ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

ΝΟΜΙΚΗ ΣΧΟΛΗ

Π.Μ.Σ.: International and European Legal Studies
ΕΙΔΙΚΕΥΣΗ: Private Law and Business Transactions
ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΕΤΟΣ: 2021-2022

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Μαρίας-Ειρήνης Παππά
Α.Μ.: 7340022101019

Processing of Electronic Communications Data from Digital Rights Ireland to the new e-Privacy Regulation

Επιβλέποντες:
Ονοματεπώνυμα επιβλεπόντων
α) Γεώργιος Γιαννόπουλος

Αθήνα, 2022

National and Kapodistrian University of Athens

Law School

LL.M. in International and European Legal Studies

Specialization: Private Law and Business Transactions

Thesis Supervisor:

1. **Associate Prof. Georgios Yannopoulos**

Thesis Committee Members:

2. **Assistant Prof. Vassiliki Christou**
3. **Professor Spyridon Vlachopoulos**

Abstract

Electronic Communications have become an important part of our everyday lives. We use our mobile phones to make phone calls, either internet-based or not, to access the Internet in order to read the news, listen to music, contact our favorites, be active in the social media. In a world, where the types of communication evolve, how much protected is our privacy? Has it been sacrificed in the altar of technology?

The purpose of this thesis is to provide a comprehensive overview of the processing of electronic communications data and the evolution of the rules regulating it over twenty years, from the adoption of Directive 2002/58/EC (e-Privacy Directive), the landmark decision of the CJEU in Digital Rights Ireland to the Proposal for a new e-Privacy Regulation.

The first section deals with the legal framework which is still applicable to the processing of electronic communications data, namely the e-Privacy Directive (Directive 2002/58/EC).

The second section copes with data retention and with an analysis of the CJEU's case-law regarding this issue, with an emphasis on the case Digital Rights Ireland (Joined Cases C-293/12 and C-593/12, Digital Rights Ireland Ltd. and others).

The last section provides an analysis of the processing of electronic communications data, as regulated in the Proposal for a new e-Privacy Regulation, which is awaited to enter into force -hopefully- during 2023 and apply in 2025.

Table of Contents

List of Abbreviations

AG	Advocate General
Charter	EU Charter of Fundamental Rights
CJEU	Court of Justice of European Union
DRIPA	Data Retention and Investigatory Powers Act
DSM	Digital Single Market
ECC	Electronic Communications Code
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
DGA	Data Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
DSM	Digital Single Market
IP	Internet Protocol
ISP	Internet Service Provider
PTS	Post and Telecom Authority
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of European Union

Introduction

A survey which was conducted between November and December 2020 across the twenty-seven Member States of the European Union (EU) has shown that a 96% has mobile telephone access, 82% of the households have internet access and 53% of them have fixed telephone access.[1] The use of electronic communications is extensive and the latter play an important role in our everyday lives. We access the Internet to read the news, to contact our favorite persons, to listen to music, to be active in the social media. Apart from the Internet, traditional communications services, such as mobile or fixed telephony services, maintain an important place on the user's preferences.

The extensive use of electronic communications implies that electronic communications data, namely the content of communications and metadata (traffic and location data), are generated and processed in the context of the provision of electronic communications services. The European legislator had recognized the need for a specific legal framework regulating the processing of data in the electronic communications sector since the 1990's, which resulted to the adoption of the e-Privacy Directive in 2002.

An important step towards the dominance of fundamental rights and specifically, of the right to privacy and the right to protection of personal data, against the bulk retention of electronic communications data was the decision of the Court of Justice of the European Union (CJEU) in the case Digital Rights Ireland in 2012. The decision in Digital Rights Ireland as well as the adoption of the General Data Protection Regulation (GDPR), which strengthened the rules regarding the processing of personal data, called for a new legal regime concerning the processing of electronic communications data that would "shield" the rights to privacy, protection of personal data and communications and that would be in consistency with GDPR. The e-Privacy Regulation, though, remains still a proposal and is awaited to be adopted.

1. The e-Privacy Directive

Since 1990 the EU had recognized the need for harmonization of national laws regarding data protection and the need for more specific rules to regulate data protection in the communications sector. The first step was the adoption of the Data

[1] Eurobarometer. "E-Communications in the Single Market." *www.europa.eu*, European Union, June 2021, https://europa.eu/eurobarometer/surveys/detail/2232.

Protection Directive (Directive 95/46/EC) in 1995 and the second step the adoption of the Telecommunications Privacy Directive (Directive 97/66/EC) *"concerning the processing of personal data and the protection of privacy in the telecommunications sector"*[2] in 1997 -seven years after the proposal. However, as soon as the Telecommunications Privacy Directive was adopted, it was considered obsolete due to the fact that the language used was more suitable for traditional fixed telephony services.[3] It was therefore replaced by the e-Privacy Directive (Directive 2002/58/EC) because of the need for adjustment to technological developments, mainly to the Internet, to ensure a high level of protection of personal data and privacy.[4] Particularly, in accordance with the principle of "technological neutrality" which the e-Privacy Directive follows, the word "call" which was used in the Telecommunications Privacy Directive was substituted by "electronic communication" so as to cover all means of communication.[5]

The e-Privacy Directive together with other four directives was part of the telecoms package, a legislative framework governing the electronic communications sector.[6] In 2009 it was amended by the Citizens' Rights Directive (Directive 2009/136/EC). The Directive's aim is the harmonization of national provisions in order to *"ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community"*.[7] It serves a dual aim,[8] firstly ensuring the compliance of the processing of electronic communications data with fundamental rights as enshrined in articles 7 and 8 of the EU Charter of Fundamental Rights and secondly, guaranteeing the free flow of such data, relevant services and equipment across the EU. Moreover, the Directive "embodies" the fundamental right to freedom of communication.[9]

[2] DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.
[3] Lloyd, Ian. "Information Technology Law". 9th Edition. Oxford University Press, p. 120.
[4] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Recital 4.
[5] Louveaux, Sophie, Perez, Asinari, et. alia. "New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector-Some Initial Remarks." Computer and Telecommunications Law Review, vol. 9, no. 5, 2003, p. 133, footnote 5.
[6] "Data protection in the electronic communications sector", EUR-lex. Available at: https://eur-lex.europa.eu/EN/legal-content/summary/data-protection-in-the-electronic-communications-sector.html
[7] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 1 (1).
[8] Van Hoboken, Joris and Frederick Zuiderven Borgesius. "Scoping Electronic Communication Privacy Rules: Data, Services and Values." Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol 6, no. 3, December 2015, p. 199.
[9] Naranjo, Diego. "E-Privacy Regulation: Good Intentions but a Lot of Work to Do." European Data Protection Law Review (EDPL), vol. 3, no. 2, 2017, p. 152.

1.1 Scope of Application

1.1.1 The material scope of application

The e-Privacy Directive applies to the *"processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks, including public communications networks supporting data collection and identification devices"*.[10] It covers the processing of personal data only in the electronic communications sector and regulates the activities of the providers of electronic communications services.[11] The Directive constitutes "lex specialis" towards the Data Protection Directive and already, General Data Protection Regulation (GDPR),[12] where the latter covers the processing of personal data irrespective of the sector concerned. More specifically, the e-Privacy Directive *"particularizes and complements"*[13] the provisions of the GDPR, which continues to cover all the other issues which are not specifically addressed by Directive 2002/58/EC.[14]

The European legislator has provided a definition of electronic communications services in Directive 2002/21/EC (the Framework Directive). According to this Directive, which is no longer in force as it has been repealed by the European Electronic Communications Code but upon which the e-Privacy Directive still relies,[15] an electronic communication service is "*a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting"*.[16] Information society services *"which do not consist wholly or mainly in the conveyance of signals on electronic communications networks"*[17] do not constitute electronic communications services. Information society services, therefore, are not wholly excluded from the scope of application. The criterion for the categorization of a service as an electronic communications service is a technical one,[18] namely the conveyance of signals on electronic communications networks. The definition of the electronic communications networks is also provided on the same legal act and are *"transmission systems and, where applicable, switching*

[10] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 3.
[11] Joined Cases C-203/15 and C-698/15, Tele 2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others, para. 70.
[12] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 1 (2).
[13] Ibid.
[14] Ibid, Recital 10.
[15] Ibid, art. 2.
[16] See DIRECTIVE 2002/21/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 2 (c).
[17] Ibid.
[18] Sein, Karin. "Interplay of Digital Content Directive, European Electronic Communications Code and Audiovisual Media Directive in Communications Sector." Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol. 12, no. 2, April 2021, p. 171.

or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed".[19] The e-Privacy Directive applies only to publicly available services and networks.

Apart from the fixed and mobile telephone services, Internet access services also fall within the scope of the e-Privacy Directive. Due to the fact that the Framework Directive is twenty years old, the aforementioned definitions and hence, the e-Privacy Directive do not cover services that have emerged during the last years and namely Voice over Internet Protocol (VoIP) services, such as Skype, WhatsApp and FaceTime, instant messaging and web-based email services,[20] which constitute the so-called Over-the-Top communications services. Regarding these services, the GDPR applies. Moreover, as already mentioned, the e-Privacy Directive is applicable only to publicly available electronic communications services which means that services provided to a limited group of users[21] do not fall within the scope of the Directive. This point had evoked the criticism of the Article 29 Working Party in 2008, which stressed the difficulty of the involved parties to determine whether the Directive applies to specific situations where the involved services are both of private and public nature, for instance when Internet access is provided to the employees of a multinational company.[22]

Article 1 (3) of the Directive establishes an exception from the scope of application. Specifically, *"activities of the state in specified fields, including the activities of the state in areas of criminal law and in the areas of public security, defence and state security, including the economic well-being of the state when the activities relate to state security matters*"[23] are excluded. The CJEU has interpreted this exception narrowly and has stressed that the only activities that fall within the scope of this

[19] See DIRECTIVE 2002/21/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 2 (a).
[20] See Explanatory Memorandum Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
[21] Louveaux, Sophie, Perez, Asinari, et. alia. "New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector-Some Initial Remarks." Computer and Telecommunications Law Review, vol. 9, no. 5, 2003, p. 134.
[22] Van Hoboken, Joris and Frederick Zuiderven Borgesius. "Scoping Electronic Communication Privacy Rules: Data, Services and Values." Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol 6, no. 3, December 2015, p. 200.
[23] Joined Cases C-203/15 and C-698/15, Tele 2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others, para. 69.

exception are those which are carried out directly by state authorities[24] and not those which are carried out by the providers of electronic communications services in compliance with obligations imposed to them by the state.[25]

The e-Privacy Directive regulates three types of data which are processed by the providers of electronic communications services in the context of their activities: a) traffic data, b) location data and c) content of communications.

1.1.2 The personal scope of application

According to GDPR, personal data concern only natural persons. Legal persons do not enjoy any protection. A significant difference between the "lex generalis", GDPR, and the "lex specialis", e-Privacy Directive, is that the latter protects also *"the legitimate interests of subscribers who are legal persons"*.[26] However, this protection that the Directive accords to legal persons shall not be considered to conflict with the definition of personal data, as provided in the GDPR. In principle, the e-Privacy Directive recognizes the legal persons only as holders of legitimate interests and not as data subjects.[27]

Before analyzing the protection accorded to legal persons, it must be noted that the Directive makes a distinction between the recipients of the electronic communications services, who can be either users or subscribers. The Directive provides only the definition of users who are natural persons who use the electronic communications services without being subscribers to the services. The definition of subscribers derives a contrario and are either natural or legal persons who have subscribed to the service and receive it in return for a fee.

The Directive does not define what the legitimate interests of the legal persons, on which protection is conferred, are. It does not provide any guidance on the recitals either. Due to this fact, it is rather uncertain whether the legitimate interests coincide with the right to protection of personal data and the right to privacy. It seems that the European legislator consciously used this terminology[28] in order to distinct the two concepts.[29] Regarding the right to protection of personal data, as enshrined in article

[24] Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others, para. 48.
[25] Ibid, para. 46.
[26] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 1 (2).
[27] JP Lopez, Luna. "The data privacy regime for legal persons in the electronic communications sector according to Directive 2002/58/EC." UiO Faculty of Law, University of Oslo, December 1, 2014, p. 20-21.
[28] The same terminology is also used in the Greek version («έννομα συμφέροντα») and in the German version of the Directive ("berechtigen Interessen").
[29] See also DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, recital 12.

8 of the Charter, if the two concepts coincided, there would be an inconsistency between the GDPR and the e-Privacy Directive, as mentioned above. The concept of "legitimate interests" is a step below the concept of a right. In case Roquette Frères SA (C-94/00) the CJEU recognized the need for protection of the privacy of legal persons.[30] Therefore, it can be inferred that legal persons have a legitimate interest in protection of their privacy. An example of a legitimate interest could be the preservation of professional secrecy. The concept is rather ambiguous, though and the lack of clarifications can be an impediment to the function of the internal market, as Member States can interpret the concept of legitimate interests in different manners and therefore, the providers of the electronic communications services can be faced with different obligations across Member States.

In order to enjoy the protection provided by the Directive, legal persons must be subscribers to the electronic communications services. They cannot be users, as users are natural persons only. It seems that the protection of the legitimate interests of legal persons is limited only to the processing of traffic data and not of location data, since, according to the definition of the latter, they relate to data of the users and not of the subscribers.[31] However, in article 9 of the Directive the European legislator states that both users and subscribers are location data subjects.[32] To the author's view this inconsistency is a clerical error and there is no reason why the legislator would grant a different protection to users and subscribers and thus, to natural and legal persons, regarding location data.

1.1.3 The territorial scope of application

In article 3 of the e-Privacy Directive it is stated that the Directive is applicable when the electronic communications services are provided "in the Community". The provider of the electronic communications services can be established either in or outside the EU, as long as the services are provided to users or subscribers who are located in the EU.

1.2 Processing of electronic communications data

[30] Case C-94/00, Roquette Frères SA and Directeur general de la concurrence, de la consommation et de la répression des fraudes, para. 27.
[31] JP Lopez, Luna. "The data privacy regime for legal persons in the electronic communications sector according to Directive 2002/58/EC." UiO Faculty of Law, University of Oslo, December 1, 2014, p. 25.
[32] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 9 (1).

1.2.1 Traffic Data

Traffic data are defined as the data which are *"processed for the purpose of the conveyance of a communication or for the billing thereof"*.[33] A communication is *"any information exchanged or conveyed between a finite number of parties by means of publicly available electronic communications services"*.[34] Traffic data are, among others, those relating "*to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network"*.[35] They consist of the data which are processed both for the use of a telephone and the use of the Internet. Email and Internet Protocol (IP) addresses, numbers called, calling numbers constitute traffic data. Due to the technological developments in the communications sector, the difficulty in drawing a clear line between the content of a communication and traffic data and the ambiguity of the definition of traffic data and specifically of the phrase *"for the purpose of conveyance of communication"*, it is unclear whether the subject of an email constitutes traffic data or content of the communication. An argument can be drawn from article 5 (1) of the Directive. The legislator uses the word "necessary" for the purpose of conveyance of a communication. Therefore, in cases where there is uncertainty regarding the nature of electronic communications data, the criterion for their classification as traffic data shall be whether they are necessary for the aforementioned purpose. Hence, the subject of an email is rather content of communications than traffic data.[36]

Traffic data can be considered to be *"in a sense more than personal"*,[37] rather *"special personal data [because their] use may make it possible to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity"*.[38]

In principle, the processing of traffic data is prohibited. Article 5 of the e-Privacy Directive states that traffic data are confidential and that storage and interception of such data is not allowed. Member States shall take all the appropriate measures to

[33] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 2 (b).
[34] Ibid, art. 2 (d).
[35] Ibid, recital 15.
[36] Louveaux, Sophie, Perez, Asinari, et. alia. "New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector-Some Initial Remarks." Computer and Telecommunications Law Review, vol. 9, no. 5, 2003, p. 136-137.
[37] Opinion of Advocate General Cruz Villalon on Cases C-293/12 and C-593/12, 12 December 2013, para. 65.
[38] Ibid, para. 74.

ensure the confidentiality of these data. The rule of confidentiality has an *"erga omnes"* applicability[39] and hence not only does it apply to providers of electronic communications services but it is also binding for other bodies.[40] There are, however, exceptions to this general rule:

a) The processing of such data by persons other than the users is allowed when the user or subscriber has provided his/her consent for such a processing. Consent has the same meaning as that laid down in the GDPR, regardless if it concerns natural or legal persons.[41] This consent shall be specific, shall be given freely and in an affirmative manner.[42] Consent is the only legal basis under which such processing is permitted. The providers of electronic communications services cannot rely for the processing on any other basis provided in article 6 of GDPR.
b) Technical storage of traffic data which is necessary for the conveyance of communication is allowed. The term "technical storage" is explained as *"any automatic, intermediate and transient storage".*[43] This storage shall serve exclusively the purpose *"of carrying out the transmission of a communication in the electronic communications network"*.[44] This processing is subject to limitations. Article 6 (1) sets the rule regarding the processing of traffic data by the providers of the electronic communications services. Specifically, they shall erase or make anonymous the traffic data when the latter are no longer required for the transmission of a communication. This moment, after which the communication is conveyed and the traffic data are no longer necessary, may vary depending on the type of the communication. For example, *"for a voice telephony call the transmission will be completed as soon as either of the users terminates the connection. For electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider".*[45] Furthermore, the legislator clarifies that the obligation to erase or make anonymous the traffic data is not inconsistent with the procedures on the Internet.[46] However, this obligation to erase or make

[39] Gumzej, Nina. "Applicability of ePrivacy Directive to National Data Retention Measures following Invalidation of the Data Retention Directive." Juridical Tribune, vol. 11, no. 3, December 2021, p. 441.
[40] Van Hoboken, Joris and Frederick Zuiderven Borgesius. "Scoping Electronic Communication Privacy Rules: Data, Services and Values." Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol 6, no. 3, December 2015, p. 202.
[41] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, recital 17.
[42] See REGULATION (EU) 2016/679, General Data Protection Regulation, art. 4 (11).
[43] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, recital 22.
[44] Ibid.
[45] Ibid, recital 27.
[46] Ibid, recital 28.

anonymous traffic data after the transmission of a communication is also subject to exceptions. Specifically:

i. According to article 6 (2) of the e-Privacy Directive, traffic data can be processed for billing and interconnection payments purposes. This processing, though, shall take place for a limited time and particularly, "*up to the end of the period during which the bill may lawfully be challenged or payment pursued*".

ii. The processing of traffic data is permitted for marketing purposes or for the provision of value added services under the condition that the user or subscriber to whom the data relate has provided his/her prior consent[47] *"on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing"*.[48] Consent constitutes the only legal basis for the processing of such data for the aforementioned purposes and has the meaning that is laid down in the GDPR and analyzed above. Value added services are defined as "*services which require the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof"*.[49] Such services could be the downloading of ringtones[50] or the provision of *"advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information"*.[51] The data shall be erased or made anonymous after the purpose for which they had been processed is achieved.

iii. Processing is allowed for the purposes of detecting *"technical failure or errors in the transmission of communications"*[52] and for the purposes of *"detecting and stopping fraud consisting of unpaid use of the service"*.[53]

[47] Ibid, art. 6 (3).
[48] Ibid, recital 26.
[49] Ibid, art. 2 (g).
[50] Lloyd, Ian. "Information Technology Law". 9th Edition. Oxford University Press, p. 127.
[51] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, recital 18.
[52] Ibid, recital 29.
[53] Ibid.

iv. The providers of electronic communications services, in conformity with legal obligations imposed on them, may inform the competent authorities about traffic data in order for the latter to resolve disputes regarding interconnection or billing.[54]

The processing under the exceptions laid down under (b) points (i), (ii) and (iii), shall be subject to strict conditions, i.e. that it shall be performed by persons who are authorized by the providers of the electronic communications services to do so and it shall be limited to what is strictly necessary for the purposes pursued.

c) Recording of traffic data is allowed when it is legally authorized and serves the purpose of *"providing evidence of a commercial transaction or of any other business communication in the course of lawful business practice"*.[55]
d) The exception established in art. 15 of the e-Privacy Directive applies which will be examined below.

1.2.2 Location Data

Location data are defined as *"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"*.[56] In digital mobile networks location data will be processed for the purpose of conveyance of a communication. In this case location data constitute traffic data and hence, the aforementioned rules regarding the processing apply.[57] There will be cases, though, that more specific location data than those needed for the conveyance of a communication in the mobile network will be processed. This processing shall take place only for the purpose of the provision of value added services, for example *"services providing individualized traffic information and guidance to drivers"*[58] and shall be limited only to what is strictly necessary and for the time necessary for the achievement of this purpose. Furthermore, such data must be made anonymous before the processing or the user or subscriber must have provided his/her consent to the provider of the services.[59]

[54] Ibid, art. 6 (5).
[55] Ibid, art. 5 (2).
[56] Ibid, art. 2 (c).
[57] Ibid, recital 35.
[58] Ibid.
[59] Ibid, art. 9 (1).

Apart from the requirements that the providers of electronic communications must follow in order for the processing of location data by them to be lawful, art. 9 sets additional safeguards. Specifically, the providers of electronic communication services must inform the users or subscribers before providing their consent about the type of the location data that will be subject to processing, the purposes and the duration of the latter and whether the data will be transmitted to third parties for the provision of the value added service. In practice, however, this information will normally be provided in a long text together with the general terms and conditions for the provision of the electronic communications services themselves,[60] by making it very difficult for the data subjects to pay attention to such information and to understand it.

The users or subscribers shall be free to withdraw their consent at any time or to "*temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication"*.[61] Finally, like traffic data, processing must be carried out only by persons who are authorized by the provider of the electronic communications services to do so or by the third parties who provide the value added service.

It must be noted that location data and their processing is more sensitive than this of traffic data due to the fact that they relate with the geographic position of the data subject at the specific time[62] where the user or subscriber uses the value added service and this can reveal many aspects of his/her everyday life. This is the reason why their processing is allowed only under strict and limited conditions.

1.2.3 Content of Communications

The last category of data regulated by the Directive concerns the content of communications. As already stated, a communication is defined as *"any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service"*.[63] This definition, though, does not include *"any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information",* [64] as could happen for example with a video on demand service.[65] Apart from a call through a fixed

[60] Lloyd, Ian. "Information Technology Law". 9th Edition. Oxford University Press, p. 127.
[61] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 9 (2).
[62] Lloyd, Ian. "Information Technology Law". 9th Edition. Oxford University Press, p. 127.
[63] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 2 (d).
[64] Ibid.
[65] Ibid, recital 16.

or a mobile phone, this definition of communication involves internet browsing and online video services, like Youtube, as well.[66] The e-Privacy Directive establishes the confidentiality of the content of communications and imposes Member States a positive obligation to ensure this confidentiality by adopting the appropriate national legislation, as already mentioned in the section for traffic data, where the same rule applies. Particularly, *"listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users"*[67] must be prohibited. Hence, in principle, processing of the content of communications is prohibited. However, article 5 of the Directive provides some exceptions which are the same with the exceptions provided for traffic data and are referred under this section briefly:

a) The users have provided explicitly their consent.
b) The exception provided in art. 15 of the Directive, which will be analyzed below, applies.
c) Technical storage of the content of the communication which is necessary for the conveyance of communication is allowed *"provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed"*.[68]
d) Recording of communications is allowed when it is legally authorized and serves the purpose of *"providing evidence of a commercial transaction or of any other business communication in the course of lawful business practice"*.[69]

1.3 The exception of art. 15 of the e-Privacy Directive

Article 15 of the e-Privacy Directive establishes an exception from the rules laid down in articles 5, 6, 8 para. 1 to 4 and 9. Specifically, it gives Member States the opportunity to adopt legal acts which restrict the rights and obligations imposed in the aforementioned articles for the attainment of specific purposes, which are exhaustively listed in article 15. These purposes are the protection of *"national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal*

[66] Van Hoboken, Joris and Frederick Zuiderven Borgesius. "Scoping Electronic Communication Privacy Rules: Data, Services and Values." Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol 6, no. 3, December 2015, p. 202.
[67] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 5 (1).
[68] Ibid, recital 22.
[69] Ibid, art. 5 (2).

offences or of unauthorized use of the electronic communication system",[70] as referred in art. 13 (1) of the Data Protection Directive and already art. 23 (1) of the GDPR.[71]

The legislator sets some prerequisites regarding the restrictions. Firstly, they must be *"necessary, appropriate and proportionate"*[72] for the attainment of the purposes mentioned above. Secondly, they must comply with the general principles of EU law and with the fundamental rights as enshrined in the Charter.[73] The retention of electronic communications data for a limited time period is referred as an indicative restriction.

Specific obligations are imposed on the providers of electronic communications services concerning the restrictions established by Member States through the implementation of legislative measures. The providers shall maintain the appropriate internal procedures in order to be able to respond to requests by the competent authorities for access to users' electronic communications data. Furthermore, they shall inform the competent authorities about *"those procedures, the number of requests received, the legal justification invoked and their response"*[74] upon request. The ultimate goal of the legislator was to provide the supervisory authorities, such as the national data protection authorities, with the power to check the processing of the electronic communications data carried out by the providers of electronic communications services pursuant to the restrictive measures adopted by the Member States.[75] It seems, though, that this provision has remained dead letter.

The CJEU has provided guidance on the interpretation and the application of article 15 of the e-Privacy Directive, which will be analyzed in the next chapter.

1.4 Obligations under the e-Privacy Directive

1.4.1 Security of processing

The providers of electronic communications services must take all the *"appropriate technical and organizational measures"*[76] in order to ensure the security of the data which are processed during the provision of their services and specifically,

[70] Ibid, art. 15 (1).
[71] Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others, para. 47.
[72] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 15 (1).
[73] Ibid, recital 2.
[74] Ibid, art. 15 (1b).
[75] Gumzej, Nina. "Applicability of ePrivacy Directive to National Data Retention Measures following Invalidation of the Data Retention Directive." Juridical Tribune, vol. 11, no. 3, December 2021, p. 446.
[76] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 4 (1)

the confidentiality of the content of communications and of traffic data. It might be necessary to cooperate with the provider of the public communications network for the aforementioned purpose with respect to network security. These measures shall ensure a level of security which is proportional to the inherent risks in the electronic communications sector.

The e-Privacy Directive provides a minimum set of goals that the technical and organizational measures must achieve. Particularly, they shall at least *"ensure that personal data can be accessed only by authorized personnel for legally authorized purposes, protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure and ensure the implementation of a security policy with respect to the processing of personal data"*.[77] Nowadays with the rapid increase of the use of the Internet the most common risk is the unauthorized access to data being transmitted through the network. A large number of transactions takes place through the Internet, such as payments, with the security of the financial data being often questioned.[78] The Directive authorizes the competent national authorities, i.e. the national data protection authorities, to review the measures taken by the providers of the electronic communications services and recommend any changes they believe that are appropriate in order to ensure a satisfying level of security.

Apart from the technical and organizational measures that the providers must take, they must also inform the subscribers about any specific risk of a breach of the security of a network and when such risks *"lie outside the scope of possible remedies by the service provider"*[79] they shall inform the users and subscribers about measures they can take themselves, such as *"using specific types of software or encryption technologies"*.[80] The legislator, though, clarifies that the obligation of the providers to inform the subscribers does not mean that the former shall not *"take, at [their] own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service"*.[81] Therefore, the providers must not "rest on their laurels" due to the fact that they have informed the subscribers. Finally, the provision of the information to the subscribers shall be free of charge apart

[77] Ibid, art, 4 (1a).
[78] Lloyd, Ian. "Information Technology Law". 9th Edition. Oxford University Press, p. 122.
[79] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, recital 20.
[80] Ibid.
[81] Ibid.

from *"any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message"*.[82]

The e-Privacy Directive imposes obligations mainly to the providers of the electronic communications services. They are charged, among others, with the obligation to ensure the security of data processed during the provision of their services. However, in art. 5 obligations are also imposed to the Member States which shall ensure through the implementation of legal acts the confidentiality of the content of communications and of traffic data and prohibit *"listening, tapping, storage or other kinds of interception or surveillance"*.[83] Furthermore, they must enforce penalties to those who violate these laws, which shall be *"effective, proportionate and dissuasive"*.[84]

1.4.2 Notification of a data breach

In case of a personal data breach, the Directive imposes on the providers of electronic communications services an obligation to notify the competent national authorities about this breach without undue delay. The Directive defines the personal data breach as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community"*.[85]

If the breach has an adverse impact on the subscribers' or individuals' personal data or privacy, they shall be notified as well without delay. The impact of a data breach on the individuals' personal data and privacy is a common place nowadays due to the extensive use of mobile communications. The providers are discharged from their obligation to notify the affected data subjects if they have informed the competent authority that they have enforced all the appropriate protective measures both generally and regarding to the data affected by the security breach. Moreover, if the provider has not notified the subscribers or individuals concerned, the former may be asked by the national competent authorities to do so, when the latter have assessed that such an adverse impact on the data subjects exists.

[82] Ibid.
[83] Ibid, art. 5 (1).
[84] Ibid, art. 15a (1).
[85] Ibid, art. 2 (i).

The notification to the subscribers or individuals affected shall at least contain a description of the breach, contact details for additional information and recommendations about measures to prevent further possible effects. The notification to the competent authorities shall contain, additionally to the aforementioned information, a description of the consequences and of the proposed or already adopted measures to remedy the breach.[86]

This provision on data breach notification was a novelty at the time it was adopted -it was introduced in the e-Privacy Directive with the amendment of 2009-, since it was not provided in the Data Protection Directive. After the enforcement of the GDPR, the data breach notification applies to all personal data irrespective of the sector involved.

1.5 The relationship with GDPR and the Directive of Electronic Commerce

When the e-Privacy Directive was adopted, the Data Protection Directive (Directive 95/46/EC) was in force and therefore all the references in the e-Privacy Directive regarding the data protection regime are in relation with the Data Protection Directive. As already mentioned, the e-Privacy Directive constitutes *"lex specialis"* towards the Data Protection Directive and *"particularizes and complements"* the latter's provisions. The GDPR came to confirm this relationship between the two legal acts as it explicitly states in art. 95 that *"This Regulation [i.e. the GDPR] shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC"*.[87] Regarding the matters which are not specifically regulated under the e-Privacy Directive, the *"lex generalis",* GDPR, will apply.[88]

The European legislator, though, has recognized the need for a review of the e-Privacy Directive, in order to be in conformity with GDPR.[89] Due to the fact that the process of the review of the e-Privacy Directive has taken longer than expected, as will be presented below, the European Data Protection Board (EDPB) has issued

[86] Ibid, art. 5 (3).
[87] See REGULATION (EU) 2016/679, General Data Protection Regulation, art. 95.
[88] Ibid, recital 173.
[89] Ibid.

Opinion 5/2019,[90] in order to provide clarifications on the relationship between the two legal acts.

The aforementioned opinion clarifies that although the e-Privacy Directive may require a specific legal basis for the processing of a specific category of data (e.g. consent by the users or subscribers for the processing of traffic data), this does not mean that such processing shall not comply with the other principles of processing as enshrined in GDPR, such as the principle of lawfulness and fairness.[91]

Moreover, the aforementioned article of GDPR, which clarifies the "lex specialis"-"lex generalis" relationship between the two legal acts, also aims to avoid imposing on the controllers *"unnecessary administrative burdens"*.[92]

On the other hand, the e-Commerce Directive (Directive 2000/31/EC) harmonizes specific national provisions regarding information society services. As already noted, the Framework Directive provides in art. 2 (c) that information society services *"which do not consist wholly or mainly in the conveyance of signals on electronic communications networks"* do not constitute electronic communications services. In principle, information society services do not fall within the scope of the e-Privacy Directive. However, when the conveyance of signals forms the exclusive or the most significant aspect of them, information society services, such as video on demand services[93] provided also that they relate to an identifiable user or subscriber, fall within the scope of the e-Privacy Directive.

In principle, the scope of application of the e-Privacy Directive and the one of the e-Commerce Directive do not coincide, apart from the case mentioned above. However, the rule of art. 5 (3) of the e-Privacy Directive regarding the storage of information or the access to information in the terminal equipment of a user or subscriber is a *"general provision"*[94] that applies not only to electronic communications service providers but also to information society service providers. The provisions regarding the processing of location data and the unsolicited communications, though, do not apply to information service providers.[95]

[90] Etteldorf, Christina. "EDPB on the Interplay between the ePrivacy Directive and the GDPR." European Data Protection Law Review (EDPL), vol. 5, no. 2, p. 224-225.
[91] See EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, para. 39.
[92] Ibid, para. 44.
[93] See DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, recital 18 in conjunction with DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, recital 16.
[94] Dumortier, Jos. "Evaluation and Review of the ePrivacy Directive." European Data Protection Law Review (EDPL), vol. 2, no. 2, 2016, p. 248.
[95] Ibid.

Hence, the e-Privacy Directive may be complementary to the e-Commerce Directive when the information society services are electronic communications services as well. The rule of art. 5 (3) of the e-Privacy Directive, though, applies to information society service providers irrespective of whether their activities fall within the scope of the e-Privacy Directive or not.

2. Data Retention: Lessons from the CJEU

2.1 The Data Retention Directive (Directive 2006/24/EC)

The response of the European legislator to the terrorist attacks in Madrid in 2004 and in London in 2005 was the adoption of the Data Retention Directive (Directive 2006/24/EC), although relevant discussions had already started in 2001 after the attack at the World Trade Center.[96] The Justice and Home Affairs Council of 2002 perceived the electronic communications and data relating to these as a means to combat criminal offences and organized crime. The reason for this was the extensive use of electronic communications.[97] Before the adoption of the abovementioned Directive, the first attempt for the implementation of the retention of communications data was the "Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism". The aim of the Framework Decision was *"the facilitation of judicial cooperation in criminal matters"*.[98] This proposal was abandoned because of concerns that had been raised by the European Parliament and the data protection authorities about its compatibility with the right to privacy and with the principle of proportionality and about its legal basis.[99]

Directive 2006/24/EC entered into force in 2006 and Member States were obliged to transpose it in their national legislations until September 15, 2007. The Directive provided for the obligation of the providers of publicly available electronic communications services or of public communications networks to retain specific data *"generated or processed by them"*[100] and make them available to the competent

[96] Galli, Francesca. "Digital Rights Ireland as an Opportunity to Foster a Desirable Approximation of Data Retention Provisions." Maastricht Journal of European and Comparative Law, vol. 23, no. 3, 2016, p. 460.
[97] See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, Recital 7.
[98] Council Document 8958/04, art. 1.
[99] Vainio, Niklas, and Samuli Miettinen. "Telecommunications Data Retention after Digital Rights Ireland: Legislative and Judicial Reactions in the Member States." International Journal of Law and Information Technology, vol. 23, no. 3, Autumn 2015, p. 292.
[100] Ibid, art. 1 para. 1.

authorities of the Member States *"for the purpose of investigation, detection and prosecution of serious crime"*.[101] The European Data Protection Supervisor (EDPS) and the Article 29 Working Party of the Directive 95/46/EC had raised concerns about the necessity, the proportionality[102] and the ambiguity[103] of the provisions of the Directive.

The aim of the Data Retention Directive was the approximation of national laws since many Member States had adopted their own legal acts on data retention for combating criminal offences. This imposed a burden on the proper function of the internal market and on electronic communications providers whose obligations diverged among Member States[104] and who had to adapt to different costs, a fact that could lead to the distortion of competition.[105]

The Data Retention Directive established a derogation from the e-Privacy Directive[106] and particularly from the provision of articles 5, 6, 9 and 15 (1) of that Directive, as it set the framework for the obligation of the telecommunications and the Internet Service Providers (ISPs) to retain traffic and location data, namely metadata. Article 5 of the Data Retention Directive obliged Member States to adopt the necessary legislation to ensure that data relating to a) the source of communication (calling phone number, personal information about the subscriber or registered user, IP address, user ID), b) the destination of communication (telephone numbers called and personal information of the subscriber or registered user, user ID of the recipient), c) the date, time and duration of a communication and access to the internet, d) the type of communication, e) the user's communication equipment and f) the location of mobile communication equipment are retained. It was clearly stated, though, that *"no data revealing the content of the communication may be retained"*.[107]

These categories of data must be retained for a minimum period of six months and a maximum period of two years[108] and the precise period would be specified by the national legislators. The procedures and the conditions regarding access to these retained data was also left at the discretion of the national legislator[109] which means

[101] Ibid.
[102] Vainio, Niklas, and Samuli Miettinen. "Telecommunications Data Retention after Digital Rights Ireland: Legislative and Judicial Reactions in the Member States." International Journal of Law and Information Technology, vol. 23, no. 3, Autumn 2015, p. 290-291.
[103] Galli, Francesca. "Digital Rights Ireland as an Opportunity to Foster a Desirable Approximation of Data Retention Provisions." Maastricht Journal of European and Comparative Law, vol. 23, no. 3, 2016, p. 467.
[104] See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, art. 1 para. 1 in conjunction with Recitals 5 and 6.
[105] Galli, Francesca. "Digital Rights Ireland as an Opportunity to Foster a Desirable Approximation of Data Retention Provisions." Maastricht Journal of European and Comparative Law, vol. 23, no. 3, 2016, p. 463.
[106] See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, art. 3 para. 1.
[107] Ibid, art. 5 para. 2.
[108] Ibid, art. 6.
[109] Ibid, art. 4.

that any authority could have access to these data -not only criminal justice authorities- and without the need of prior judicial authorization.[110] Another issue that was not ruled by the Directive but was left to the national legislator was the definition of "serious crime",[111] which meant that Member States could adopt a very broad definition that could lead to the extensive access to and to the subsequent use of the metadata. The Commission's Evaluation Report of the Data Protection Directive in 2011 showed that Member States actually used their discretion by allowing several national authorities, such as the police, tax authorities, security or intelligence services, to have access to these data.[112]

Although it was declared in Recital 22 that *"the Directive respects the fundamental rights and the principles recognized by the Charter of Fundamental Rights of the European Union"*, serious concerns were raised by the Member States about the compatibility of the Directive and of the laws which transposed it in the national legal systems with the right to privacy and to protection of personal data. Specifically, by 2011, when the Commission's Evaluation Report was issued, only 25 Member States had transposed the Directive in their national legal systems. Austria and Sweden were the two countries which had not done so whereas Belgium had done it only partially. Furthermore, cases challenging the compatibility of the national laws transposing the Directive with the fundamental rights as enshrined in the Member States' constitutions were brought before the supreme courts of Bulgaria, Romania, Germany, Cyprus and the Czech Republic. A case was also brought before the Hungarian Supreme Court but it was terminated because of restrictions placed on filing cases before the Constitutional Court. All the courts found that the national provisions infringed fundamental rights and were therefore, unconstitutional. However, none of them ruled on the validity of the Directive.[113]

In 2006 the Data Retention Directive was directly called in question by Ireland before the Court of Justice of European Union (CJEU), where it requested the Court to annul the Directive, *"on the ground that it was not adopted on an appropriate legal basis"*.[114] Ireland, supported by the Slovak Republic, argued that art. 95 EC (now art.

[110] Guild, Elspeth, and Carrera, Sergio. "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive". CEPS Liberty and Security in Europe Papers No. 65, May 2014, p. 3.
[111] Rauhofer, Judith, and Daithi Mac Sithigh. "The Data Retention Directive Never Existed." SCRIPTed: A Journal of Law, Technology and Society, vol. 11, no. 1, April 2014, p. 119.
[112] Ojanen, Tuomas. "Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12." European Constitutional Law Review, vol. 10, no. 3, December 2014, p. 530-531.
[113] Fabbrini, Federico. "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States." Harvard Human Rights Journal, 28, 2015, p. 75.
[114] Case C-301/06 Ir. v. Parliament and Council of the European Union, 2009, para. 1.

114 TFEU) was an inappropriate legal basis as *"the sole objective or, at least, the main or predominant objective of that directive is to facilitate the investigation, detection and prosecution of crime, including terrorism and its 'centre of gravity' does not concern the functioning of the internal market. Therefore, the only legal basis on which the measures contained in Directive 2006/24 may be validly based is Title VI of the EU Treaty, in particular Articles 30 EU, 31(1)(c) EU and 34(2)(b) EU"*. [115] In other words, the Irish government claimed that the Directive's main objective was law enforcement.[116] On the other hand, the European Parliament, supported by the Kingdom of Spain, the Kingdom of the Netherlands, the Commission of the European Communities and the European Data Protection Supervisor, argued that *"Recitals 5 and 6 in the preamble thereto make it clear that the main or predominant purpose of that directive is to eliminate obstacles to the internal market for electronic communications services, while recital 25 confirms that the access to and use of the retained data for law-enforcement purposes fall outside the scope of Community competence"*.[117] On the same path, the Council claimed that *"the need to combat crime, including terrorism, was a determining factor in the decision to amend the scope of the rights and obligations laid down in Articles 5, 6 and 9 of Directive 2002/58, that circumstance did not prevent Directive 2006/24 from having to be adopted on the basis of Article 95 EC. Neither Articles 30 EU, 31 EU and 34 EU nor any other article in the EU Treaty can serve as the basis for a measure which, in substance, has the objective of amending the conditions under which service providers carry out their activities or of making the system established by Directive 2002/58 inapplicable to them"*.[118]

The CJEU found in 2009 that *"it is apparent that the differences between the various national rules adopted on the retention of data relating to electronic communications were liable to have a direct impact on the functioning of the internal market and that it was foreseeable that that impact would become more serious with the passage of time. Such a situation justified the Community legislature in pursuing the objective of safeguarding the proper functioning of the internal market through the adoption of harmonized rules"*.[119] It, therefore, dismissed the action. However, Advocate General (AG) Cruz Villalon in his opinion on joined cases C-293/12 and C-593/12, even though he declared the accuracy of the CJEU's ruling that the predominant objective of the Directive is the proper function of the internal market,

[115] Ibid, para. 28 and 58.
[116] Guild, Elspeth, and Carrera, Sergio. "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive". CEPS Liberty and Security in Europe Papers No. 65, May 2014, p. 4.
[117] Case C-301/06 Ir. v. Parliament and Council of the European Union, 2009, para. 35.
[118] Ibid, para. 43 and 44.
[119] Ibid, para. 71 and 72.

recognized that there is an "ultimate"/ "background" objective and used these words interchangeably. This "ultimate objective" is the prevention of serious crime.[120] He then asked whether under art. 5(4) TEU the issues of stricto sensu proportionality of the Directive with the "predominant" objective that it pursues can be resolved by considering the "background" objective of the Directive. It is significant that the AG used the word "ultimate". Even though he declared explicitly that the issue of the legal basis of the Directive has been validated and he did not challenge it, it can be inferred by the use of the word "ultimate" that he recognized that the "center of gravity" of the Directive was indeed the prevention of serious crime. More clearly than the AG, the CJEU in the later case Digital Rights Irelands, stated that *"the material objective of the directive is to contribute to the fight against serious crime and, thus, ultimately to public security"*[121] by contradicting in this way its previous finding and by placing law enforcement as the main objective of the Directive.

It is remarkable that the CJEU in the case Ireland v. Parliament and Council stressed that *"the action brought by Ireland relates solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006/24"*[122]*,* by leaving in this way room for the challenge of the compatibility of the Directive with fundamental rights.

2.2 Digital Rights Ireland: A real triumph for privacy?

Two references from Ireland and Austria for a preliminary ruling were the sparkles that triggered the CJEU's landmark judgement of 2014. The CJEU was now faced with the validity of the Data Retention Directive and its compatibility with fundamental rights as enshrined in the EU Charter of Fundamental Rights. Case C-293/12 started from an action before the High Court of Ireland by a Non-Governmental Organization called "Digital Rights Ireland", the object of which is the promotion and protection of civil and human rights in the field of communication technologies,[123] about the *"legality of national legislative and administrative measures"* [124] concerning the retention of electronic communications data. Case C-594/12 initiated from an action brought before the Constitutional Court of Austria by the Government of the Province

[120] Opinion of Advocate General Cruz Villalon on Cases C-293/12 and C-593/12, 12 December 2013, para. 102 and 103.
[121] Joined Cases C-293/12 and C-593/12, Digital Rights Ireland Ltd. and others, para. 40.
[122] Ibid, para. 57.
[123] Opinion of Advocate General Cruz Villalon on Cases C-293/12 and C-593/12, 12 December 2013, para. 10.
[124] Joined Cases C-293/12 and C-593/12, Digital Rights Ireland Ltd. and others, para. 2.

of Carinthia and by Mr Seitlinger and 11,129 other applicants about the compatibility of the Austrian national law implementing the Data Retention Directive with the Federal Constitutional Law.

Both courts stayed proceedings and referred to the CJEU. Both courts asked whether Directive 2006/24 is in accordance with the right to privacy, the right to protection of personal data and the right to freedom of expression as laid down in Articles 7, 8 and 11 of the Charter respectively. The Irish Court also asked whether the Directive is compatible with the right to move and reside freely within the territory of Member States as established in Article 21 TFEU and with the right to good administration as enshrined in Article 41 of the Charter. The Austrian Court recognized that data retention influences *"almost exclusively persons whose conduct in no way justifies the retention of data relating to them"*[125] and challenged the appropriateness of this legal instrument for the attainment of its objectives and the proportionality of interference with the relevant fundamental rights. The further questions the Austrian Court referred concern the relationship between primary and secondary EU law[126] and the relationship between the case-law of the ECtHR and primary EU law. The two cases were joined.

Advocate General Cruz Villalon delivered his opinion in December 2013. AG recognized that the implementation of the Data Retention Directive could have an effect on the exercise of the freedom of expression but he stated that *"that effect would be merely a collateral consequence of interference with the right to privacy"*.[127] He also did not examine in substance the claim of the High Court for the alleged incompatibility of the Directive with Article 21 TFEU and Article 41 of the Charter due to its vagueness and proceeded to examine the compatibility of the Directive with Articles 7 and 8 of the Charter. Firstly, he clarified that the right to privacy and the right to the protection of personal data are two separate rights which belong to the same broad category of privacy rights.[128] The fact that a legal instrument, in casu Directive 2006/24, might be in accordance with the right to privacy as enshrined in Article 7 does not mean per se that it will be compatible with the right to protection of personal data as enshrined in Article 8 of the Charter and vice versa that *"legislation limiting the right to the protection of personal data in compliance with Article 8 of the Charter may nevertheless be*

[125] Ibid, para. 20.
[126] Marin, Luisa. "The Fate of the Data Retention Directive: About Mass Surveillance and Fundamental Rights in the EU Legal Order." Research Handbook on EU Criminal Law, Forthcoming, Criminal Justice, Borders and Citizenship Research Paper No. 2697462, November 2015, p. 8.
[127] Opinion of Advocate General Cruz Villalon on Cases C-293/12 and C-593/12, 12 December 2013, para. 52.
[128] Fabbrini, Federico. "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States." Harvard Human Rights Journal, 28, 2015, p. 77.

regarded as constituting a disproportionate interference with Article 7".[129] After this distinction, he concluded that Article 7 applies to the recording and retention of electronic communications data whereas Article 8 applies to their subsequent processing. As the scope of the Directive covers only the retention of data and not their access and subsequent use by the competent authorities, which was left at the discretion of the national legislator, he took the view that there is no need for further examination of the interference of the provisions of the Directive with Article 8 of the Charter.[130]

In his analysis of the interference of the Directive with Article 7 of the Charter, AG Villalon recognized that the Data Retention Directive *"constitutes a particularly serious interference with the right to privacy",*[131] as communications data retention creates a feeling of constant surveillance and data may be transmitted to third parties. According to the AG, the whole Directive is incompatible with art. 52 (1) of the Charter, as the limitations on fundamental rights imposed by the provisions of the Directive are not followed with the appropriate guarantees for the access to and use of the communications data but rather such guarantees are left at the discretion of the Member States. Furthermore, Article 6 of the Directive which provides for a maximum period of two years for the retention of the data is not in accordance with the right to privacy as enshrined in art. 7 of the Charter and with art. 52 (1) of the same legal instrument because it is not limited to what is strictly necessary and thus, the Directive fails the proportionality test. Even though the AG found the Directive to be invalid for the afore mentioned reasons, he suggested the suspension of this finding until the EU adopts another legal instrument to cover this invalidity.

Due to the importance of the case, the CJEU heard the preliminary references as a Grand Chamber composed by fifteen judges and delivered its decision on April 8, 2014. Firstly, the Court recognized the rights that are affected by the Data Retention Directive, secondly it dealt with the issue whether its provisions intervene with these fundamental rights and finally it examined the implementation of art. 52 (1) of the Charter on this interference.

The CJEU recognized that the rights affected by the provisions of the Directive are those of privacy, protection of personal data and freedom of expression as laid down in Articles 7, 8 and 11 of the Charter respectively. Regarding the latter, it clarified

[129] Opinion of Advocate General Cruz Villalon on Cases C-293/12 and C-593/12, 12 December 2013, para. 61.
[130] Rauhofer, Judith, and Daithi Mac Sithigh. "The Data Retention Directive Never Existed." SCRIPTed: A Journal of Law, Technology and Society, vol. 11, no. 1, April 2014, p. 121.
[131] Opinion of Advocate General Cruz Villalon on Cases C-293/12 and C-593/12, 12 December 2013, para. 70.

that even though *"the Directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression"*.[132] However, it focused its analysis on the rights to privacy and protection of personal data, which conceived them as two distinct rights, as the AG did.[133] The judges recognized that the categories of data to be retained *"may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them"*.[134] Unlikely AG Villalon, the CJEU ruled that the retention of the data itself, not only the subsequent access to and use of the data, constitutes an act of processing and therefore falls within the scope of Article 8 of the Charter.[135]

Subsequently, the CJEU confirmed that both the obligations imposed on electronic communications service providers for the bulk retention of metadata and the access to these data by the competent authorities constitute an intervention with the right to privacy and with the right to protection of personal data and are two separate interferences.[136] It also stated that the nature of the data, meaning whether they are sensitive or not, does not play a role in the existence of such an intervention. Confirming the AG's suggestions, the Court also found that this interference is "particularly serious" because the bulk retention of data and their subsequent use *"without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance"*.[137]

The CJEU proceeded then with the examination of the application of art. 52 (1) of the Charter in order to determine whether this interference is justified. The prerequisites set by this article are that any limitation on the exercise of rights and freedoms: a) must be provided for by law, b) respect their essence and c) be in accordance with the principle of proportionality, meaning that the limitation is

[132] Joined Cases C-293/12 and C-593/12, Digital Rights Ireland Ltd. and others, para. 28.
[133] Ibid, para. 29.
[134] Ibid, para. 27.
[135] Ibid, para. 29.
[136] Marin, Luisa. "The Fate of the Data Retention Directive: About Mass Surveillance and Fundamental Rights in the EU Legal Order." Research Handbook on EU Criminal Law, Forthcoming, Criminal Justice, Borders and Citizenship Research Paper No. 2697462, November 2015, p. 9.
[137] Joined Cases C-293/12 and C-593/12, Digital Rights Ireland Ltd. and others, para. 37.

appropriate and necessary for the objective pursued. The CJEU did not analyze at all the first prerequisite but implicitly accepted that it is met since it referred to some aspects of it.[138] In the examination of the second prerequisite it drew an even clearer line for the distinction of the rights to privacy and to protection of personal data, as mentioned above, since it examined the effect of the interference on the essence of the two rights separately.

The Court held that the essence of the right to privacy is not affected. It based this finding on the fact that the Directive does not *"permit the acquisition of knowledge of the content of electronic communications"*.[139] It seems that the CJEU made a distinction between metadata and the content of the electronic communications and considered the latter to constitute a more serious intervention with the right to privacy. However, the Court did not provide for any reasons for this view. It seems that it considered the effect on the essence of the right "quantitatively" rather than "qualitatively",[140] meaning that the effect on the essence of the right is to be determined based on the degree of the interference – it is not sufficient to be particularly serious- rather than on the kind of the intervention.[141] In a world, where technology develops rapidly and electronic communications become an even more important part of our everyday lives, retention of location and traffic data can reveal such information, including sensitive, as the content of communications does.

Concerning the essence of the right to protection of personal data, similarly the CJEU held it is not affected because the electronic communications providers must comply with certain data protection and data security principles.[142]

As mentioned above, the CJEU by contradicting its previous finding in Ireland v. European Parliament and Council accepted that the material objective of the Directive is to combat serious crime and examined the application of the principle of proportionality on the basis of this objective. Firstly, it found that *"the fight against serious crime"* is an objective that serves the general interest and due to the extensive use of electronic communications the retention of data relating to these to allow possible access to them by the competent authorities serves an objective of general

[138] Ojanen, Tuomas. "Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12." European Constitutional Law Review, vol. 10, no. 3, December 2014, p. 536.
[139] Joined Cases C-293/12 and C-593/12, Digital Rights Ireland Ltd. and others, para. 39.
[140] Brkan, Maja. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning." The Essence of Fundamental Rights in EU Law, 17-18 May 2018, Leuven, p. 9.
[141] Ibid.
[142] Joined Cases C-293/12 and C-593/12, Digital Rights Ireland Ltd. and others, para. 40.

interest.[143] After citing the ECtHR case law,[144] it stressed that its review of the Directive will be strict because of *"the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24"*.[145]

Regarding the first fold of the proportionality test, namely appropriateness, the CJEU accepted that the retention of electronic communications data is an appropriate means for the achievement of the legitimate aim pursued by the Directive. As far as the second fold is concerned, that of necessity, the CJEU found that the Data Retention Directive was not necessary for the purpose of the fight against serious crime and was, thus, disproportionate. The Court clarified that the protection of personal data is significant for the right to privacy and as AG in his Opinion, placed the two rights, which are distinct, under the same "family", with the right to protection of personal data being supplementary to that of privacy and covering the respect for privacy when personal data are processed.[146]

The CJEU based its reasoning on the following facts:

a) The Directive *"covers, in a generalized manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime"*.[147] There were no limitations on the personal scope of the Directive but it covered anyone, even though there were no sufficient indications for his/her direct or indirect involvement in serious crime. It even covered persons, who were subject to professional secrecy.
b) The Directive did not limit the scope of the data to be retained but covered all communications data. There was no requirement for these to be linked with a threat to public security, for example by being restricted to *"data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences"*.[148]

[143] Ibid, para. 42-44.
[144] Ibid, para. 47.
[145] Ibid, para. 48.
[146] Guild, Elspeth, and Carrera, Sergio. "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive". CEPS Liberty and Security in Europe Papers No. 65, May 2014, p. 7.
[147] Joined Cases C-293/12 and C-593/12, Digital Rights Ireland Ltd. and others, para. 57.
[148] Ibid, para. 59.

c) The provisions of the Directive were rather vague and left too much discretion to the national legislators since they failed to establish *"any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that […] may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law"*.[149] The Directive restricted neither the purpose of the access and use of the retained data to the prevention of serious crime nor the number of people who are authorized to access these data. Furthermore, it did not make access and use of the data subject to prior judicial or administrative review.

d) The data retention period which is between six and twenty-four months applies to all data irrespective of the categories of the data and their *"possible usefulness for the purposes of the objective pursued or according to the persons concerned"*.[150] The determination of the exact period was left at the discretion of the national legislators without providing that this determination shall be based on objective criteria in order to be limited to what is strictly necessary.

e) Finally, the Directive failed to provide adequate safeguards for the protection of the data retained *"against the risk of abuse and against any unlawful access and use of that data"*[151] and did not require that the data are retained within the EU, which could lead to a very low level of protection because it cannot be controlled that the providers comply with the EU regime.

The CJEU found that the Directive failed to pass the proportionality test and held that there is no need to examine the other questions. It concluded with the simple phrase *"Directive 2006/24/EC is invalid"*. The importance of this ruling lays on the fact that the CJEU did not let the exception, i.e. mass surveillance, become the rule[152] and did not sacrifice privacy in the altar of terrorism and crime. By finding, however, that the essence of the rights to privacy and to protection of personal data is not affected,

[149] Ibid, para. 60.
[150] Ibid, para. 61.
[151] Ibid, para. 66.
[152] Marin, Luisa. "The Fate of the Data Retention Directive: About Mass Surveillance and Fundamental Rights in the EU Legal Order." Research Handbook on EU Criminal Law, Forthcoming, Criminal Justice, Borders and Citizenship Research Paper No. 2697462, November 2015, p. 11.

it left room for the enforcement of data retention laws, which must comply though with strict requirements in order to pass the proportionality test. These requirements are provided a contrario[153] by the CJEU's ruling and are summarized as follows:

a) They shall contain *"clear and precise rules on their scope and application"* and provide minimum safeguards for the effective protection of data against unauthorized access, misuse and abuse,[154]
b) The personal scope of the laws shall cover only persons for whom sufficient evidence exists that they are directly or indirectly involved in serious crimes. Persons who are subject to professional secrecy must be excluded,
c) The scope shall be limited to the retention of data relating to a threat and specifically, relating to a specific time period and/or geographical zone and/or people who are suspected of involving in serious crime or could contribute to combat it,
d) They shall set *"substantive and procedural conditions"*[155] for the access and subsequent use of the data retained by the competent authorities, the purpose of this kind of processing shall be explicitly limited only to the investigation of crime, the determination of the authorized persons shall be based on objective criteria and their number shall be limited to what is strictly necessary,
e) Access and use of the data shall be subject to prior judicial or administrative review,
f) They shall set objective criteria for the determination of the period of retention and this period must vary according to the categories of data retained,
g) They shall provide clear and strict rules to ensure the *"integrity and confidentiality*" of personal data taking into account the *"vast quantity, the sensitive nature and the risk of unlawful access to the data"*[156]
h) They shall provide that the electronic communications service providers shall take all the appropriate technical and organizational measures to ensure a high level of protection and security of the personal data and the data shall be destroyed after the retention period,
i) They shall provide that the data shall be retained only within the EU.

[153] Galli, Francesca. "Digital Rights Ireland as an Opportunity to Foster a Desirable Approximation of Data Retention Provisions." Maastricht Journal of European and Comparative Law, vol. 23, no. 3, 2016, p. 470.
[154] Joined Cases C-293/12 and C-593/12, Digital Rights Ireland Ltd. and others, para. 54.
[155] Ibid, para. 61.
[156] Joined Cases C-293/12 and C-593/12, Digital Rights Ireland Ltd. and others, para. 66.

Apart from the abovementioned reasons, Digital Rights Ireland decision was a milestone because the CJEU reviewed secondary EU law in the light of its compatibility with fundamental rights as enshrined in the Charter in a strict manner[157] and for the first time invalidated a Directive in its entirety due to its incompatibility with the provisions of the Charter.[158] Unlikely AG Villalon who suggested to suspend the invalidity of the Directive until the EU adopts another legal instrument to cover this invalidity, the Court did not set any restriction on the temporal effect of its ruling. The invalidity is retrospective running at the time the Directive was put into force. The decision was welcomed by the EDPS who saw that the Court set a new challenge to the EU *"to take a firm position in discussions with third countries, particularly the USA, on the access and use of communications data of EU residents"*.[159]

The consequence of the declaration of the invalidity of the Data Retention Directive was that it led to a void. Regarding the national laws that transposed the Directive in the Member States, they were not per se invalid except for those of Ireland and Austria which were bound by the CJEU and had to comply with its ruling.[160] The EU law does not regulate what happens in such cases and therefore, the response of the national authorities to the CJEU's judgement differentiated with some courts invalidating the national laws that transposed the Directive, like it happened in Romania, Slovenia and Bulgaria,[161] Slovakia and the Netherlands[162] whereas other countries like UK and France maintained in force data retention laws.[163] The UK after the annulment of the Directive adopted emergency legislation, the Data Retention and Investigatory Powers Act 2014 (DRIPA), while France reacted before the invalidation of the Directive by adopting several data retention laws.[164] In any case, it must be borne in mind that 15 (1) of the e-Privacy Directive provides a legal basis for Member States to adopt laws allowing the retention of electronic communications data for reasons of *"national security, prevention, investigation, detection and prosecution of*

[157] Ojanen, Tuomas. "Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12." European Constitutional Law Review, vol. 10, no. 3, December 2014, p. 529.
[158] Rauhofer, Judith, and Daithi Mac Sithigh. "The Data Retention Directive Never Existed." SCRIPTed: A Journal of Law, Technology and Society, vol. 11, no. 1, April 2014, p. 119.
[159] Guild, Elspeth, and Carrera, Sergio. "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive". CEPS Liberty and Security in Europe Papers No. 65, May 2014, p. 9.
[160] Fabbrini, Federico. "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States." Harvard Human Rights Journal, 28, 2015, p. 88.
[161] Nesterova, Irena. "Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards." European Society of International Law (ESIL) 2016 Annual Conference (Riga), January 2017, p. 11.
[162] Vainio, Niklas, and Samuli Miettinen. "Telecommunications Data Retention after Digital Rights Ireland: Legislative and Judicial Reactions in the Member States." International Journal of Law and Information Technology, vol. 23, no. 3, Autumn 2015, pp. 301-303
[163] Drewry, Lawrence. "Crimes without Culprits: Why the European Union Needs Data Retention, and How It Can Be Balanced with the Right to Privacy." Wisconsin International Law Journal, vol. 33, no. 4, 2015, p. 737.
[164] Ibid, p. 738.

criminal offenses".[165] Such laws, though, must respect the fundamental rights of privacy and protection of personal data and comply with the principles and safeguards the CJEU set. After the annulment of the Directive, both national legislators and courts had to review their national laws regarding data retention to ensure that they comply with the Charter and the principles laid down by the court.

Data retention was not condemned by the CJEU as such. It does not interfere with the essence of the rights to privacy and to protection of personal data. What was condemned was the lack of proportionality and the bulk retention of electronic communications data which affected the entire European population.

2.3 In the aftermath of Digital Rights Ireland: ECtHR's and CJEU's case law

The European Court of Human Rights (ECtHR) in cases Zakharov v. Russia and Szabó and Vissy v. Hungary dealt with mass surveillance. In the first case a complaint was filed by Mr. Zakharov before the ECtHR that the existence of a law providing for mobile communications interception by the Russian competent authorities was incompatible with art. 8 of the European Convention on Human Rights (ECHR). In the second case the complaint concerned the incompatibility of laws providing for surveillance of the content of communications for reasons of national security with art. 8, 6 and 13 of ECHR. In both cases the complaints were accepted by the Court on the basis that such laws, even though they pursued a legitimate aim, i.e. national security, combating of crime and the *"protection of economic well-being"*,[166] went beyond what is strictly necessary. The Court set the conditions that secret surveillance laws must meet in order to pass the necessity test but it clarified that such legislation will pass this test only "*under exceptional circumstances"*.[167] The influence of the ECtHR by the CJEU's ruling in Digital Rights Ireland is apparent in the former's reasoning in the aforementioned cases, as the minimum standards the secret surveillance laws must meet are similar to those the CJEU set, such as the requirement of "foreseeability", in the sense that the provisions must be clear and precise. In Szabó and Vissy v. Hungary the ECtHR directly cited the CJEU's decision as the involved party was a Member State. It must be noted, though, that the difference between these cases lays on the fact that the ECtHR's cases concerned the content of

[165] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 15 (1).
[166] Zakharov v. Russia, para. 237.
[167] Cole Mark D., and Annelies Vandendriessche. "From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabo/Vissy in Strasbourg." European Data Protection Law Review (EDPL), vol. 2, no. 1, 2016, p. 127.

communications whereas the cases before the CJEU concerned the retention of metadata.

After the Digital Rights Ireland decision, concerns were raised within the EU regarding the compatibility of national laws providing for communications data retention with the Charter and regarding the application of the principles set in Digital Rights Ireland. The first case in which the CJEU dealt with these issues was the joined case Tele 2 Sverige AB v. Post-och telestyrelsen (C-203/15) and Secretary of State for the Home Department (C-698/15) v. Tom Watson and others. In particular, the former case is between a Swedish electronic communications provider, Tele 2 Sverige AB, and the Swedish Post and Telecom Authority (PTS) because the provider after the annulment of the Data Retention Directive refused to retain metadata and notified the PTS that it would erase any data it had retained. The PTS then ordered the provider to continue to retain metadata because it was obliged to do so according to the national legislation. The Swedish Court then referred to the CJEU and asked whether *"a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter"*.[168] In case it is not compatible, the Court further asked whether the retention is permitted if it is followed by sufficient safeguards regarding access and data protection and by a maximum period of six months for the retention. The latter case is between Tom Watson and others and the Secretary of State for the Home Department regarding the compatibility of the first section of DRIPA with EU law. The UK court asked whether *"the Digital Rights judgment lays down mandatory requirements of EU law applicable to a Member State's domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of the Charter"*.[169]

The CJEU first ruled whether national legislation providing for the retention of communications data and access to these data for national security and law enforcement purposes falls within the scope of the e-Privacy Directive. The answer was in the affirmative since both the retention of data and granting access to the competent authorities constitutes an act of processing on behalf of the communications service providers. Data retention forms a unit with the subsequent access to the data by the competent authorities and the purpose of such legislation is

[168] Joined Cases C-203/15 and C-698/15, Tele 2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others, para. 50.
[169] Ibid, para. 59.

to *"make data accessible to the competent national authorities"*.[170] Thus, such legislation falls within the scope of the e-Privacy Directive according to art. 1. The CJEU proceeded then by confirming and "extending" its ruling in Digital Rights Ireland.[171] Firstly, it stressed that national laws providing for data retention constitute an interference not only with art. 7 and 8 of the Charter but also with art. 11, the right to freedom of expression. Secondly, it is remarkable that it confirmed that metadata *"provide the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications"*,[172] by equating in this way metadata with the content of communications, a point on which the Court was criticized in its former ruling. It then answered that "*general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication is not permitted"*.[173] Art. 15 (1) which is an exception to the principle of confidentiality as enshrined in art. 5 (1) of that Directive must be interpreted strictly and the objectives laid down in this article are exhaustive. Unlikely Digital Rights Ireland decision where the CJEU recognized the failures of the Data Retention Directive, in this case it listed in a positive manner the conditions that national legislations must meet in order to pass the proportionality test. Additionally to the requirements set by the CJEU in Digital Rights Ireland, it demanded notification of the persons, the data of whom have been accessed by the authorities. Even though the Court did not refer to mandatory requirements, it is clear that these conditions are mandatory.[174] In this list it cites the aforementioned cases of the ECtHR.

It must be stressed that while listing the requirements regarding access to metadata by the competent authorities – i.e. link between the data and the objective pursued and individuals *"suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime"*-[175] the Court recognized that in cases of threat of national security due to terrorist activities *"access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities"*[176] and that access can escape

[170] Ibid, para. 79.
[171] O'Leary, Siofra. "Balancing Rights in a Digital Age." Irish Jurist, 59, p. 86.
[172] Joined Cases C-203/15 and C-698/15, Tele 2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others, para. 99.
[173] Ibid, para. 112.
[174] Celeste, Edoardo. "The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios." European Constitutional Law Review, vol. 15, no. 1, March 2019, p. 143.
[175] Joined Cases C-203/15 and C-698/15, Tele 2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others, para. 119.
[176] Ibid.

prior judicial or administrative review in urgent cases. Therefore, it could be inferred that bulk data retention could pass the necessity test if it could contribute to the prevention of serious threats to national security.[177]

The CJEU dealt with this issue in the cases Privacy International (C-623/17) and in La Quadrature du Net (joined cases C-511/18, C-512/18 and C-520/18). The referring courts asked in essence whether the requirements set in Tele 2 case apply in data retention laws for purposes of national security. The Court ruled that general and indiscriminate retention and transmission of metadata, which takes place permanently and without the existence of any serious threat,[178] is not allowed. However, in La Quadrature du Net it ruled that bulk data retention could be permitted for the purposes of combatting *"a genuine, present or foreseeable serious threat to national security"*[179] subject to prior judicial or administrative review. The aim of such review is to confirm that a threat exists, that the strict conditions established are followed and that such retention takes place only for the time that is strictly necessary to the aim pursued. This time, though, can be extended in the case where the threat continues to exist.[180]

The CJEU therefore drew a line between data retention laws for law enforcement and national security purposes. In the first case bulk data retention is not allowed because it exceeds what is strictly necessary whereas in the second case it is permitted when strict requirements are met.

In the recent case C-140/20 (G.D. v. Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General), the judgement on which was issued in April 2022, the CJEU, as a Grand Chamber, by citing the caseσ La Quadrature du Net (the findings of which on data retention for the purposes of combating serious crime will be analyzed under this case for the avoidance of repetitions) and Prokuratuur, provided further clarifications on data retention and access to data for the purposes of combating serious crime and preventing serious threats to public security. The case commenced again from Ireland, which referred to the CJEU. The Court once again stressed that art. 15 (1) of the e-Privacy Directive is an exception to the principle of confidentiality, as enshrined in the

[177] Rojszcak, Marcin. "National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts." European Constitutional Law Review, 17, 2021, p. 614-615.
[178] Ibid, p. 623.
[179] Zalnieriute, Monika. "A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union." Modern Law Review, 85(1) MLR, p. 206.
[180] Joined Cases C 511/18, C 512/18 and C 520/18, La Quadrature du Net and Others, para. 168

same Directive, and therefore, the interpretation of this article shall be strict in order not for the exception to become the rule.[181]

The Court proceeded to clarify that the interpretation of art. 15 (1) of the e-Privacy Directive demands striking a balance between the rights to the integrity of the person, to prohibition of torture and inhuman or degrading treatment, to liberty and security and to protection of private life, as enshrined in art. 3, 4, 6 and 7 of the Charter respectively, on the one hand and the rights to respect for communication, to protection of personal data and to freedom of expression on the other hand.[182] For the purposes of finding this balance account shall be taken on the seriousness of the interference and on the proportionality of such interference with the aim pursued.[183]

In case La Quadrature du Net the CJEU found -a finding that is repeated in case Commissioner of An Garda Síochána- that national security surpasses the other objectives laid down in art. 15 (1) of the e-Privacy Directive, among which *"combating serious crime and safeguarding public security"*[184] and hence, the latter cannot be treated like the former, even if the criminal offences concerned are particularly serious. Therefore, the protection of national security justifies bulk data retention whereas for the purposes of combating serious crime and preventing serious threats to public security, only *"targeted and expedited data retention"* [185] is permitted. This *"targeted and expedited retention"* shall be based on personal criteria, i.e. the identification of persons who are *"subject of an investigation or other measures of current surveillance or of a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending",*[186] on geographical criteria and on any other *"objective and non-discriminatory"*[187] criteria, established by the Member States.

It then clarified that as far as the *"expedited retention"* is concerned, Member States may require the electronic communications service providers to retain metadata for a specific time period, after the issuance of a relevant decision by the competent authorities, which is subject to judicial review.[188] Furthermore, the Court emphasized that Member States must lay down clear and precise rules regarding the objectives that such measures may pursue and such measures shall pass the proportionality

[181] Case C-140/20, G.D. v. Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General, para. 40.
[182] Ibid, para. 48-50.
[183] Ibid, para. 53.
[184] Ibid, para. 57.
[185] Ibid, para. 70.
[186] Ibid, para. 78.
[187] Ibid, para. 83.
[188] Ibid, para. 86.

test.[189] An interesting finding of the CJEU in case La Quadrature du Net, which is repeated in this case as well, is that such expedited retention may also cover persons who are not suspects of committing or having organized a serious crime or being a serious threat to public security, such as *"data concerning the victim thereof, and his or her social or professional circle"*, provided that such data are appropriate for combating serious crime or preventing a serious threat to public security.[190]

Even though the CJEU ruled for a *"targeted and expedited retention"*, it also allowed a general and indiscriminate retention only of specific data, namely of *"data relating to the civil identity of users of electronic communications systems and of IP addresses assigned to the source of a connection"*.[191] The CJEU held that the general retention only of the aforementioned categories of data is appropriate, strictly necessary and stricto sensu proportionate for the attainment of the purposes of combating serious crime and preventing a serious threat to public security. A bulk retention of all metadata, however, is not limited to what is strictly necessary but there should be a connection, even an indirect one, between the data and the objective pursued.[192]

It is also significant that the Court stressed that the difficulty in defining the criteria and conditions, under which the targeted retention of traffic and location data may take place, shall not lead to the bulk retention of these data and thus, the exception shall not be turned into a rule.[193] The Court also repeated the principle that the data shall be erased or made anonymous as long as they are no longer necessary for the attainment of the purpose pursued. It gives the option, though, that they may be retained for a longer period *"in order to shed light on serious criminal offences or acts adversely affecting national security"*.[194]

The CJEU dealt with the access to the retained data as well. An important clarification is that the competent authorities shall not have access to metadata, which have been generally and indiscriminately retained for national security purposes but only to those that have been retained for the purposes of combating serious crimes or preventing serious threats to public security.[195] Access shall be granted only when it is strictly necessary for the achievement of the aim pursued and shall be subject to prior judicial or administrative review, which must be carried out before accessing the data

[189] Ibid, para. 87.
[190] Ibid, para. 88.
[191] Ibid, para. 70.
[192] Ibid, para. 95.
[193] Ibid, para. 84.
[194] Ibid, para. 85.
[195] Ibid, para. 98-100.

"except in the event of duly justified urgency, in which case the review must take place within a short time".[196] Finally, the CJEU repeated its settled case-law that in cases where an administrative body is authorized to carry out the aforementioned review this body shall be an independent third party.[197]

By examining the CJEU's case-law within a time period of eight years (from the judgement in Digital Rights Ireland in 2014 since the judgement in Commissioner of An Garda Síochána in 2022), it is inferred that the Court has created layers concerning the retention of electronic communications data based on the objectives that the legal measures providing for the data retention pursue. On the upper layer national security stands which allows for a general and indiscriminate data retention provided that certain conditions are met. On the mid layer combating of serious crime and prevention of a serious threat to public security stands which permits the *"targeted and expedited data retention"* as well as the general and indiscriminate retention of specific categories of electronic communications data. On the lower layer there are other law enforcement purposes which allow for the targeted data retention only.

3. The proposal for an e-Privacy Regulation

3.1 The long route in the European Parliament

In 2015 the Commission adopted the Digital Single Market (DSM) strategy, the purpose of which is to *"increase trust in and the security of digital services"*.[198] For this purpose, GDPR has been adopted and in the meanwhile the Commission has also announced the reform of the legal framework concerning the processing of data in the electronic communications sector, namely of the e-Privacy Directive. In a study that the above legal body conducted in 2015, it was found that the e-Privacy Directive has not achieved its goals and that the scope of application of the Directive diverged among Member States due to the power of the national legislators to transpose the provisions of the Directive in their national legal systems.[199] The review of the Directive -the public consultation of which began in April 2016-[200] aims to remedy these failures and

[196] Ibid, para. 110.
[197] Ibid, para. 108.
[198] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Explanatory Memorandum, para. 1.1.
[199] "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation". *digital-strategy.ec.europa.eu*, European Commission, June 10 2015. https://digital-strategy.ec.europa.eu/en/library/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data
[200] "Public Consultation on the Evaluation and Review of the ePrivacy Directive". *digital-strategy.ec.europa.eu*, European Commission, April 12 2016. https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-evaluation-and-review-eprivacy-directive

particularly, to ensure a higher level of privacy protection for the users of the electronic communications services and an equal level of competition for all market players.[201]

The Commission has realized the need of the e-Privacy Directive to adapt to the technological developments in the electronic communications sector and specifically, to the new ways of communication that have emerged during the last decade and are extensively used. These new ways are internet-based services, such as Voice over IP, instant messaging and web-based e-mail services.[202] They are called Over-the-Top services. These services do not fall within the scope of the e-Privacy Directive, as already noted above.

The legal instrument that the Commission chose to incorporate the review of the e-Privacy Directive is that of a Regulation. As a Regulation is immediately applicable in the national legal systems without the need of being transposed in them, as is the case with a Directive, the aforementioned divergences in the national laws of Member States can be avoided and a more consistent level of protection can be achieved across the EU. Furthermore, the role of the e-Privacy Regulation, as that of the e-Privacy Directive, is to *"particularize and complement"*[203] the provisions of the GDPR. The choice of this legal instrument also serves the consistency between the two legal acts,[204] where the e-Privacy Regulation supplements the GDPR's provisions.

The Commission finally published the proposal for an e-Privacy Regulation in January 2017. The e-Privacy Regulation would allegedly apply along with GDPR in 2018. However, even though five years have passed since the initial publication, the Regulation has not been adopted yet. After the failure of the Austrian, Romanian, Finish and Croatian presidencies of the Council to reach an agreement for the beginning of negotiations, the Portuguese presidency managed to reach this desired agreement on a negotiating mandate in February 2021. While the trialogue between the Commission, the European Parliament and the Council was taking place, France, which was in the presidency, changed the negotiating mandate in March 2022.[205] Currently, the aforementioned bodies continue to negotiate regarding the adoption of

[201] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Explanatory Memorandum, para. 1.1.
[202] Ibid.
[203] Ibid, art. 1 (3).
[204] Ibid, Explanatory Memorandum, para. 2.4.
[205] "EU: e-Privacy: Council proposed amended mandate whilst in negotiations with Parliament." *Statewatch*, April 20, 2022, https://www.statewatch.org/news/2022/april/eu-e-privacy-council-proposed-amended-mandate-whilst-in-negotiations-with-parliament/.

the Regulation which is not expected to enter into force before 2023 and to apply before 2025.[206]

The proposed Regulation, like the e-Privacy Directive, serves a dual aim. The first one is to ensure the protection of the right to privacy and communications, as enshrined in art. 7 of the Charter, and the right to the protection of personal data, as enshrined in art. 8 of the Charter, in connection with the provision and use of electronic communications services.[207] The second one is to ensure the free flow of the electronic communications data and services across the EU.[208] For the first time, the European legislator refers explicitly to the protection of the right to communication, which forms an aspect of the right to privacy. Since the use of electronic communications has increased rapidly during the last years, the right to communication and more specifically the right to confidentiality of communications, as will be analyzed below, constitutes a fundamental pillar of contemporary societies.[209]

3.2 Scope of Application

3.2.1 The material scope of application

Article 2 of the proposal refers to the material scope of application. According to this article, the Regulation *"applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services"*.[210] For the definition of the electronic communications services the European legislator relies on the definitions provided in the European Electronic Communications Code (ECC, Directive 2018/1972),[211] a point on which it has been criticized by the European Data Protection Supervisor (EDPS) -and justifiably to the author's view- due to the fact that amendments of the ECC will lead to changes of the definitions of the Regulation and mainly due to the fact that the ECC serves economic purposes whereas the e-Privacy Regulation the protection of fundamental rights. Therefore, the former's definitions are not expected to be satisfactory enough

[206] Beranek Zanon, Nicole. "ePrivacy Regulation: EU Council agrees on the draft". *www.lexology.com*, Härting Rechtsanwälte, March 24,2022. https://www.lexology.com/library/detail.aspx?g=2c0eca0b-c828-4fd6-ac0f-21fdbeded2bb
[207] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Explanatory Memorandum, art. 1 (1).
[208] Ibid, art. 1 (2).
[209] Buttarelli, Giovanni. "The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union." European Data Protection Law Review (EDPL), vol. 3, no. 2, 2017, p. 156.
[210] Ibid, art. 2 (1).
[211] Ibid, art. 4 (1) b.

for the latter's purposes.[212] In other words, the ECC's definitions may lead to a decreased material scope of application of the e-Privacy Regulation.[213]

According to the ECC, an electronic communications service is *"a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services: (a) 'internet access service' […]; (b) interpersonal communications service; and (c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting"*.[214] In contrast with the Framework Directive, upon which the e-Privacy Directive relies for the definition of electronic communications services, the Electronic Communications Code does not depend on a technical criterion (i.e. the conveyance of signals) in order to classify a service as an electronic communications one but rather on the *"end-users perspective"*.[215] The conveyance of signals is not the decisive criterion for the categorization but rather what the end-users perceive as a communication.

The e-Privacy Regulation expands the scope of its predecessor and covers Over-the-Top Services, like Voice over IP (e.g. Skype, WhatsApp), messaging services and web-based e-mail services. Another novelty is that the Regulation applies also to machine-to-machine communications in the Internet of Things[216] (e.g. smart TVs, intelligent cars). The fact that an interpersonal communications service is ancillary to another one does not preclude the application of the Regulation (e.g. online games where the players can message each other).[217] The new Regulation covers the gap of the e-Privacy Directive, which has failed to keep up with the technological developments and remedies the inconsistencies in the accorded protection to the users between the traditional and the modern types of communication services which are nevertheless *"functionally equivalent"*.[218]

---

[212] Opinion 6/2017 "EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)." April 24 2017, p. 11.
[213] Naranjo, Diego. "E-Privacy Regulation: Good Intentions but a Lot of Work to Do." European Data Protection Law Review (EDPL), vol. 3, no. 2, 2017, p. 153.
[214] See DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 2 (4).
[215] Sein, Karin. "Interplay of Digital Content Directive, European Electronic Communications Code and Audiovisual Media Directive in Communications Sector." Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol. 12, no. 2, April 2021, p. 172.
[216] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), recital 12.
[217] Ibid, art. 4 (2) in conjunction with Opinion 6/2017 "EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)." April 24 2017, p. 9.
[218] Opinion 6/2017 "EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)." April 24 2017, p. 8.

It derives a contrario from the exception established in art. 2 (2) (c) that the Regulation is applicable only to electronic communications which are publicly available. The proposal provides some guidance regarding the nature of services in cases where it is ambiguous whether they are of public or of private nature. In recital 13 the European legislator clarifies that wireless networks that provide internet access to an indefinite number of people in public and "semi-private" places, such as *"hotspots situated at different places within a city, department stores, shopping malls and hospitals"*[219] fall within the scope of the Regulation. On the contrary, networks accessible to a limited number of end-users, such as corporate networks, do not fall within the scope.

The other three exceptions from the material scope of application, as laid down in art. 2 (2) of the proposed Regulation, are identical to those provided in art. 1 (3) of the e-Privacy Directive.

For the first time the European legislator provides for the definition of electronic communication data. They shall be defined, though, in an extensive and *"technology neutral way"*[220] in order to incorporate *"electronic communications content and electronic communications metadata"*.[221] Therefore, there are two categories of electronic communications data. Electronic communications content is defined as *"the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound"*[222] and electronic communications metadata as *"data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication"*.[223] The definition of metadata encompasses only the processing of data that takes place in the electronic communications network, which is defined in the ECC as *"transmission systems […] which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals".*[224]

[219] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), recital 13.
[220] Ibid, recital 14.
[221] Ibid, art. 4 (3) a.
[222] Ibid, art. 4 (3) b.
[223] Ibid, art. 4 (3) c.
[224] See DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 2 (1).

Therefore, this definition does not cover such data processed by equipment which is not part of the electronic communications network, as could be the case for example with "associated services".[225] Finally, it is notable that the legislator has abandoned the distinction between traffic and location data which now fall under the definition of metadata and consequently, the different treatment regarding their processing, which was unjustifiable under the previous legal regime as they are processed in the context of functionally similar services.[226]

3.2.2 The personal scope of application

The e-Privacy Regulation, exactly as its predecessor, accords protection to both natural and legal persons.[227] The proposal recognizes that *"electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value"*.[228] It seems that the European legislator specified the ambiguous concept of *"legitimate interests"* of the e-Privacy Directive to cover mainly economic interests under the e-Privacy Regulation.

Furthermore, the distinction between users and subscribers is abandoned and these terms are substituted by the term "end-users". The definition of the end-user is provided in the ECC, where in art. 2 (14) it is stated that *"end-user means a user not providing public electronic communications networks or publicly available electronic communications services"*. According to this legal act, a user is *"a natural or legal person using or requesting a publicly available electronic communications service"*.[229] The term end-user definitely encompasses the term "user" of the previous legal regime but it is not clear whether it encompasses the concept of the subscriber as well. The provisions of the Proposal, though, show that the subscribers are also incorporated in the notion of end-users, since it is stated in art. 3 (1) that the Regulation applies *"to the provision of electronic communications services to end-users irrespective of whether a payment of the end-user is required"*. There are also explicit references to the subscription to electronic communications services (see indicatively recitals 14 and 37). It seems, therefore, that it would be preferrable for the purposes of the e-Privacy

[225] Opinion 6/2017 "EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)." April 24 2017, p. 12.
[226] Dumortier, Jos. "Evaluation and Review of the ePrivacy Directive." European Data Protection Law Review (EDPL), vol. 2, no. 2, 2016, p. 248.
[227] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 1 (1).
[228] Ibid, recital 3.
[229] See DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 2 (13).

Regulation not to rely on the definitions of the ECC but to incorporate the definition of "end-users" in the legal act for the reasons analyzed above, too.

The level of the accorded protection to natural and legal persons is equivalent. Particularly, the rules laid down in GDPR, regarding for example the definition of consent, their rights concerning the supervisory authorities,[230] apply to legal persons as well.

3.2.3 The territorial scope of application

The territorial scope of application of the e-Privacy Regulation is identical to that of the e-Privacy Directive. Specifically, the proposed e-Privacy Regulation applies to *"the provision of electronic communications services to end-users in the Union"*.[231] It is irrelevant whether the processing of electronic communications data takes place in the Union or whether the electronic communications service provider is established within the Union. Even though the wording is not identical with that of art. 3 of the GDPR, the territorial scope of the two legal acts is actually the same.

Regarding the case, where the provider is established outside the EU, a novelty is introduced in the Regulation. This is the obligation of the provider to maintain a representative in one of the Member States where the end users are located. The appointment of the representative shall be done in writing.

The designation of the representative serves a dual aim, the protection of the end-users and the facilitation of the work of supervisory authorities. Firstly, the end-users can address to the representative, who is located in the Union, more easily than to the provider who is established outside the EU in order to resolve any questions of them regarding the processing of their electronic communications data. Accordingly, the supervisory authorities can immediately ask the representative to provide them any necessary information in order to ensure compliance with the provisions of the Regulation rather than addressing to the provider, which could be more time consuming. [232]

[230] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), recital 3.
[231] Ibid, art. 3 (1).
[232] Ibid, art. 3 (4).

In any case, the appointment of a representative does not affect the right of end-users to bring a legal action directly against the providers of electronic communications services who are established outside the EU.[233]

3.3 Processing of electronic communications data

3.3.1 The principle of confidentiality

The e-Privacy Regulation, as its predecessor, follows the principle of confidentiality. Electronic communications data shall be confidential. This principle is enshrined in art. 5 where it is stated that *"any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation"*.[234] This principle is not rigid, since there are exceptions to this rule laid down by the proposed Regulation and which will be analyzed below. The phrase *"any interference"* encompasses all possible means of achieving the interception of electronic communications data, i.e. through human intervention or through automatic processing by machines.[235] The rule of confidentiality applies from the time that a communication starts until its receipt from the addressee. The EDPS featured a gap concerning the scope of the principle of confidentiality. That is that it does not *"cover the communications data stored in the cloud"*,[236] a technology used extensively nowadays. Furthermore, the proposal, as its predecessor, does not provide an exhaustive list of the ways of interference but rather leaves room for any type of interception, as technology develops rapidly and new *"technical ways to engage in interception"*[237] emerge.

For the first time the European legislator incorporates in a legal act the CJEU's findings regarding the equation of the importance of metadata with the content of communications. Specifically, already from the beginning of the Regulation (in recital 2) the legislator declares that both the content of communications and metadata can reveal "very sensitive and personal information",[238] such as aspects of their social lives,

[233] Ibid, art. 3 (5).
[234] Ibid, art. 5.
[235] Ibid, recital 15.
[236] Opinion 6/2017 "EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)." April 24 2017, p. 13.
[237] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), recital 15.
[238] Ibid, recital 2.

activities, habits and interests. It is also clarified that the principle of confidentiality is applicable to *"current and future means of communication"*[239]. Messaging through social media, instant messaging apps and internet phone calls explicitly fall within the scope of the Regulation and their providers shall comply with the rules of it.

Article 5 of the proposed Regulation establishes an *"erga omnes"* applicable rule. Since no distinction is made, the rule of confidentiality is binding not only for the providers of electronic communications services, but also for other bodies.

3.3.2 The exceptions to principle of confidentiality

Regardless of the category of electronic communications data, i.e. content of communications or metadata, their processing by the electronic communications networks and services providers is allowed when:

a) It is necessary for the transmission of a communication.[240] This exception reflects the technical storage exception, established by the e-Privacy Directive. In the case of the e-Privacy Regulation, the legislator does not use the term "technical storage" but refers to *"any automatic, transient storage",*[241]which is actually the definition of "technical storage" used in the e-Privacy Directive. Such storage of electronic communications data shall not be prohibited as far as it is necessary for the transmission of a communication. This storage, though, is subject to specific limitations. Firstly, the electronic communications data shall be processed only for the purpose of transmitting the communication and secondly, they shall be processed only for the time necessary for the attainment of the abovementioned purpose.[242] With these limitations the principles of purpose and storage limitation, as enshrined in art. 5 of the GDPR, are encompassed.
b) It is necessary for the maintenance or recovery of the security of electronic communications networks and services or for the identification of technical faults or errors in the transmission of communications.[243] Recital 16 provides some guidance on this exception by clarifying that checks of security threats and processing of metadata for the purpose of maintaining

[239] Ibid, recital 1.
[240] Ibid, art. 6 (1) a.
[241] Ibid, recital 16.
[242] Ibid, art. 6 (1) a in conjunction with recital 16.
[243] Ibid, art. 6 (1) b.

the necessary level of quality of electronic communications services fall under this exception. The processing that takes place under this exception must be limited to the time necessary for the attainment of these purposes.

c) The exception of art. 11 applies, which will be analyzed below.

Apart from these general exceptions that apply to both the content of communications and metadata, the European legislator has provided for further exceptions for each specific category of electronic communications data. Regarding the processing of metadata, the Regulation extends the range of the exceptions that were provided under the e-Privacy Directive.[244]

The processing of metadata is also allowed under the following conditions:

a) It is necessary in order to meet obligatory quality standards of the electronic communications services pursuant to the ECC or Regulation 2015/2120. This exception is subject to limitations, namely that such processing takes place for the attainment of this specific purpose and for the time necessary for this achievement. This exception is a novelty of the Regulation and is in conformity with the legal developments, i.e. the implementation of the ECC and of the Regulation 2015/2120, which did not exist when the e-Privacy Directive was enforced.

b) It is necessary for *"billing purposes and interconnection payment"* and for finding or preventing *"fraudulent or abusive use or subscription to electronic communications services"*.[245] This exception was included in the e-Privacy Directive as well.

c) Consent has been provided by the end-users concerned regarding the processing of their metadata in connection with some specific purposes, such as the provision of a service[246] or for commercial usages.[247] However, it is a prerequisite for the application of this exception that such data cannot be processed for these purposes while being made anonymous. Consent has the same meaning as that provided in GDPR, irrespectively of whether the end-user is a natural or legal person. It must be specific, given freely and in an affirmative manner.[248] End-users shall be also free to withdraw their consent at any time and be reminded of that option by the electronic

[244] Ibid, recital 17.
[245] Ibid, art. 6 (2) b.
[246] Ibid, art. 6 (2) c.
[247] Ibis, recital 17.
[248] See REGULATION (EU) 2016/679, General Data Protection Regulation, art. 4 (11).

communications service providers every six months.[249] This obligation of reminder is a novelty, as such provision does not exist in GDPR nor in the e-Privacy Directive. This obligation is imposed on the electronic communications service providers due to the sensitivity of the data processed. Consent is the only legal basis, under which the electronic communications service providers have the right to process metadata. They cannot rely on any other basis provided in art. 6 of GDPR. In fact, this exception reflects the one of the provision of value added services laid down in the e-Privacy Directive, a term that is not used in the proposal. In the clarification of this exception in the recitals of the proposal, the legislator provides a useful guidance on location data. As mentioned above, the distinction between traffic and location data is abandoned in the e-Privacy Regulation and they are covered by the term "metadata". However, the European legislator stresses that the term "metadata" encompasses only *"data on the location of the device generated for the purposes of granting and maintaining access and connection to the service [and that] location data that is generated other than in the context of providing electronic communications services should not be considered as metadata"*.[250] This distinction, though, is rather ambiguous because it is unclear whether *"location data collected through apps that use the data from the GPS-functionality in smart devices, and/or generate location data based on nearby WiFi-routers, and/or location data collected with on-board navigation assistants and/or other ways"*[251] are considered metadata. The processing of location data that are not metadata shall be carried out in accordance with GDPR. For the purposes of this exception, the commercial usage of metadata may include *"the provision of heatmaps, [the] display of traffic movements"*[252] and the provision of services may include *"protection against fraudulent activities, broadband internet access and voice communications services"*.[253] In accordance with GDPR, the electronic communications service providers may be required to conduct a data protection impact assessment or take the advice of the supervisory

[249] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 9 (3).
[250] Ibid, recital 17.
[251] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), April 4,2017, p. 29-30.
[252] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, recital 17.
[253] Ibid, recital 18.

authorities, when the processing entails high risks to the rights and freedoms of the end-users.

As far as the content of communications is concerned, the European legislator declares the finding of the CJEU in the landmark decision of Digital Rights Ireland, namely that the content of communications constitutes the essence of the fundamental right to privacy, as enshrined in art. 7 of the Charter.[254] Therefore, the processing of the content shall be subject to strict and precise conditions. A line is drawn to the scope of application of the e-Privacy Regulation. It is clarified that after the receipt of the content of the communication by the addressee, the e-Privacy Regulation does not apply but any act of processing carried out by the end-users or by third parties, such as recording or storage, falls under the scope of GDPR. The additional exceptions, under which processing of content is permitted, are consent based. Particularly, it is allowed when:

a) The processing takes place in the context of the provision of a specific service, after the end-user or end-users concerned have provided their consent. A further prerequisite is that the processing of the content is necessary for the provision of the service, in the sense that otherwise it is impossible to be performed.[255] This exception refers to the case, where the provision of the service is requested by the end-user.[256] Consent has the meaning that was analyzed above.
b) All end-users concerned have provided their consent to the processing of the content of communications *"for one or more specified purposes"*.[257] These purposes do not refer to the provision of a service, a case which is encompassed in the previous exception. An example of this case is the *"processing of electronic communications data in transit"*,[258] such as the scanning of emails for the detection and deletion of *"certain pre-defined material"*.[259] The processing of the content in this case is allowed only when it cannot take place with the data being anonymized. Finally, for this specific case of processing the legislator imposes a further burden on the electronic

[254] Ibid, recital 19.
[255] Ibid, art. 6 (3) a.
[256] This interpretation of the exception derives from recital 19, where a distinction is made regarding the need of consultation of the supervisory authorities.
[257] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 6 (3) b.
[258] Ibid, recital 19.
[259] Ibid.

> communications service providers, which is the consultation of the supervisory authority and the conduct of data protection impact assessment. In contrast with the last exception of processing metadata, as mentioned above, in this case there is a presumption that the processing of the content of communications entails a high risk to the fundamental rights and freedoms of the end-users and therefore, the advice of the supervisory authorities and the conduct of a data protection impact assessment is necessary prior to the processing.[260]

A fist issue that arises from the aforementioned additional exceptions and specifically from exception (c) of the processing of metadata and the exceptions of the processing of electronic communications content is the meaning of the term *"end-users concerned"*, which the legislator uses and whose consent is necessary for the processing of their electronic communications data. As already mentioned above, the proposal does not contain a definition of the term "end-user" but rather relies on the definition provided in the ECC. By using the term *"end-users concerned"* it is unclear whose consent is really needed. It seems that by using this terminology the European legislator aims to the protection of the users, who actually make use of the service provided and whose consent is needed, rather than that of the subscribers.[261] Moreover, in some cases the term *"end-users concerned"* is used [e.g. art. 6 (2)(c) and art. 6 (3)(a)] and in others *"all end-users concerned"* [e.g. art. 6 (3)(b)]. This inconsistency in the text of the proposal is unjustifiable. In any case, when consent is required for the processing of the electronic communication data, the consent of all the involved persons in a communication (i.e. both of the sender and the receiver) shall be provided[262] in order for the processing to be lawful. Hence, the proposal shall provide some clarifications regarding the persons, whose consent is required and shall not leave the interpretation of this essential matter at the discretion of the Member States, which are entitled to clarify the provisions of the proposal.[263]

A second issue that arises is the fact that the level of protection of metadata and of the content of communications differs. This choice of the legislator contradicts the finding that metadata may reveal "very sensitive and personal information", as the content of communications may do. It is unjustifiable why in the case of the content

[260] Ibid.
[261] Opinion 6/2017 "EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)." April 24 2017, p. 14.
[262] Ibid, p. 14-15.
[263] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), recital 7.

there is a presumption that processing entails high risks to fundamental rights and therefore, a data protection impact assessment and prior consultation of the authorities will be required in any case, whereas in the case of metadata processing might involve such risks. The same conditions for consent shall apply to the two categories of electronic communications data and the same level of protection shall be granted.[264]

3.3.3 The obligation of erasure or anonymization of electronic communications data

Article 7 of the e-Privacy Regulation incorporates the obligation of the electronic communications service providers to erase or make anonymous the electronic communications data after the transmission of the communication, an obligation imposed on them by the e-Privacy Directive too. Specifically, after the receipt of the content of the communication by the addressee, in the case of the electronic communications content and after the transmission of the communication, in the case of metadata, the electronic communications service providers shall erase the electronic communications data or make them anonymous. The electronic communications data shall not be retained, except when one of the exceptions of art. 6 (1) (b), 6(2), 6(3) or art. 11 applies. As soon as the necessary processing for the transmission of the communication takes place in accordance with art. 6 (1) (a), the providers are subject to this obligation. In the case, though, where metadata are processed in the context of art. 6 (2)(b), i.e. for billing purposes, they shall be erased or made anonymous after *"the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law"*.[265]

It must be noted that electronic communications metadata can be further processed after having been made anonymous.[266]

3.4 The exception of art. 11 of the e-Privacy Regulation

The proposal does not lay down any specific rules on data retention but, like its predecessor, contents itself in providing the general exception and leaving the particularization of it at the discretion of the Member States or of the EU -an option that

[264] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), April 4,2017, p. 13.
[265] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, art. 7 (3).
[266] European Data Protection Board (EDPB). "Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications." May 25,2018, p. 2.

was not provided in art. 15 of the e-Privacy Directive and is in accordance with art. 23 of GDPR. Particularly, the EU or Member States may adopt legislative measures which restrict the scope of the rights and obligations established by the articles regarding the processing of electronic communications content and metadata. Such restrictions must comply with the principles of Union law and with the CJEU's case law[267] and specifically, they must respect the essence of the fundamental rights to privacy and to protection of personal data, as enshrined in art. 7 and 8 of the Charter respectively, and must be necessary, appropriate and stricto sensu proportionate to the aim they pursue, in other words they must be compatible with the principle of proportionality.

The aims that such measures may pursue are listed exhaustively in art. 11 with reference to art. 23 (1) of GDPR. Specifically, the aims are the protection of *"national security, defence, public security, the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security"*[268] or carrying out *"a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests"*.[269]

The e-Privacy Regulation imposes obligations on the electronic communications service providers, who shall maintain *"internal procedures"*[270] in order to reply to requests for access to electronic communications data, in accordance with the legislative measures adopted. Moreover, information regarding the *"procedures, the number of requests received, the legal justification invoked and their response"*[271] shall be provided to the supervisory authorities, upon request. The representative of the providers may be the person who provides such information to the authorities.[272]

The fact that the material scope of application of the Proposal is broader than that of the e-Privacy Directive does not mean that Member States have the discretion

[267] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Explanatory Memorandum, para. 1.3.
[268] See REGULATION (EU) 2016/679, General Data Protection Regulation, art. 23(1)(a) to (e).
[269] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 11 (1).
[270] Ibid, art. 11 (2).
[271] Ibid.
[272] Ibid, recital 26.

to extend *"automatically"*[273] any existing or future laws, adopted in accordance with art. 15 of the e-Privacy Directive, to cover any electronic communications services, i.e. those that do not fall under the scope of the e-Privacy Directive. Member States will have to establish that the proportionality test is passed, in order to extend the scope of such legislative measures.

Even though the wording of art. 11 is similar to that of art. 15 of the e-Privacy Directive, the Proposal expands the objectives that such legislative measures may pursue. For instance, the execution of criminal penalties was not incorporated in the previous regime. Furthermore, the phrase *"other important objectives of general public interest of the Union or of a Member State"* established in art. 23(1)(e) of GDPR, is rather generic and may lead to the exploitation of the rule of art. 11 by the Member States, which may interpret *"important objective of general interest"*, as they wish. The conditions of art. 23(1) of GDPR do not refer to special categories of data and therefore, it would be preferrable that the e-Privacy Regulation listed the aims in art. 11 explicitly rather than making reference to the GDPR.[274]

3.5 Other obligations of the electronic communications service providers – the relationship with DMA, DSA and DGA

The obligations that were imposed on the electronic communications service providers regarding the security of processing of electronic communications data and the data breach notification are not incorporated in the e-Privacy Regulation, since the obligation to take *"appropriate technical and organizational measures"*[275] and to notify the authorities and the persons concerned, if needed, in a case of a data breach[276] are incorporated in the GDPR. The obligations for security are also part of the ECC. As already noted, GDPR applies when the e-Privacy Regulation does not contain any specific provisions. Concerning the security of processing, the EDPS suggested that the GDPR's provisions are not adequate, since they apply to the processing of personal data and that all communications data shall be protected.[277] Indeed, the

[273] Buttarelli, Giovanni. "The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union." European Data Protection Law Review (EDPL), vol. 3, no. 2, 2017, p. 158.
[274] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), April 4,2017, p. 23-24.
[275] See REGULATION (EU) 2016/679, General Data Protection Regulation, art. 32.
[276] Ibid, art. 33 and 34.
[277] Opinion 6/2017 "EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)." April 24 2017, p. 34.

Proposal states that *"electronic communications data may include personal data"*.[278] In fact, electronic communications data generally qualify as personal data,[279] as defined in GDPR, and the relevant provisions of GDPR will apply. In order to ensure that the level of protection is not undermined, it would be preferrable to incorporate in the Proposal a specific provision regarding the security of processing, as in the e-Privacy Directive.

Under the e-Privacy Regulation, the electronic communications service providers shall inform the end-users about risks that may jeopardize the security of networks and electronic communications services. If the measures the providers have to adopt do not cover such risks, they shall also inform the end-users about any appropriate measures the latter can take *"to protect the security of their communications"*[280] and about any possible costs. The measures the end-users can take are the use of *"specific types of software or encryption technologies"*.[281] As already mentioned, the electronic communications service providers are obliged to take at their own costs appropriate technical and organizational measures to mitigate *"any new, unforeseen security risks"*[282] and maintain a level of security. This obligation is not offset against the obligation to inform end-users. The information shall be provided free of charge.

There is an ambiguity regarding the persons who shall be informed. It shall be clarified that the natural persons using the services are the ones who shall be informed.[283]

An important legal development of 2022 was the adoption of the Digital Markets Act (DMA, Regulation 2022/1925), of the Digital Services Act (DSA, Regulation 2022/2065) and of the Data Governance Act (DGA, Regulation 2022/868), which will extend the obligations of the electronic communications service providers as soon as they will become applicable.

The DMA, whose aim is "*the proper functioning of the internal market*" through the approximation of rules in order to maintain *"for all businesses, contestable and fair*

[278] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), recital 4.
[279] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), April 4,2017, p. 27.
[280] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 17 in conjunction with recital 37.
[281] Ibid, recital 37.
[282] Ibid.
[283] Opinion 6/2017 "EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)." April 24 2017, p. 33.

markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users",[284] does not apply to markets relating to electronic communications networks and electronic communications services, apart from those *"related to number-independent interpersonal communications services"*.[285] Thus, in principle, the scope of application of the e-Privacy Regulation and of the DMA do not coincide, except for the aforementioned category of electronic communications services, in which Facebook Messenger, Zoom and WhatsApp belong. As soon as such a service is provided or offered by an electronic communications service provider who qualifies as a *"gatekeeper"*, as defined in art. 2 (1) and 3 of DMA, the provider will also be subject to the obligations established in DMA concerning the processing of data and specifically, of electronic communications data. Particularly, the processing of "*personal data of end users using services of third parties that make use of core platform services of the gatekeeper"* for the provision of online advertising services,[286] the amalgamation of personal data generated in the context of the relevant service with data *"from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services",*[287] the *"cross-use [of] personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa"*[288] and the "*signing in [of] end users to other services of the gatekeeper in order to combine personal data"*[289] are prohibited, unless the end user has provided his/her consent for such a processing. Consent has the same meaning as that provided in GDPR. However, apart from consent the gatekeeper may also rely on the legal bases provided in art. 6 (1), points (c), (d) and (e) of GDPR, in order for the processing to be lawful.[290] Furthermore, data, which is not publicly available but *"is generated or provided by those business users in the context of their use of the relevant core platform services or of the services provided together with, or in support of, the relevant core platform services, including data generated or provided by the customers of business users"* shall not be used, in order to compete with business users.[291]

A specific obligation imposed on gatekeepers who provide number-independent interpersonal communications services in the context of their obligation on interoperability is that processing in the form of collection and exchange of personal

[284] See REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 1 (1)
[285] Ibid, art. 1 (2).
[286] Ibid, art. 5 (2)(a).
[287] Ibid, art. 5 (2)(b).
[288] Ibid, art. 5 (2)(c).
[289] Ibid, art. 5 (2)(d).
[290] Ibid, art. 5 (2).
[291] Ibid, art. 6 (2).

data of the end-users with the provider of such services who asks for interoperability shall be limited to what is strictly necessary for the purpose of *"effective interoperability"* and be in accordance with GDPR and the e-Privacy Directive, which is still applicable.[292] DMA explicitly states that the implementation of the aforementioned obligations of the gatekeepers shall comply with GDPR and the e-Privacy Directive.[293]

With the enforcement of DMA on November 1, 2022 and with its application from June 25, 2023 specific acts of processing are prohibited. The acts incorporated in art. 5 of the DMA shall be allowed if the end-users have provided their consent or another legal basis of art. 6, as analyzed above, applies. These acts listed in DMA do not coincide with the exceptions established in art. 6 of the e-Privacy Regulation, under which the processing of electronic communications data is permitted and hence, the cases of permitted processing are extended. It is problematic that under DMA processing can be carried out not only after the end-users have provided their consent but also if the cases of art. 6 (1), points (c), (d) and (e) of GDPR apply, whereas under the e-Privacy Regulation (and the e-Privacy Directive) processing is permitted only if the end-users have provided their consent. However, due to the explicit reference that compliance with the e-Privacy Directive (and with the e-Privacy Regulation from the time that it will be enforced) must be ensured, to the author's view, consent shall be the only legal basis under which processing of electronic communications data under DMA shall be permitted.

The DSA applies to intermediary services and its aim is the *"proper functioning of the internal market"* by the approximation of rules "*for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected"*.[294] The application of DSA does not affect the application of GDPR and of the e-Privacy Directive, which cover other aspects of intermediary services and are complementary to the provisions of DSA,[295] as long as their scope of application coincides. Intermediary services are information society services which, in principle, do not fall within the definition of electronic communication services, as provided in the ECC.[296] However, there are certain information society services which are electronic communications services as well[297] and therefore, will fall within the scope of the e-

[292] Ibid, art. 7 (8).
[293] Ibid, art. 8 (1).
[294] See REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 1 (1).
[295] Ibid, art. 2 (4)(g).
[296] See DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, recital 7.
[297] Ibid, recital 10.

Privacy Regulation. As long as electronic communications services constitute information society services, DSA will apply along with the e-Privacy Regulation.

The DGA establishes *"the conditions for the re-use within the Union of certain categories of data held by public sector bodies, a notification and supervisory framework for the provision of data intermediation services, a framework for voluntary registration of entities which collect and process data made available for altruistic purposes and a framework for the establishment of a European Data Innovation Board".*[298] The DGA's aim is to facilitate the flow of data. The application of DGA does not affect the one of GDPR and e-Privacy Directive nor provides a legal basis for the lawful processing of data. In the case of a conflict with GDPR or the e-Privacy Directive, the latter will apply.[299] The material scope of application of DGA covers data *"held by public sector bodies which are protected on grounds of commercial confidentiality, including business, professional and company secrets, statistical confidentiality, the protection of intellectual property rights of third parties or the protection of personal data, insofar as such data fall outside the scope of Directive (EU) 2019/1024".*[300] For the purposes of this Regulation, electronic communications service providers fall within the definition of data holders, since without being the data subject they have the right to *"grant access to or to share certain personal data or non-personal data"*,[301] provided that the conditions for such processing are met, according to art. 6 and 7 of the e-Privacy Regulation. Electronic communications service providers may transmit those data to data intermediation service providers.[302]

3.6 The relationship with GDPR

As already mentioned, the e-Privacy Regulation is designed to *"particularize and complement"*[303] the General Data Protection Regulation. When no specific rules are provided in the e-Privacy Regulation, the *"lex generalis"* GDPR will apply. The European legislator declares that the e-Privacy Regulation *"does not lower the level of protection enjoyed by natural persons"*[304] under GDPR.

[298] See REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, art. 1 (1).
[299] Ibid, art. 1 (3).
[300] Ibid, art. 3 (1).
[301] Ibid, art. 2 (8).
[302] Ibid, art. 12.
[303] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 1 (3).
[304] Ibid, recital 5.

Despite this explicit declaration, though, there is a point in the e-Privacy Regulation, where the level of protection is lower than that of GDPR. In the exceptions to the principle of confidentiality and particularly in that of art. 6 (1) (b) regarding processing for security purposes, the processing of electronic communications data is allowed if it is "*necessary"* for this purpose. On the contrary, in recital 49 of GDPR it is required that processing is *"strictly necessary"* for such purposes. Whether this inconsistency is unintentional or not, the word "strictly" shall be added before "necessary" in all the exceptions provided in art. 6 of the Proposal, in order to ensure that these exceptions are interpreted narrowly.[305]

Similarly to the e-Privacy Directive, when consent of the end-users is required for the lawfulness of processing, it cannot be replaced by any other legal basis provided in art. 6 of GDPR. However, the processing of electronic communications data under the e-Privacy Regulation shall comply with the principles of processing, as established in art. 5 of GDPR.

3.7 Remedies, liability and penalties

The supervisory authorities responsible for the implementation of GDPR are also responsible for that of the e-Privacy Regulation,[306] which can lead to the consistent application of the two legal acts,[307] which is necessary since the one complements the other.

In accordance with GDPR, a new complex of provisions concerning "Remedies, Liability and Penalties" is introduced in the Proposal. The end-users have the rights enshrined in art. 77 to 79 of GDPR and specifically, the right to file a complaint to the supervisory authorities, the right to *"an effective judicial remedy against a legally binding decision of a supervisory authority"* and the right to *"an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her [electronic communications] data in non-compliance with the [e-Privacy] Regulation"*. Article 21 of the e-Privacy Regulation that grants the end-users the afore mentioned rights does not refer to the right to "*mandate a not-for-profit body, organization or association*" to

[305] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), April 4,2017, p. 20.
[306] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 18.
[307] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), April 4,2017, p. 7.

exercise the afore mentioned rights and the right to compensation, which will be analyzed below, on behalf of the data subjects and to the option of the Member States to allow such organizations to act independently of the data subjects' mandate, a right which is enshrined in art. 80 of GDPR. This right is partially reflected in art. 21 (2) of the Proposal. This provision grants the right to third parties, either natural or legal persons, who are affected by violations of the Regulation and have *"a legitimate interest in the cessation or prohibition of such infringements",*[308] to bring legal actions for such violations. However, it would be preferrable that the collective redress mechanism of art. 80 of GDPR is explicitly provided in the e-Privacy Regulation.[309]

The end-users are also entitled to compensation for the material or immaterial damage they suffered because of the violation of the Regulation.[310] The burden of proof is on the infringer, who has to prove the lack of responsibility for the event that caused the damage, pursuant to art. 82 of GDPR.

Finally, administrative fines shall be imposed in cases of violation of art. 5 to 7 of the e-Privacy Regulation, which can be up to 20,000,000 Euros or *"up to 4% of the total worldwide annual turnover of the preceding financial year"*,[311] if an undertaking is involved. Between these levels of fines the greater prevails. By establishing a certain level of fines, harmonization and a standard level of protection is achieved across the EU.[312] However, regarding the infringement of the obligation to inform end-users pursuant to art. 17 of the Regulation, the determination of fines is left at the discretion of the Member States.[313]

Conclusion

After analyzing the twenty-years journey from the adoption of the e-Privacy Directive in 2002 to present, with the enforcement of the e-Privacy Regulation being

[308] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 21 (2).
[309] Opinion 6/2017 "EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)." April 24 2017, p. 35.
[310] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 22.
[311] Ibid, art. 23 (3).
[312] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), April 4,2017, p. 7.
[313] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 23 (4).

"around the corner", the time has come to answer the question whether privacy has been sacrificed in the altar of technology.

The CJEU has laid good foundations by prohibiting bulk data retention to become the rule in a world where electronic communications data are generated and processed constantly. It has weighed the fundamental rights carefully and has created layers for the protection of privacy based on the objectives pursued.

The e-Privacy Regulation definitely makes some steps forward by extending the scope of application, in relation to the e-Privacy Directive, to cover services which have emerged during the last decade, such as Over-the-Top services and for which there was an unjustifiable inconsistency, as they fell under the scope of GDPR, even though users perceived them as electronic communications services. The e-Privacy Regulation and GDPR, where the former complements the latter, are designed to form the two pillars of the protection of the fundamental rights to privacy and personal data, as enshrined in art. 7 and 8 of the Charter respectively.

The steps taken by the European legislator in the proposal for a new e-Privacy Regulation are at the right side by establishing rules which prevent the profiling of users.[314] However, since the final text is not yet adopted, it is necessary that the ambiguities, which were mentioned above, are clarified, in order to leave no room for interpretations that could jeopardize the objectives pursued by the Regulation.

The final formulation of the text of the Regulation remains to be seen after the completion of the trilateral negotiations. During this trialogue it is essential that the focus remains on the protection of privacy and that no concessions will be made that will lead to more flexible rules concerning the processing of electronic communications data. After the enforcement of the e-Privacy Regulation, hopefully we will be able to say that it was slow in coming but well worth waiting for.

Bibliography

1. "Data protection in the electronic communications sector", EUR-lex. Available at: https://eur-lex.europa.eu/EN/legal-content/summary/data-protection-in-the-electronic-communications-sector.html
2. "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation". *digital-strategy.ec.europa.eu*,

[314] Buruiana, Andreea. "The Legal Consequences of the Facebook-Cambridge Analytica Scandal on the EU Information Society: the proposal of E-Privacy Regulation." Law Annals from Titu Maiorescu University, 2021, p. 57.

European Commission, June 10 2015. https://digital-strategy.ec.europa.eu/en/library/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data

3. "Public Consultation on the Evaluation and Review of the ePrivacy Directive". *digital-strategy.ec.europa.eu*, European Commission, April 12 2016. https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-evaluation-and-review-eprivacy-directive
4. ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), April 4,2017.
5. Benedikt, Kristin. "New Act on Privacy and Electronic Communications." European Data Protection Law Review (EDPL), vol. 7, no. 2, 2021, pp. 254-259. HeinOnline.
6. Beranek Zanon, Nicole. "ePrivacy Regulation: EU Council agrees on the draft". *www.lexology.com*, Härting Rechtsanwälte, March 24,2022. https://www.lexology.com/library/detail.aspx?g=2c0eca0b-c828-4fd6-ac0f-21fdbeded2bb
7. Boban, Marija. "E-privacy Regulation- New European Framework for Regulation on Privacy and Electronic Communications Designed to Protect User Privacy in the Digital Age." Economic and Social Development, 2019, pp. 176-187.
8. Brkan, Maja. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning." The Essence of Fundamental Rights in EU Law, 17-18 May 2018, Leuven, pp. 1-21. Available at SSRN: https://ssrn.com/abstract=3325267
9. Buruiana, Andreea. "The Legal Consequences of the Facebook-Cambridge Analytica Scandal on the EU Information Society: the proposal of E-Privacy Regulation." Law Annals from Titu Maiorescu University, 2021, pp. 47-58. HeinOnline.
10. Buttarelli, Giovanni. "The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union." European Data Protection Law Review (EDPL), vol. 3, no. 2, 2017, pp. 155-159. HeinOnline.
11. Calomme, Caroline. "Strict Safeguards to Restrict General Data Retention Obligations Imposed by the Member States." European Data Protection Law Review (EDPL), vol. 2, no. 4, 2016, pp. 590-595. HeinOnline.
12. Carolan, Eoin, and M. Rossario Castillo-Mayen. "Why More Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws." Virginia Journal of Law & Technology, vol. 19, no. 2, Winter 2015, pp. 324-388. HeinOnline.

13. Celeste, Edoardo. "The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios." European Constitutional Law Review, vol. 15, no. 1, March 2019, pp. 134-157. HeinOnline.
14. Cole Mark D., and Annelies Vandendriessche. "From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabo/Vissy in Strasbourg." European Data Protection Law Review (EDPL), vol. 2, no. 1, 2016, pp. 121-129. HeinOnline.
15. Drewry, Lawrence. "Crimes without Culprits: Why the European Union Needs Data Retention, and How It Can Be Balanced with the Right to Privacy." Wisconsin International Law Journal, vol. 33, no. 4, 2015, pp. 728-754. HeinOnline.
16. Dumortier, Jos. “Evaluation and Review of the ePrivacy Directive.” European Data Protection Law Review (EDPL), vol. 2, no. 2, 2016, pp. 247-252. HeinOnline.
17. EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.
18. Etteldorf, Christina. “Data Protection Authorities Try to Fill the Gap between GDPR and e-Privacy Rules.” European Data Protection Law Review (EDPL), vol 4, no. 2, 2018, pp. 235-238. HeinOnline.
19. Etteldorf, Christina. “EDPB on the Interplay between the ePrivacy Directive and the GDPR.” European Data Protection Law Review (EDPL), vol. 5, no. 2, pp. 224-231. HeinOnline.
20. European Data Protection Board (EDPB). “Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications.” May 25,2018.
21. European Digital Rights (EDRi). “Quick Guide on the Proposal of an e-Privacy Regulation.” March, 2017, pp. 1-5. Available at: https://edri.org/files/epd-revision/ePR_EDRi_quickguide_20170309.pdf
22. Fabbrini, Federico. “Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States.” Harvard Human Rights Journal, 28, 2015, pp. 65-96. HeinOnline.
23. Galli, Francesca. "Digital Rights Ireland as an Opportunity to Foster a Desirable Approximation of Data Retention Provisions." Maastricht Journal of European and Comparative Law, vol. 23, no. 3, 2016, pp. 460-477. HeinOnline.
24. Gniewek, Alicia. “Google Privacy Policy- In Breach of EU Law.” Massaryk University Journal of Law and Technology, vol. 7, no. 2, Fall 2013, pp. 319-346. HeinOnline.

25. Guild, Elspeth, and Carrera, Sergio. “The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive”. CEPS Liberty and Security in Europe Papers No. 65, May 2014, pp. 1-15. Available at SSRN: https://ssrn.com/abstract=2445901
26. Gumzej, Nina. “Applicability of ePrivacy Directive to National Data Retention Measures following Invalidation of the Data Retention Directive.” Juridical Tribune, vol. 11, no. 3, December 2021, pp. 430-451. HeinOnline.
27. JP Lopez, Luna. “The data privacy regime for legal persons in the electronic communications sector according to Directive 2002/58/EC.” UiO Faculty of Law, University of Oslo, December 1, 2014, pp. 1-45. Available at: https://www.duo.uio.no/bitstream/handle/10852/43031/8024-ICTLTHESIS.pdf?sequence=1
28. Lloyd, Ian. “Information Technology Law”. 9th Edition. Oxford University Press.
29. Louveaux, Sophie, Perez, Asinari, et. alia. “New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector-Some Initial Remarks.” Computer and Telecommunications Law Review, vol. 9, no. 5, 2003, pp. 133-138. Available at: https://researchportal.unamur.be/en/publications/new-european-directive-200258-on-the-processing-of-personal-data-
30. Marin, Luisa. “The Fate of the Data Retention Directive: About Mass Surveillance and Fundamental Rights in the EU Legal Order.” Research Handbook on EU Criminal Law, Forthcoming, Criminal Justice, Borders and Citizenship Research Paper No. 2697462, November 2015, pp. 1-21. Available at SSRN: https://ssrn.com/abstract=2697462.
31. McIntyre, TJ. “Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective.” Edward Elgar Publishing in Judges as Guardians of Constitutionalism and Human Rights, 2015, pp. 1-20. Available at SSRN: https://ssrn.com/abstract=2694512
32. Murray, Andrew. “Information Technology Law.” 4th Edition, Oxford University Press, 2019.
33. Naranjo, Diego. “E-Privacy Regulation: Good Intentions but a Lot of Work to Do.” European Data Protection Law Review (EDPL), vol. 3, no. 2, 2017, pp. 152-154. HeinOnline.
34. Nesterova, Irena. “Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards.” European Society of International Law (ESIL) 2016 Annual

Conference (Riga), January 2017, pp. 1-15. Available at SSRN: https://ssrn.com/abstract=2911999.

35. Ojanen, Tuomas. "Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12." European Constitutional Law Review, vol. 10, no. 3, December 2014, pp. 528-541. HeinOnline.
36. O'Leary, Siofra. "Balancing Rights in a Digital Age." Irish Jurist, 59, pp. 59-92. HeinOnline.
37. Opinion 6/2017 “EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation).” April 24 2017.
38. Rauhofer, Judith, and Daithi Mac Sithigh. "The Data Retention Directive Never Existed." SCRIPTed: A Journal of Law, Technology and Society, vol. 11, no. 1, April 2014, pp. 118-127. HeinOnline.
39. Roberts, Andrew. “Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v. Minister for Communications.” The Modern Law Review, vol. 78, no. 3, May 2015, pp. 535-548. Available at: https://doi.org/10.1111/1468-2230.12127
40. Rojszcak, Marcin. “National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts.” European Constitutional Law Review, 17, 2021, pp. 607-635. Available at: https://doi.org/10.1017/S1574019621000353
41. Sein, Karin. “Interplay of Digital Content Directive, European Electronic Communications Code and Audiovisual Media Directive in Communications Sector.” Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol. 12, no. 2, April 2021, pp. 169-180. HeinOnline.
42. Sippel, Birgit. “Proposal for a regulation on privacy and electronic communications.” *https://www.europarl.europa.eu/*, European Parliament, September 20, 2022. https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform?sid=6201
43. Vainio, Niklas, and Samuli Miettinen. "Telecommunications Data Retention after Digital Rights Ireland: Legislative and Judicial Reactions in the Member States." International Journal of Law and Information Technology, vol. 23, no. 3, Autumn 2015, pp. 290-309. HeinOnline.
44. Van Hoboken, Joris and Frederick Zuiderven Borgesius. “Scoping Electronic Communication Privacy Rules: Data, Services and Values.” Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol 6, no. 3, December 2015, pp. 198-210. HeinOnline.

45. Villarica, Michelle Marie. “Introductory Note to Tele2 Sverige AB v. Post-Och Telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice and Geoffrey Lewis (CJEU).” International Legal Materials 57(1), 2018, pp. 125-127. HeinOnline.
46. Voss, W. Gregory. “First the GDPR now the Proposed ePrivacy Regulation.” Journal of Internet Law, vol. 21, no. 1, July 2017, pp. 3-11. Available at SSRN: https://ssrn.com/abstract=3008765
47. Zalnieriute, Monika. “A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union.” Modern Law Review, 85(1) MLR, pp. 198-218. Available at: https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2230.12652.
48. Zanfir, Gabriela. “How CJEU’s Privacy Spring construed the human rights shield in the digital age.” European Judicial Systems as a Challenge for Democracy, 2015, pp. 111-126. Available at: https://doi.org/10.1017/9781780685236.009
49. Zanfir-Fortuna, Gabriela. “The Draft LIBE Report on the e-Privacy Regulation”. International Journal for the Data Protection Officer, Privacy offer and Privacy Counsel, vol. 1, no. 7, 2017, pp. 8-12. HeinOnline.