughout the EPD, there are many general references that are not explicitly clarified as being only for natural persons, only for legal persons, or for both. This imprecision makes it difficult to know the legitimate interests of legal persons with regard their data privacy prerogatives in the electronic communications sector.

The EPD recognizes certain "rights" of legal persons in relation to the protection of their data in the electronic communications sector. We state this because at least in article 1(2) of the EPD, it is possible to conclude that the legitimate interests—whatever this means—of legal persons regarding privacy and personal data protection should be protected by EU Member States.

Now, with regard to the recitals of the EPD—principally recitals (7), (8), (12) and (26)—EU lawmakers have made several precise decisions regarding the protection of the fundamental rights and freedoms of natural persons (particularly with regard to their rights to privacy and confidentiality) and of the legitimate interests of legal persons (particularly with regard to the processing of data by information and communication technologies). Hence, we assume that EU lawmakers did not wish to include legal persons as recipients of the fundamental rights to privacy and confidentiality, but only as recipients of the entitlement to the protection of personal data when data are processed by electronic means (i.e., when the respective legal person plays the role of subscriber to any electronic communication service provider). However, this right appears not to have a direct connection to legal persons because the EPD is completely clear in stating that with regard to legal persons, Member States should protect only their legitimate interests—a concept that we will discuss later.[51]

Accordingly, we estimate that the data privacy regime, when considered in a general manner, has to be particularized in the case of legal persons under the protection of the EPD. Indeed, legal persons have not been recognized fully as data subjects in the broad sense of the EPD (or the DPD). Instead, they are only recognized as holders of legitimate interests with

[50] Bygrave (2014), p 112

[51] *Infra*, section 4.2

regard to the protection of personal data by electronic means, and only when they are subscribers to an e-communications service.

Therefore, the concept of data privacy for legal persons, according to the EPD, is restricted such that a legal person can only be considered a legitimate subject of the protection of personal data when the respective legal person is playing the role of a subscriber of an electronic communications service provision. Nevertheless, the meaning of "legitimate interests" remains unclear.

3.4 Uncertain recognition of legal persons as data subjects

As we stated in section 3.2, although it appears that the EPD, as its main scope and aim, has to particularize and complement the DPD, it is necessary to take some care with its scope, which can differ from the scope of the DPD. Indeed, one of the main differences between the EPD and the DPD is that while the latter considers only natural persons data subjects,[52] the former establishes in article 1(2) that "the provisions of… [the EPD] particularise [sic] and complement [the DPD]… [and] provide for protection of the legitimate interests of subscribers who are legal persons." Thus, contrary to the DPD, the EPD does recognize legal persons, albeit in an uncertain manner and regarding their legitimate interests—an approach that we believe to be very broad and that would be problematic to implement.[53]

In fact, the entire text of the EPD does not make it clear whether EU lawmakers wanted to recognize legal persons as data subjects because the EPD's dispositions refer only to the legitimate interests of those juristic entities.[54] Moreover, there is no definition of what those legitimate interests signify. On the one hand, there is uncertainty concerning the legal nature of juristic entities before the EPD because as we previously stated,[55] if it can be certain that EU lawmakers did not recognize any right to privacy or confidentiality of legal persons, it is uncertain whether they recognized the right to the protection of the personal data of those enti-

---

[52] See articles 1(1) and 2(a) of the DPD

[53] See *infra*, section 4.2

[54] See *supra*, section 3.3

[55] *Idem*

ties. On the other hand, it is unclear whether legal persons would be entitled to personal data protection or whether they would have only legitimate interests in that regard—and, if so, what those legitimate interests would imply.

Unfortunately, in case law, the uncertainty of whether legal persons can be recognized as data subjects and thus as holders of the right to data privacy continues. If it is true that the ECtHR has stated that legal persons (based on article 8 of the ECHR) must be recognized as holders of the right to respect for home and correspondence, it is also true that the same Court has not tackled the issue regarding privacy and personal data.[56]

4 Situation of legal persons in the e-Privacy Directive

The protection that the EPD provides for legal persons is controversial not only because of the uncertainty that its dispositions leave concerning whether those entities are really holders of any rights or are only holders of legitimate interests (whatever this means) but also because EU lawmakers imposed on legal persons certain limitations regarding the protection they should receive, based on the EPD.

In fact, even under the supposition that legal persons are recognized as data subjects in the EPD, EU lawmakers imposed two more limitations on the entities protected by the provisions of the EPD. First, not every legal person may be protected by the EPD, but only those that are subscribers to any electronic communications provider. Secondly, the protection that a subscriber that is a legal person may receive is related only to its legitimate interests (whatever those legitimate interests mean). This is the restricted object of protection that the EPD considers for legal persons, which is difficult to understand.

In this section, we will to tackle the limitations that refer to the nature of the subscribers that legal persons should reach and to the nature of the object of protection provided by the EPD for those entities. Regarding both limitations, we also will discuss their potential implications.

[56] Bernh v Norway, paras 104-107

4.1 Legal persons as subscribers

In order to be protected by EPD dispositions, a legal person must play the role of a subscriber to any electronic communications service. Thus, in understanding this quality, we consider it important to know what a subscriber role implies in relation to the EPD. Consequently, in this section, we will discuss the meaning of subscriber and whether the EPD's guidelines are adequate to build a clear definition of this quality of legal persons.

First, it is noteworthy that the EPD does not provide any definition of what it means to be the subscriber to an electronic communications service provision. Although at first glance, it appears irrelevant whether the EPD gives such a definition, we suggest that it would be useful, mainly because the EPD does provide a definition of user (i.e., "any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service").[57] Thus, legal persons cannot be considered users of an electronic communications service; however, they can be subscribers to the same service. Then, regarding legal persons, we could posit the case of a subscriber to an electronic communications service that is not considered also a user. This seems an odd case and one that may not be easily understood by lay people. Hence, it is necessary to examine this further.

From a semantic perspective, which we think is the most important sense that a law should impart because a law is directed towards a certain group of people that it supposes have a common language, we can understand that a subscriber is any person who "[pays] money to get a publication or service regularly".[58] Thus, in terms of the EPD, a subscriber is any person who pays money to receive an electronic communications service regularly. It seems obvious that someone who pays to get a regular service is going to use it (at least in a certain manner or through individuals authorized by him, as in the case of legal persons, which, because their disembodiment, are unable to use a service directly; or as in the case of a parent who is a subscriber to an Internet service provision, whose children use the service) and, thus, is going to be a user of the said service. Nevertheless, for the EPD, this logic (which even is easier to understand by ordinary people who do not differentiate between a user and a subscriber) is not

[57] Article 2(a) of the EPD

[58] "Subscribe" in the *Merriam-Webster Dictionary*

valid. Indeed, as we stated above, the EPD establishes that a user is any natural person who uses an electronic communications service, regardless of whether he or she subscribes to it. This seems logical; however, at the same time, it allow us to deem any subscriber a user, even though not every user is a subscriber. However, this assumption applies only to natural persons, not legal persons. Thus, the question that remains concerns the definition of the subscriber as a legal person.

To answer this last question, we combine our reading of articles 1(2) and 2(2) of the EPD. This reading informs us that a subscriber that is a legal person is any juristic entity that pays money to receive services regularly from any electronic communications service provider, but without being considered a user of those services and that, accordingly, is recognized through the protection of its legal interests regarding data protection.

Obviously, this definition reveals that the dispositions in the EPD regarding the role of subscriber legal persons are restrictive. That is, to be recognized as a legal person and to be entitled to the protection such recognition provides constitutes a limitation on legal persons, mainly to avoid becoming users of electronic communications services, so that they can receive the same protections as natural persons do. However, this limitation creates difficulties regarding the implementation of the EPD, which is discussed as follows.

In addition to the complications in understanding the EPD provisions regarding the nature of legal persons as subscribers (without being users) to an electronic communications service, to the effect of protecting their legitimate interests with regard to the EPD, the consequences of this quality of subscriber create two major difficulties in implementing the EPD concerning the two main types of data that this Directive protects: traffic data and location data.[59]

According to article 2(b) of the EPD, "traffic data means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". Thus, because this disposition refers to any data, it is understandable that it includes data from any user or subscriber, even legal persons; thus all the dispositions in the EPD related to traffic data could involve the protection of the legitimate interests of legal persons that are subscribers to any electronic communications service.

---

[59] See *supra*, section 3.2

Now, with regard to the term location data, article 2(c) of the EPD establishes that it "means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service." It is evident that this definition excludes legal persons because, as we noted above, according to article 2(a) of the same Directive, a user is a natural person. Consequently, there arises a difference: On the one hand, legal persons can receive protection related to traffic data; however, on the other hand, they cannot receive protection related to location data. Although it seems logical because of the disembodiment of legal persons, it could be problematic, as we show below.

Hence, the main question that arises concerns what happens when there is any mix of traffic data and location data, such as in the case of data regarding the location of a subscriber legal person's terminal equipment, which may be necessary to know for billing purposes. How can we separate these data as they relate to EPD protection? Alternatively, what happens when some individuals receive services through the terminal equipment of a subscriber legal person? Is this location data not protected with regard to its location by making, not the legal person, but the individuals responsible? If this is so, the location data of the respective individuals run the risk of becoming known indirectly, given that the location data of the subscriber legal person is not protected.

Therefore, imposed on legal persons by the EPD, this quality appears not only a limitation on receiving protection but also a cause of complications with regard to the implementation of this directive. This is mainly because, as we discussed earlier in this paper,[60] an adequate law for the information society should be simple, easily understandable, respected, and followed by its recipients. This does not seem to be the case of the EPD, which, as we have shown, is not easy to understand.

4.2 Legal persons' legitimate interests as objects of protection

The other restriction regarding the application of the EPD to legal persons is that they are protected only with regard to their legitimate interests. Nevertheless, the EPD does not clarify

[60] *Supra* section 2.1

what these legitimate interests signify. Thus, we see it as useful to discuss these legitimate interests, which are the objects of the protection of the EPD with respect to legal persons.

The concept of legitimate interest is not easy to explain. In fact, even a specialized reference source, such as the Black's Law Dictionary, does not include the term. Although it is true that several articles have explored this concept, they did so with regard to specific matters, without giving any concrete definition or even mixing the concepts of legitimate interests and rights.[61] Thus, it is not possible to obtain a general idea of the meaning of legitimate interest, which could be very problematic in the development of a single market. Although it is true that "flexibility is welcomed by business-oriented supporters, [it is also true that] it removes a degree of legal certainty, or may even create a loophole in the legal system. This is particularly the case when norms are formulated ambiguously and no guidance is provided. The risks are increased further if these norms… need implementation in the various Member States."[62]

Hence, given that the EPD states, on the one hand, that natural persons have the right to be protected and on the other hand, that legal persons have the legitimate interest to be protected,[63] the first assumption we can make is that rights and legitimate interests are different. Second, based on the semantic perspective, we can give the following definition of legitimate interest.

Legitimate signifies "allowed according to rules or laws; real, accepted, or official, and fair or reasonable."[64] Interest, *inter alia*, means "a quality that attracts your attention and makes you want to… or to be involved in something."[65] Therefore, a legitimate interest can be defined (at least rudimentarily; the scope of this paper is not to build a definition of legitimate interest) as a juristic standard that, because it is not a right, implies the recognition that something—at least the compliance of law—should be provided to its holder.

As we can confirm, this concept is not easy to explain. We will show that even judges have found it difficult to address this point of legitimate interest with regard to legal persons

---

[61] See, for instance, Balboni *et al* (2013), pp 7 and 11; Ferretti (2014), pp 857, 858, 860, 867 and 868; Greenberg (2013), p 689; Negrut (2013), p 55, and Piar (2012), pp 144, 145, 146 and 166

[62] Ferretti (2014), p 845

[63] See articles 1(1) and 1(2) of the EPD

[64] "Legitimate" in the *Merriam-Webster Dictionary*

[65] *Ibid*, "interest"

and data privacy even though article 8 of ECHR, which can be considered a milestone in data privacy, can be taken as a good reference to explain whether legal persons are data privacy right holders, according to the EPD.[66]

Nevertheless, English courts have expressed some doubt regarding whether article 8 of ECHR comprises corporate privacy or not. To answer this question, scholars have analyzed cases, such as the 2001 "R v Broadcasting Standards Commission ex parte BBC [2001] QB 885 ('BBC'),"[67] in which the "decision sends out mixed signals on the issue of corporate privacy. On the one hand, by holding that regulation of broadcasting standards under the Broadcasting Act 1996 extends to unwarranted interferences with the privacy of a company, the Court recognized that corporate entities have privacy interests. However, on the issue of whether a corporation has a legal right to privacy, in particular under article 8 of the ECHR, Lord Woolf MR adopted a non-committal stance, Hale LJ expressed some doubts and Lord Mustill voiced serious skepticism."[68]

We can infer from the above that legitimate interests are different from rights and thus that legal persons are not holders of rights. Moreover, at least among English judges, it is not unanimously clear whether legal persons can be recognized as holders of rights to data privacy.

Moreover, the decision quoted above gives us an idea of the complexity surrounding the nature of legal persons facing the law, specifically, those facing data privacy law. It is obvious that even lawyers find it difficult to understand not only how somebody can have a legal interest but not a right but also the difference between those concepts. Thus, this complexity regarding the nature of legal persons facing data privacy law is a clear obstacle for the implementation of the EPD in cyberspace and, therefore, the information society in general[69] because a rule that implements the EPD as it is, in which lawmakers recognize legitimate interests but not rights for legal persons, will be meaningful for neither lay people who conform to and manage electronic communications services providers nor legal persons who may be subscribers of those providers.

---

[66] See *supra*, section 1.3

[67] Quoted at Applin (2008), p 7 *et seq*

[68] Aplin (2008), p 9

[69] See *supra*, section 2.1

Furthermore, (continuing with the reference to the ECHR because we consider it very important for data privacy) scholarship on the topic has recognized that "On the issue of whether article 8 (of ECHR) extends to corporate entities the *travaux preparatoires* offers little guidance."[70] Hence, it seems that EU lawmakers, knowing the uncertainty created by the ECHR (which entered into force on September 3, 1953), decided not to include legal persons as data subjects in the EPD, instead choosing to recognize them only as holders of legitimate interests. Nevertheless, the lack of a more definite answer and the inclusion of these nebulous legitimate interests have increased the complexity of the law because it is now necessary to know what those legitimate interests, which are not rights, mean.

However, increasing the complexity of this point, the ECtHR, (regarding the issue of whether legal persons have a right to privacy according to the ECHR, which could be a very good reference for elucidating whether legal persons have a right to data privacy according to the EPD) has decided that "in certain circumstances the rights guaranteed by Art. 8 of the Convention may be construed as including the right to respect for a company's registered office, branches or other business premises."[71] Thus, it is obvious that there is no definitive criterion for whether legal persons have an entitlement to privacy or not. Hence, no good reference exists with regard to the implications of the legitimate interests stated in the EPD.

Hence, we believe that this complicates the implementation of the EPD because, on the one hand, legal persons are not data subjects but only holders of legitimate interests. However, on the other hand, they—that is, legal persons—could have, in certain circumstances, a right to privacy derived from article 8 of the ECHR. The question then concerns how to know when legal persons are only holders of legitimate interests regarding data privacy according to the EPD and when these same persons are rights holders of privacy according to the ECHR (which we have taken here as an important reference because its article 8 is a cornerstone of the right to privacy in Europe, which is related to any issue concerned data privacy). We believe that this distinction can cause severe confusion, which is a negative factor in the implementation of law in the cyberspace context. Moreover, if the ECtHR has recognized that legal

---

[70] Aplin (2008), p 11

[71] *Ibid*, p 13

persons have a right to privacy, based on article 8 of the ECHR, it might raise the question of whether a national legislation that implements the EPD violates article 8.

Now, in the effort to define the concept of legal persons' legitimate interests regarding data privacy, we found that some scholars stated that these interests consist of the quest for the best conditions for organizational autonomy because core secrets are crucial to maintaining the independence of an organization. Namely, legal persons are interested in preserving a certain degree of secrecy with respect to their operations. Specifically, the legitimate interests of legal persons with regard to privacy concern the protection of the information of their clients, employees, and decision-making practices, as well as their commercial innovations and activities.[72]

However, this explanation of the legitimate privacy interests of legal persons has been used to assert that, in certain legal systems, such as the English one, the means against libel are sufficient to protect legal persons against such threats; thus, the recognition of a separate right to privacy for these entities is unnecessary.[73] However, with regard to the recognition of the protection of privacy for legal persons, it has been stated that defamation action only covers false information of a defamatory nature; that is, true statements are not prohibited. Thus, the privacy interests of corporations are not completely protected.[74]

Moreover, it has been stated that "it is not justifiable to allow corporations to control information that is no longer 'secret' or 'confidential', on the basis of it being 'private', because this would enable them to have a monopoly over information, which in turn would conflict with the important aims of competition and innovation."[75]

We can see that by excluding the intermediate concept of legitimate interests, this concept is problematic and that perhaps the EPD rules should more definitive regarding whether legal persons have a right to privacy or not. However, the following discussion will discuss in detail the consequences that this broad concept of legitimate interests may have.

The main consequence of the nebulous protection that the EPD provides legal persons, that is, the protection of their legitimate interests (which, as we showed, is a very broad and

---

[72] Aplin (2008), pp 29-31

[73] *Ibid*, p 31

[74] *Ibid*, p 33

[75] *Ibid*, p 39

undefined concept), is ambivalence. On one hand, we find potential risks, and on the other hand, we find potential benefits.

Concerning the potential risks, we find that the main risks consist of a threat to the harmonization of the EU, which could affect the performance of the electronic communications sector throughout the community because of the lack of equivalent protection for legal persons, which, as we have recognized, represent an important portion of the EU market. Indeed, by taking into account that the EPD refers only to the protection of the legitimate interests of subscribers legal persons without providing a minimum definition of what these legitimate interests signify, it is expected that Member States would implement the respective EPD provisions into their national laws in a free manner, according to their own legal traditions. However, this would provoke multiple divergences, which would act against the harmonization that the EU seeks to achieve. Unfortunately, the scope of this paper prevents the detailed comparison of the different national laws of the Member States that have implemented the EPD. Moreover, in our research, we did not find any judgment from the Court of Justice of the European Union—the so-called European Court of Justice (ECJ)—to illustrate how this court has tackled the concept of legitimate interests in the EPD. We therefore refer to this concept as a potential risk.

Nevertheless, in a community such as the EU, many national legal systems with different legal traditions coexist. Hence, a broad and undefined concept such as the one under discussion could represent a potential benefit because its breadth and ambiguity represent a guarantee of respect for the different legal systems of the Member States, which probably recognize and regulate differently the existence of legal persons, that is, legal fictions.

Moreover, in the global perspective, we must remember that the information society is characterized by the absence of borders; therefore, the breadth and ambiguity of the concept under discussion may also be useful in adapting to the different perspectives that exist regarding legal persons. Hence, the EPD, with its undefined concept of the legitimate interests of subscriber legal persons, could also be advantageous because it avoids EU legal barriers through its relations with non-European countries.

Indeed, conceptions of the rights of legal persons differ, even in countries that have tackled this topic deeply (e.g., the US, where there have been arguments both for and against such rights).[76]

---

[76] Aplin (2008), pp 21-23

The broad concept of the legitimate interests of legal persons has been useful in respecting different perspectives regarding the data privacy rights of juristic entities. For instance, in the case of English law, the perspective has shifted from the conception that legal persons ought not to be recognized as holders of privacy rights because they cannot suffer injured feelings to the notion that legal persons deserve to be recognized as holders of privacy rights because their reputations could be injured.[77]

We believe that even the ECJ has contributed to this vagueness. It has not given a concise ruling regarding whether legal persons have a right to privacy; instead, it has only stated the general principle of respecting the private activities of both natural and legal persons. In fact, soon after the enactment of the EPD, the ECJ made a decision that hindered the clarification of the concept of the legitimate interests of legal persons regarding data privacy. In a judgment on October 22, 2002, the Court reaffirmed that "…the need for protection against arbitrary or disproportionate intervention by public authorities in the sphere of the private activities of any person, whether natural or legal, constitutes a general principle of Community law. [And] …the competent authorities of the Member States are required to respect that general principle."[78] We believe that this statement has hindered the clarification of the situation of legal persons with regard to the fundamental right to privacy because the ECJ recognized, as a general principle of community law, the respect of the private activities of any person, including expressly legal persons. The question then arises regarding whether the legitimate interests recognized in the EPD do constitute rights against intrusions into the private sphere of legal persons or whether they only are a prerogative for protection in specific cases.

We dare to think that these legitimate interests constitute a right to privacy because "Privacy is not necessarily a personal right of which only natural persons can take advantage… one of the branches of US privacy law prevents the appropriation of a plaintiff's name or likeness for commercial purposes, and this action is available to corporations. So there is nothing inherent in the nature of privacy which wholly prevents it from being applied to corporations just because they are not natural persons."[79] The US experience offers some

[77] Aplin (2008), pp 24-28

[78] Roquette Frères, paras 27 and 28

[79] Taylor (2002), p 720

examples the recognition of legal persons as data subjects that deserve protection against the negative use of their personal data. This could indicate that the global perspective on legal persons' rights regarding data privacy is very diverse and therefore needs to reach a certain consensus if they are to be useful and meaningful worldwide and without barriers, which is the essence of the information society.

Moreover, "it should be recognized that it is contradictory for [any] legal system to create fictitious persons and then to use their very fictitiousness as a reason for denying them legal rights."[80] Given this logic, we can say that the EPD—and largely the DPD—formalizes this contradiction because it not only recognizes the existence of legal persons but also establishes restrictions on their data privacy rights.

Obviously, the above argument does not mean that legal persons should be recognized in the same manner as natural persons are. Indeed, "this does not mean that corporations are to be placed on the same footing as individuals when it comes to privacy, but they are not to be wholly excluded from privacy protection either. Excluding them entirely means that the deterrent effect of the law... is removed with respect to corporations."[81] Moreover, "In an age of computer hacking and sophisticated industrial espionage, it is not desirable to abandon this deterrent function of… law,"[82] mainly because "Corporations are likely to be the main target of hackers and a principal target of the media."[83]

Lastly, regarding the usual argument that legal persons should not be recognized as full privacy holders. Because as corporations, they require only the protection of commercial information (rather than personal). It has been stated, "Corporations, in fact, come in all shapes and sizes, and it is too simplistic to say that their interests are always commercial."[84] Thus, commercial protection could not be a justification for the recognition of the right to data privacy for legal persons. Consider the following supporting arguments: "What about a medical practitioner who has incorporated a medical practice? If a newspaper proposes to publish confidential patient

---

[80] Taylor (2002), p 720

[81] *Idem*

[82] Taylor (2002), p 721

[83] *Idem*

[84] *Idem*

notes without naming the patients themselves, so that the patients cannot sue, is the company to be left without redress in any new law of privacy simply because of the fact of incorporation?"[85]

5 The most controversial e-Privacy Directive provisions for legal persons

The EPD comprises two kinds of dispositions that, despite their importance to the new conditions of the information society, are expressly directed only to natural persons and exclude application to legal persons. Moreover, the freedom of regulation to protect the legitimate interests of legal persons concerning the topics to which these dispositions refer is given to the EU Member States. Now, we can say that this distinction seems inconvenient because the digital context does not distinguish between natural persons and legal persons. These dispositions relate the following: first, unsolicited communications for direct marketing purposes—better known as spam—and second, directories of subscribers. In this section, we will discuss both.

In addition, according to article 1(2) of the EPD, the intention is to particularize and complement the DPD in the electronic communications sector. Hence, it is expected that these Directives correspond. However, taking into account that the former recognizes protection for legal persons, while the latter does not, the provisions of the EPD that refer to the DPD and could be applied to legal entities present the problems of interpretation and implementation. We will discuss this issue in the following section.

5.1 Spam and directories of subscribers

In the EPD, the recitals recognize the importance of protecting both the rights of natural persons and the legitimate interests of legal persons against the potential risks of data privacy violations caused by spam and the directories of subscribers. Indeed, recital (38) establishes that "Directories of subscribers… are widely distributed and public. The right to privacy of natural persons and the legitimate interests of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which." Recital

[85] Taylor (2002), p 721

(40) provides that "Safeguards should be provided for subscribers against intrusion of their privacy by [spam]". The same recital explains, "[spam] may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment."

Hence, according to the recitals of the EPD, it appears that EU lawmakers recognize the convenience of protecting both individuals and legal persons. As recitals (38) and (40) indicate, EU lawmakers refer to the right to privacy of natural persons and the legitimate interests of legal persons as worth protecting against risks of data privacy violations caused by the practices of spam and the publication of directories of subscribers. Nevertheless, in the regulatory part of the EPD (i.e., its articles), EU lawmakers made certain exceptions in order to exclude the application of the EPD to legal persons, giving discretion to Member States to regulate this matter according to Community Law and applicable national legislation. For clarity, we include here certain parts of the following articles of the EPD:

> 12(1) Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public … in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic version…
>
> 12(2) Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which…
>
> […]
>
> 12(4) Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.
>
> […]
>
> 13(1) The use of … communications systems … for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.
>
> […]

> 13(3) Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing … are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications…
>
> […]
>
> 13(5) Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

The question then is why EU lawmakers decided to exclude the application of these dispositions to legal persons. The recitals indicate that the lawmakers seemed aware that these kinds of practices—spam and the development of directories of subscribes—could incur serious damage to data subjects in the electronic communications sector. This damage would occur for two main reasons: the reception of unsolicited communication implies a breach of the receiver's privacy; these kinds of communications could damage the systems that conduct electronic communications because they are cheap to send and their massiveness could saturate a system, potentially necessitating expensive repair costs.[86] In fact, "Experts estimate that spam constitutes roughly 50 percent of the e-mail circulating on the Internet."[87]

Apparently aware of these reasons, EU lawmakers established several dispositions in the EPD to care for the data privacy of subscribers and users. However, these dispositions are expressly applicable only to natural persons. Regarding legal persons, the EU lawmaker gave discretion to Member States to protect their legitimate interests according to Community Law and their national legislations. This exception seems truly confusing, and it is one of the reasons that scholars have stated that the EPD lacks clarity in several key areas related to direct marketing communications.[88]

---

[86] Crichard (2003), p 300

[87] The editors of the *Encyclopedia Britannica* (2013)

[88] Donovan (2004), p 127

Hence, although the EPD has attempted to combine the rules on the directories of subscribers and unsolicited communications under one technology-neutral regulation, the result is that "it proposes different rules for different types of communications and different types of recipient. With certain areas left to the discretion of Member States it is also likely that different rules will be introduced in different Member States. There will certainly not be any one size fits all approach."[89] Moreover, the rules of the EPD transcribed above could give Member States the option to decide whether the rights given to natural persons should extend to legal persons. Consequently, there may be anomalies in the nation-level implementation throughout the EU, and this lack of harmonization could affect Community marketing.[90] Thus, the exception that EU lawmakers introduced in the EPD concerning the application of its dispositions to protect legal persons offers both pros and cons.

The potential benefit we find for the exceptions contained in the EPD with regard to the application of the dispositions to legal persons consists of their inherent respect for the characteristics that the legal systems of Member States can have in relation to the regulation of the legal persons and their consideration as holders of rights and subjects of duties.[91]

Indeed, "cultural values and privacy perceptions differ from country to country, with those dissimilar values and perceptions intertwined with and exerting a significant influence over legal environments."[92] This is crucial, even regarding the recipients of law, who according to our discussion of law in cyberspace, respect the law because they consider it meaningful.[93] For example, "When comparing U.S. privacy concerns with non-U.S. privacy concerns, a … survey of over 1000 Internet users in 30 countries indicates that non-U.S. respondents express more concern about organizations using consumer data for customization and personalization purposes."[94] This indicates that the law needs to fit specific zones in order to be meaningful and thus warrant the respect of the people in those zones.

---

[89] Crichard (2003), p 303

[90] Donovan (2004), p 130

[91] *Supra*, section 4.2

[92] Baumer (2004), p 401

[93] *Supra*, section 2.1

[94] Baumer (2004), p 401

However, we believe that the greatest potential risk of the exception with regard the implementation of articles 12 and 13 of the EPD by the national legislations of Member States in relation to the protection of legal persons concerns the lack of harmonization in the EU concerning the protection of the legitimate interests of juristic entities related to spam and the directories of subscribers. These issues are highly relevant to current information and communication technologies in the information society because of the potential risks to data privacy caused by wide distribution and publicity—in the case of directories of subscribers—and their easy, cheap and mass distribution—in the case of spam.[95]

In fact, we must remember, "EU Directives function as commands to Member States to enact laws consistent with the Directive."[96] Thus, as established in article 1(1) of the EPD, "This Directive provides for the harmonization of the national provisions required to ensure an equivalent level of protection." Thus, any matter that is not included in its dispositions would represent a risk of non-harmonization, which is contrary to the principal aim of a political-economic integration, such as the EU, and the construction of a single market.[97]

We also consider that this exception to the general application of the dispositions of the EPD, which is in favor of legal persons through the EU, could generate "legal heavens," that is, juristic entities that are preferable according to the protection provided by Member States. This could result in the concentration of commercial activity in some Member States, to the detriment of other Member States.[98]

Similarly, understanding the differences that could arise from the diverse national rules that Member States could enact without following the general dispositions given by the EPD, is key to meeting successfully the requirements of information privacy in a worldwide marketplace that depends on trans-border data flows, particularly when the regulatory approaches

---

[95] See *supra*, the beginning of this section 5.1

[96] Baumer (2004), p 409

[97] *Supra*, section 2.1

[98] The limited extent of this paper prevented us from undertaking exhaustive research into the matter in order to present a comparative study on this point, which is why we reiterate that these are simply reflections on suggested potential risks.

of other countries are more restrictive than those in an IT manager's home location.[99] Hence, in the case of the EU, even without considering its regulatory conflicts with other non-European countries, it could face internal problems that do not foster the building of a single market, as was the desire of the EU lawmakers. Because the Member States are free to legislate protective laws, they should provide for the legitimate interests of legal persons regarding spam and directories of subscribers. Thus, the providers of electronic communications services may find it necessary to abide by divergent national legislations, which could be complicated when these providers offer their services regionally.

Consequently, the EPD represents the potential risk of a heavy normative burden for the providers of electronic communications services regarding their subscribers' legal persons, which are understood as businesses that participate and contribute to global commerce, through the provision of electronic communications services. This is because the providers that are affected must still take advice about and ensure compliance with not only their national legislation but also a whole host of related legislations. Even a provider of electronic communications services engaged in the simplest level of e-commerce, such as sending advertisements to subscribers by email, must consider not only national rules but also a myriad of other laws and codes of conduct.[100]

5.2 Dispositions referring to the Data Protection Directive

The DPD is the main regulation of data privacy in the EU, and legal persons are not considered in its dispositions. According to articles 1(1) and 2(a) of the DPD, Member States shall protect natural persons, and legal persons are not mentioned. Moreover, the concept of personal data refers only to information related to identified or identifiable natural persons; again, legal persons are not mentioned.

However, the EPD, according to recital (10) and article 1(2), adapts the DPD regarding the electronic communications sector. Nevertheless, unlike the DPD, the EPD recognizes legal persons as holders of legitimate interests, which merit protection when they play the role of subscriber

[99] Baumer (2004), p 401

[100] Crichard (2003), p 303

to any electronic communications service. This lack of correspondence raises certain questions regarding the application of the DPD to legal persons, which we discuss in this section.

Indeed, the principal problems regarding the non-consideration of legal persons within the DPD concern the emergence of difficulties in implementing the EPD, which adapts the DPD to cover the electronic communications sector and the occurrence of uncertainties regarding how some dispositions of the EPD that are related to the DPD would be applied to legal persons.

For instance, article 2(f) of the EPD establishes the definition of "consent," stating that it "corresponds to the data subject's consent in the [DPD]." Moreover, consent could be given "by a user or subscriber [and we must remember that a legal person can be a subscriber]." Thus, there is a lack of clarity regarding whether the DPD is applicable to legal persons, at least with regard to justifying their consent as subscribers to any electronic communications service, according to the EPD. In general, the question is whether it could be understood that all the other dispositions in the EPD that refer to subscribers, without specifying whether they are individuals or legal entities, are applicable to legal persons, where the DPD is concerned.

This nebulous situation gives rise to an uncertainty in matters that have been considered significant in data privacy in the information society, such as the issue the threat of cookies to privacy and data protection.

In fact, an example of a legal framework regarding the use of cookies is set out in article 5(3) of the EPD (which also covers other relevant issues, such as spyware, web bugs, hidden identifiers and other similar devices).[101] This article states, "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with [the DPD]."

Hence, the question is whether legal persons should be excluded from the application of this provision because it also relates to the DPD. If the answer to this question were affirmative, we would have to differentiate between two types of subscribers (namely, subscribers as natural persons and subscribers as legal persons) in the application of the EPD. If the

[101] Debusseré (2005), pp 80 and 83

answer were negative, the DPD would necessarily have to be applied in issues concerning legal persons, which would be contrary to the abovementioned dispositions of this Directive. Thus, the implied certainty[102] might be contrary to the minimum requirements for an adequate law for cyberspace.[103]

Consequently, it has been considered that because of these difficulties and uncertainties related to applying the EPD and connecting it to the DPD, the "[EPD] in general… [is] not [a] masterpiece[s] of logic and clear legislative art."[104] Indeed, "one of the most far-reaching gaps is the lack of a clear description of the exact interaction between [EPD] and its mother [DPD]."[105] This lack of logic and clarity increases the risk of national legislations that implement the EPD such that it is meaningless for electronic communications service providers and users and, thus, inadequate in cyberspace.

6 Conclusion

The arrival of information and communication technologies (principally, the Internet) has led to an alternative reality—cyberspace—where people can interact based on the idea of a global village without borders, where the exchange of data and information is almost unlimited, and where social relations may be pervasive and lack respect for any private sphere, as decided by users.

This new worldwide phenomenon has made it necessary for the law to revisit the traditional means of influencing people to behave lawfully. Furthermore, scholars of law have noted that regarding compliance with the law, the traditional model of imposition, primarily through coercion, has been left behind. Lawmakers have turned to a model that uses a strong sense of persuasiveness to encourage cyberspace users to comply with the law. Hence, if the providers of electronic communications services as well as the users of and subscribers to those services are expected to comply with the law, then it should be meaningful for them, in order that they respect and understand it, as well as implement its provisions.

---

[102] Debusseré (2005), p 87

[103] *Supra*, section 2.1

[104] Debusseré (2005), p 96

[105] *Ibid*, p 97

However, at first glance, the EPD is far from the simplicity required for easy understanding. In adapting the DPD to apply to the electronic communications sector, the EPD included several samples of the absence of coordination between the two. In general, the lack of correspondence relates to the inclusion of legal persons as subjects of protection because the DPD does not consider them as such. Because of this discrepancy, several issues concerning how to remedy the lack of coordination arise, which makes the EPD confusing and difficult to apply to key issues of the digital context, such as cookies.

Moreover, the protection that the EPD has established for juristic entities is, on the one hand, indefinite and restrictive because it states that the legitimate interests of legal persons, which are difficult to define, should be protected (an issue for which the EPD is not useful because it does not provide any description of these interests). Furthermore, such interests should be protected only when legal persons are subscribers to an electronic communications service. On the other hand, two topics that are relevant to data privacy in the digital context—spam and the entry of personal data into a directory of subscribers—are excluded and left for Member States to implement in favor of legal persons. However, Member States can protect the legitimate interests of juristic entities according to the Community Law—whatever this means—and their national legislations.

Hence, the data privacy regime for legal persons established by the EPD is not only nebulous and complicated but also uncertain. According to scholars and judges, this vagueness has been little addressed in doctrines and jurisprudence. More than a decade after the enactment of the EPD, it continues to be neglected.

At first glance, the EPD seems pessimistic. Thus, we could say that the data protection regime for legal persons according to this Directive is not adequate for the information society, mainly because the EPD is complex. A closer examination reveals that the data privacy regime established by the EPD for legal persons offers not only risks but also benefits with regard to the features of the EU and the information society.

Indeed, we conclude that the EPD is generally complex and even vague regarding the protection it provides for legal persons, mainly because it does not delimit the object of protection for those juristic entities. It makes some exceptions concerning the application of several provisions to legal persons, and it gives Member States the liberty to regulate certain issues according to Community Law and their national legislations. These characteristics could represent both risks and benefits.

On one hand, the characteristics of the EPD are potential risks because they work against the building of the single market that the EU desires because they allow Member States to regulate freely how they will protect legal persons in the electronic communications sector. Moreover, the potential diversity of rules could produce a high normative burden on the providers of electronic communications services in the EU. Such providers must observe not only their national laws but also other the laws of other EU nations in order protect legal persons in the regional context. This could lead to the appearance of "data privacy havens," such that the commercial activity of legal persons could concentrate in certain EU Member States, to the detriment of others.

On the other hand, these features are a potential benefit for not only the EU but also legal persons in the information society. In fact, if we remember that the EU is an economic and political integration shaped by multiple countries, we must understand that the cultural diversity among Member States is considerably high. Thus, if law is deeply influenced by culture and is a part of culture, Directives require enough flexibility to allow Member States to implement them in their national legislations, while respecting their own legal traditions. Accordingly, the exceptions provided by the EPD could be seen as a framework for respecting the legal traditions of Member States, mainly with regard to the way in which they choose to regulate legal persons (given that such persons are not real individuals but legal fictions, they are influenced by the cultures embedded in the legal traditions of each country).

Similarly, if we consider that the information society is characterized by the communication and exchange of information in the global village, we could conclude that many cultures are embedded within the society and that rules need to be flexible enough to defer to different legal conceptions, such as the legal fictions called corporations or legal persons.

Therefore, until now, legal persons have been held in suspense regarding the regime established by the EPD with regard to their data privacy. Thus, scholars and judges should soon work to shed more light on this topic, which undoubtedly will remain relevant for law and the information society.

7 Bibliography

References to legal instruments refer to their amended states as of January 2014. The websites were last accessed on November 3, 2014.

Legal instruments

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

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector

Cases

Bern Larsen Holding AS and others v Norway. *Judgment of the European Court of Human Rights (First Section)*. Application no. 24117/08. July 8, 2013 (final)

Roquette Frères. *Judgment of the European Court of Justice*. Case C-94/00. October 22, 2002

Books and articles

Palin, Tanya. *A right of privacy for corporations?* Social Science Research Network. (2008)

Baker Miner, Abu and Siri Hagar Mohr Yassin. "Retention of communications data: a bumpy road ahead" in *Journal of Computer & Information Law*. Vol. XXII. (2004). 731-758

Balcony, Paolo, Daniel Cooper, Rosario Imperial and Mild Macerate. "Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection" in *International Data Privacy Law*. (2013). 1-18

Bauer, David L., Julia B. Earp and J.C. Poindexter. "Internet privacy law: a comparison between the United States and the European Union" in *Computers & Security*. Elsevier. (2004). 400-412

Burges, Sean. "Economic integration" in *Encyclopedia Britannica*. (2013). At http://www.britannica.com/EBchecked/topic/178433/economic-integration

Bissell, Jennifer. "Cyberspace" in *Encyclopedia Britannica*. (2013). At http://www.britannica.com/EBchecked/topic/147819/cyberspace

Bygrave, Lee A. *Data privacy law. An international perspective*. Oxford. (2014)

Carozza, Paolo. "European law" in *Encyclopedia Britannica*. (2014). At http://www.britannica.com/EBchecked/topic/1443520/European-law

Crichard, Mark. "Telecoms privacy directive – UK implementation. Privacy and electronic communications" in *Computer Law & Security Report*. Vol. 19. No. 4. Elsevier. (2003). 299-303

Debusseré, Frederic. "The EU e-Privacy Directive: A monstrous attempt to starve the cookie monster?" in *International Journal of Law and Information Technology*. Vol. 13. No. 1. Oxford. (2005). 70-97

Donovan, Colleen. "Implementation of the e-Privacy Directive in the UK – Understanding the new rules" in *Computer Law & Security Report*. Vol. 20. No. 2. Elsevier Science. (2004). 127-132

Edwards, Lilian. "Privacy and data protection online: the laws don't work?" in Edwards, Lilian and Charlotte Waelde (editors). *Law and the Internet*. 3rd edition. Hart. (2009). 443-488

Ferretti, Federico. "Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?" in *Common Market Law Review*. No. 51. Kluwer Law International. (2014). 843-868

Gabel, Matthew J. "European Union (EU)" in *Encyclopedia Britannica*. (2014). At http://www.britannica.com/EBchecked/topic/196399/European-Union-EU

Greenberg, Daniel. "Initial interest confusion plus non-commercial freedom of speech: right or legitimate interest in an infringing domain name?" in *Journal of Intellectual Property Law & Practice*. Vol. 8. No. 9. (2013). 689-690

Knauer, Nancy J. "Legal fictions and juristic truth" in *St. Thomas Law Review*. Vol. 23. (2010). 1-49

Negrut, Vasilica. "Subjective right and the legitimate interest in the Romanian administrative law" in *Acta Universitatis Danubius. Juridica*. Vol. 9. No. 1. (2013). 50-57

Piar, Daniel F. "Morality as a legitimate government interest" in *Penn State Law Review*. Vol. 117. No. 1. (2012). 139-169

Poullet, Yves. "About the e-Privacy Directive: towards a third generation of data protection legislation?" in Gutwirth, S. *et al* [sic] (editors). *Data Protection in a Profiled World*. Springer Science+Business [sic] Media B.V. (2010). 3-30

Raab, Charles D. "Privacy as a security value" in Wiese Schartum, Dag, Lee A. Bygrave and Anne Gunn Berge Bekken (editors). *Jon Bing. A tribute*. Gyldendal. (2014). 39-58

Reed, Chris. *Making laws for cyberspace*. Oxford. (2012)

Reed, Chris. "You talkin' to me?" in Wiese Schartum, Dag, Lee A. Bygrave and Anne Gunn Berge Bekken (editors). *Jon Bing. A tribute*. Gyldendal. (2014). 154-170

Schane, Sanford A. "The corporation is a person: the language of a legal fiction" in *Tulane Law Review*. Vol. 61. (1987). 563-609

Taylor, Greg and David Wright. "Case notes. Australian Broadcasting Corporation v Lenah Game Meats. Privacy, injunctions and possums: an analysis of the high court's decision" in *Melbourne University Law Review*. Vol 26. (2002). 707-735

The editors of the Encyclopedia Britannica. "Spam" in *Encyclopedia Britannica*. (2013). At http://www.britannica.com/EBchecked/topic/941678/spam

Walden, Ian. "European Union Communications Law" in Walden, Ian (editor). *Telecommunications Law and Regulation*. 4th edition reprinted. Oxford (2013). 143-186

Miscellaneous

Black's Law Dictionary. Free Online Legal Dictionary. 2nd edition. At http://thelawdictionary.org

Council of the European Union. *Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure—General Approach*. 26 May (2014). At http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209870%202014%20INIT

Council of the European Union. *New EU framework for protection of trade secrets*. Press release of the Council. No. 306. 26 May (2014-2). At http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/intm/142780.pdf

"Data protection in the electronic communications sector" in *EUR-Lex. Access to European Union Law*. At http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1412874510404&uri=URISERV:l24120

Merriam-Webster Dictionary. At http://www.merriam-webster.com