Applicability of ePrivacy Directive to national data retention measures following invalidation of the Data Retention Directive

Associate professor **Nina GUMZEJ**[1]

Abstract

The paper analyses rules pertinent for examination of national data retention measures regulating data processing activities of providers of electronic communication services following invalidation of the Data Retention Directive in 2014, on which subject the CJEU issued a total of five judgments up until June 2021. Focus of this analysis is the issue of applicability of EU law as interpreted in the CJEU case law, most specifically Article 15, paragraph 1 of the ePrivacy Directive containing legal safeguards for the restrictions of rights and obligations in that directive on the confidentiality of communications as well as the processing of traffic and location data. Such restrictions are as a rule manifested in different national data retention measures, which may pursue law enforcement and public security, as well as national security objectives. This examination is supported also by analysis of rules on the scope of ePrivacy Directive and its relationship with the general personal data protection framework. Overall findings in the paper provide a frame for further detailed research on the topic of future regulation of retention measures at national/EU level (Proposal for ePrivacy Regulation, possible new EU data retention legislation) and a comparative assessment of relevant CJEU jurisprudence with that of the European Court of Human Rights in respect of compatibility of retention measures with the guarantees of fundamental rights and freedoms and allowed restrictions thereof in the European legal system.

Keywords*: data retention; confidentiality of communications; ePrivacy Directive; General Data Protection Regulation; law enforcement; national security.*

JEL Classification: K24

DOI: 10.24818/TBJ/2021/11/3.02

1. Introduction

Ever since first initiatives in 2004 to regulate data retention EU-wide (with a Council Framework Decision[2]), *i.e.*, the duty of telecommunication service providers to collect and store, for the purposes of more effective fight against crime, electronic communications data pertaining to all of their users, questions were raised concerning *necessity* of that measure with regard to protected interests, and in

[1] Nina Gumzej - Faculty of Law, University of Zagreb, Republic of Croatia, ngumzej@pravo.hr.

[2] Council of the EU. "Initiative from France, Ireland, Sweden and United Kingdom: 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." 8958/04 EXT 1, Brussels, October 19, 2004.

particular *proportionality* thereof with regard to its objectives (preventing, investigating, detecting and prosecuting crime, including terrorism). This is taking into account in particular the all the more numerous and advanced possibilities of data analysis and profiling. Namely, mandatory storage of large amounts of sensitive data pertaining to communications of all users of relevant telecommunication services, indifferent to any suspicion on their perpetrating a criminal offense, and for the purpose of future potential need for some of the data relating to some of those individuals, constitutes in itself a serious interference with individuals' fundamental rights and freedoms. At the time it was in particular considered to be a significant limitation of the fundamental right to privacy in the form of the right to respect for private life and confidentiality of correspondence, as guaranteed by Article 8 of the European Convention on Human Rights.[3] In terms of guarantees of fundamental rights and freedoms as laid out in the Charter of Fundamental Rights of the European Union (hereinafter: the Charter), data retention constitutes an interference with the guarantees of the right to privacy, in particular communications privacy (Article 7) and the right to the protection of personal data (Article 8). It may, furthermore, significantly affect also the freedom of expression (Article 11). As for limitations on the exercise of rights and freedoms under the Charter, such as those posed by data retention measures, they must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, those limitations may only be made if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others (Article 52 para. 1 of the Charter).

The EU-wide data retention measure was eventually passed in form of an EU Directive 2006/24/EC (hereinafter: *Data Retention Directive*), under the first Community pillar, *i.e.,* on the basis of the rules on the functioning of the internal market[4], and above mentioned human rights concerns were touched upon by affirmations on established necessity of that measure, its having met the requirements of Article 8 of the European Convention on Human Rights, as well as ensured safeguards for the respect for private life, confidentiality of communications and personal data protection right.[5]

The aim of harmonizing retention at the level of EU law, as a proven "necessary and effective investigative tool for law enforcement in several Member

---

[3] European Parliament. "Report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks (8958/2004-C6 0198/2004-2004/0813(CNS)," Final A6-0174/2005, May 31, 2005. Note: analysis in this paper will focus on guarantees of relevant rights and freedoms as stipulated in the Charter of Fundamental Rights of the European Union.

[4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Union (hereinafter: OJ) L 105, 13.4.2006, 54-63.

[5] Recitals 9 and 22 of the Data Retention Directive. For an excellent historical overview, see: Eleni Kosta and Peggy Valcke, "Retaining the data retention directive," *Computer Law & Security Review* 22, issue 5 (2006): 370-380.

States", was to create a level playing field for providers of publicly available electronic communications services and public communications networks in the EU[6] in respect of mandatory storage of the data they process (*traffic, location data and related identification data of all of their users*) for a certain time period (6 months to 2 years), and ensure their availability for the purpose of investigating, detecting and prosecuting *serious criminal offenses*, *as defined by each EU Member State in domestic law*.[7] Required data to be retained included the data necessary to: trace and identify the source of a communication and its destination; to identify the date, time, duration and type of a communication; to identify users' communication equipment, and the data to identify the location of mobile communication equipment (data relating to content of communications were not to be retained[8]). As explained in the Commission's Proposal for the Data Retention Directive[9], unavailability of traffic data for law enforcement purposes, which data the telecommunications operators normally processed and stored for their business purposes, became particularly obvious in recent years due to development of free electronic communications services and other services, the billing of which does not depend on used traffic data (*e.g.* flat rate, prepaid tariffs, voice-over-Internet protocol). This situation is pertinent in particular to requirements of *Directive 2002/58/EC on privacy and electronic communications* (hereinafter: the *ePrivacy Directive*)[10], which regulates *inter alia* special duties of providers of electronic communication services (operators) when collecting and processing traffic data for business (including billing) purposes. In other words, the storage of data relating to above mentioned free and other services would not under the ePrivacy Directive be allowed unless there was a specifically prescribed duty requiring operators to collect and store them (such as that established under the data retention legislation).

---

[6] See Article 1, para. 1 and recitals 5-6 of the Data Retention Directive.

[7] See Articles 1, 5 and 6, as well as recital 9 of the Data Retention Directive.

[8] Article 5, para. 2 and recital 13 in connection with Article 1, para. 2 of the Data Retention Directive.

[9] "Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC", COM(2005) 438 final - 2005/0182 (COD), September 21, 2005. Also see: "Commission Staff Working Document. Annex to the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment," COM(2005) 438 final, Brussels, September 21, 2005.

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, July 31, 2002, 37-47. The ePrivacy Directive that is currently in force was last amended by Directive 2009/136/EC – the Citizens' Rights Directive: Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, December 18, 2009, 11-36.

In 2014, the CJEU issued a "landmark decision in the CJEU fundamental rights jurisprudence"[11], by which it invalidated the Data Retention Directive in its entirety (joined Cases C-293/12 and C-594/12, hereinafter also as: the 2014 ruling[12]). Concerns of exercised arbitrary powers (domination[13]) of the State in enforcement of mass data retention programmes in the prevailing interest of fighting (serious) crime lay in core of this decision. In addition to the challenges made to the national legislation governing data retention in several EU Member States also prior to the CJEU ruling[14], the Data Retention Directive invalidation formally instigated reviews of compatibility of existing national data retention schemes with the EU law, subject to varying interpretations (permissive – strict).[15] Starting from 2016 and up until June 2021 the CJEU embarked on a resolution of a number of unclear issues following Data Retention Directive invalidation, concerning the legality of existing national data retention schemes under EU law[16], on which subject it issued a total of five judgments.[17] As part of ongoing research into this topic, this paper provides a legal analysis of rules pertinent for examination of the post-2014 ruling national data retention measures. Consequently, following a brief overview of the CJEU 2014 ruling in the next section of this paper, the third section will focus on analysis of the ePrivacy Directive that is vital for assessment of the applicability of EU requirements to national data retention measures and the compatibility of such retention measures with the EU law, to the extent that such measures regulate relevant data retention

[11] Niklas Vainio 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* 23, issue 3 (Autumn 2015): 300.

[12] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources *et al*. and Kärntner Landesregierung *et al*., EU:C:2014:238.

[13] See Andrew J. Roberts, "Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications," *The Modern Law Review* 78, issue 3 (2015): 535-548.

[14] Eleni Kosta, „The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection," October 15, 2013, available at SSRN: https://ssrn.com/abstract=2675803 or http://dx.doi.org/ 10.2139/ssrn.2675803.

[15] In their analysis of relevant national developments following invalidation of the Data Retention Directive, Vainio and Miettinen observed two lines of interpretation of the 2014 ruling: permissive – by governments; strict – by domestic courts. Vainio and Miettinen, *supra* note 11, 290–309. For an excellent overview of judgments (before and after invalidation of the Data Retention Directive), see: Marek Zubik, Jan Podkowik and Robert Rybski, „Data Retention in Judgments of National Constitutional Courts," in *European Constitutional Courts towards Data Retention Laws*, Law, Governance and Technology Series - Issues in Privacy and Data Protection 45 (Cham: Springer Nature Switzerland AG, 2021), 39-173.

[16] Zlatan Meskic and Darko Samardzic, „The Strict Necessity Test on Data Protection by the CJEU: A Proportionality Test to Face the Challenges at the Beginning of a New Digital Era in the Midst of Security Concerns," *Croatian Yearbook of European Law & Policy* 13, no. 1 (2017): 139.

[17] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, EU:C:2016:970; C-207/16, Ministerio Fiscal, EU:C:2018:788; Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier ministre and Others, EU:C:2020:791; C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, EU:C:2020:790; C-746/18, Criminal proceedings against Prokuratuur, EU:C:2021:152.

(*i.e.*, data processing) activities of the providers of electronic communication services. In addition to the rules on the scope of application and its relationship with the general personal data protection framework, pertinent for research in this paper are in particular provisions of the ePrivacy Directive providing legal safeguards in the processing of different types of data pertaining to users of electronic communication services, and the rules regulating the options for Member States to derogate from those safeguards (by adopting, *inter alia*, data retention measures). The issue of applicability of ePrivacy Directive's requirements, in particular its Article 15, paragraph 1, to national data retention measures regulating activities of providers of electronic communication services, and which measures may pursue law enforcement, public security as well as national security objectives, is explored in this paper in relation to relevant CJEU judgments rendered subsequent to the 2014 ruling.

2. Invalidation of the Data Retention Directive

In the 2014 ruling, the CJEU confirmed that the retention of the data for the purpose of allowing competent national authorities to have possible access to them, does genuinely satisfy an objective of general interest, *i.e.*, contribution to the fight against serious crime and ultimately to public security. However, the proportionality principle was not respected in adoption of the Directive.[18] Consequently, the Court declared the entire Directive invalid[19], with an *ex tunc* effect. Justifications of the Court are herein provided in brief.[20]

Namely, the Directive required the retention of a very broad scope of data related to the way of using electronic communications, which are used widely and are of increasing importance in the everyday life of citizens. The data pertaining to subscribers or service users concern almost the entire European population and since a series of conclusions may on the basis of such data be made about those individuals' private lives, the data are considered particularly sensitive. Retention, therefore, constitutes a significant interference with their fundamental rights, affecting not only the right to respect to privacy but also the right to personal data protection, and it may also affect the freedom of expression: "data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those

[18] Jonida Milaj, „Invalidation of the data retention directive – Extending the proportionality test," *Computer Law & Security Review* 31, issue 5 (October 2015): 611.

[19] As commented in the doctrine: „general and radical nature of the ruling is unprecedented." Xavier Tracol, „Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it," *Computer Law & Security Review* 30, issue 6 (December 2014): 743.

[20] While a more detailed analysis by this author goes outside the scope of this paper, there is an abundance of excellent reviews and analyses available on this topic. See, for example, a list of writings maintained at the EUR-Lex database in relation to this judgment (Joined Cases C-293/12 and C-594/12), available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:62012CJ0293.

data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period. Those data, taken as a whole, 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."[21]

The data to be retained concerned also those EU citizens for whom there was no evidence whatsoever of any connection to the serious criminal offense, for the suppression of which the retention measure was prescribed, and no distinctions, limitations or exceptions were specified (*e.g.* no exceptions were provided as regards a person's communications that are subject to the duty of professional secrecy under national law).

Furthermore, the Directive failed to specify any objective criteria for the purpose of prescribing the limitation of the right of access to the data by competent national authorities and their subsequent use for the purpose of investing, detecting and prosecuting criminal offenses that may be considered sufficiently serious to justify such interference (given the scope of infringement of fundamental rights). On the contrary, it only generally referred to the serious criminal offenses as defined by each Member State in its own domestic law.

Additionally, the Directive did not prescribe substantive or procedural requirements regarding data access and their continued use by competent authorities. Access of competent authorities was not subject to the requirement of prior review either by a court or by an independent administrative body. Also, no sufficient safeguards were provided, as required under Article 8 of the Charter, to ensure effective protection of retained personal data from risks of abuse nor was there a prescribed duty of Member States to regulate those issues accordingly under national law.

As far as the retention period was concerned, the Directive prescribed no difference in relation to the different categories of retained data and, in the defined period of at least six months to two years for determining retention period in domestic law no rule was prescribed to ensure that such determination is based on objective criteria (*i.e.*, to ensure that the determined period is restricted to what is strictly necessary).

Finally, the Directive failed to ensure that the relevant operators apply a particularly high level of protection and security to the retained data, in particular by requiring irreversible destruction thereof at the end of the retention period, and the storage thereof on the EU territory.[22]

---

[21] C-293/12 and C-594/12, *supra* note 12, points 26-27.

[22] The latter, namely, departs from Article 8, para. 3 of the Charter on independent supervision of data protection and security requirements.

3. ePrivacy Directive and national data retention following invalidation of the Data Retention Directive

3.1 Introductory remarks[23]

The first Directive on privacy and telecommunications (Directive 97/66/EC[24]) was passed, following the earlier adopted *General Data Protection Directive*[25], in response to specific challenges recognized for privacy and personal data protection rights due to digital technology developments in public communication networks in the EU.[26] That directive, which was in fact "accused of being outdated at the moment of its introduction"[27] was later replaced by the current *ePrivacy Directive* due to growing risks for fundamental rights, which originated from the more recent technological developments, considerably higher data processing capacities and possibilities of new digital networks, and development of the Internet in particular.[28]

The ePrivacy Directive applies to the *processing of personal data* in connection with the provision of publicly available electronic communications services in public communications networks in the EU.[29] It "harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, 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" and aims to ensure full respect in particular for guarantees to privacy and data protection (Articles 7 and 8 of the Charter).[30] Taking this into account, the ePrivacy Directive particularized and complemented as *lex specialis* the earlier General Data Protection Directive - *lex*

[23] The analysis is based on, and, where applicable, builds upon author's findings from her earlier paper: Nina Gumzej, "Evolving Challenges and Legal Safeguards in Processing User Data in Electronic Communications," in *Proceedings of the 12th International Conference on Telecommunications – ConTEL 2013*, *Zagreb, June 26-28, 2013*, Zagreb: IEEE, 271-281.

[24] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, January 30, 1998, 1-8.

[25] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, November 23, 1995, 31-50.

[26] Article 1 (2) of Directive 97/66/EC and recitals 3, 11 thereof.

[27] Vagelis Papakonstantinou and Paul de Hert, "The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implentation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights," *The John Marshall Journal of Information Technology & Privacy Law* 29, issue 1 (2011): 40.

[28] Recitals 5-6 of the ePrivacy Directive.

[29] This is including public communications networks supporting data collection and identification devices. Article 3 of the ePrivacy Directive.

[30] Article 1, para. 1 and recital 2 of the ePrivacy Directive, respectively.

generalis.[31] Consequently, where no specific rules were established in the ePrivacy Directive, rules of the General Data Protection Directive applied to the processing of data regulated by the ePrivacy Directive that also qualified as personal data processing under the General Data Protection Directive.[32] It should here be noted also that, while the General Data Protection Directive (and its successor, the current General Data Protection Regulation[33]) regulates exclusively the processing of personal data (of natural persons), the ePrivacy Directive contains also safeguards aimed toward the protection of legal persons' legitimate interests.[34]

In its case law under the General Data Protection Directive, the CJEU interpreted the personal data concept and related issue of direct and indirect identifiability with respect to Internet Protocol (IP) addresses (traffic data/electronic communications metadata) that are assigned to the devices used by persons to connect to the Internet. It ruled that IP addresses, which are assigned by Internet access providers to their users (in order for them to be able to connect to the Internet) constitute personal data toward those providers (those operators also keep a database with their users' identification data).[35] Furthermore, IP addresses collected by other internet service providers (online media service providers) when persons access their website, and where those providers themselves have no additional data needed to identify said persons, may also constitute personal data for such providers where legal means are available toward identification of said persons with the additional data from the Internet access provider. Specifically that would be the case where a cyber-attack occurs, where legal channels exist that enable such providers to contact the competent authority (e.g. the police) so that the latter can take necessary steps to obtain the relevant identification data from the Internet access provider, on the basis of said IP addresses, and bring criminal proceedings.[36] In the present case the relevant internet service provider collecting IP addresses (data controller) did not itself have additional data enabling identification. The Court's interpretation was largely based on recital 26 of the General Data Protection Directive, according to

---

[31] See Article 1, para. 2 and recital 10 of the ePrivacy Directive. For relevant CJEU case law, see C-119/12, Josef Probst v mr.nexnet GmbH, EU:C:2012:748.

[32] "*Personal data*" under the Directive meant any information relating to identified or identifiable natural person ('data subject'), where an identifiable person is one who can be identified directly or indirectly, in particular by reference to identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, while the „*processing of personal data*" signified any operation or set of operations performed on such data (whether or not by automatic means, e.g. collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, destruction). Emphasis added by author. Article 2a-2b of the General Data Protection Directive.

[33] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, May 4, 2016, 1–88; Corrigendum: OJ L 127, May 23, 2018, 2–5.

[34] Article 1, paragraph 2 and recital 12 of the ePrivacy Directive.

[35] Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), EU:C:2011:771.

[36] C-582/14, Patrick Breyer v Bundesrepublik Deutschland, EU:C:2016:779.

which, in order to determine if a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller *or by any other person to identify the said person*. That recital is similarly reproduced in the current General Data Protection Regulation[37] and with the exclusion of important newly added examples of digital identifiers such as location data and online identifiers, core definition of personal data under the General Data Protection Regulation essentially remained same as under the earlier Directive.[38] Consequently, where identifiability of natural persons is approached in the digital context and in a networked environment, it is expected that a broad interpretation of personal data, in line with the earlier CJEU jurisprudence on the General Data Protection Directive and taking into account relevant technological developments, would continue to apply also under the General Data Protection Regulation. Furthermore, the earlier noted *lex generalis/specialis* relationship between the General Data Protection Directive and the ePrivacy Directive continues to apply also in respect of the current General Data Protection Regulation and the ePrivacy Directive.[39]

Data relating to subscribers and users, which are processed and stored by providers of public communications networks or publicly available electronic communications services in order to establish connections and transmit information, contain information on private life of natural persons and concern the right to respect for their correspondence.[40] In its jurisprudence the CJEU has repeatedly recognized that the traffic data (metadata) derived from electronic communications may reveal very sensitive information about the individual (e.g. data that makes it possible to trace and identify the source of and destination of a communication, to identify the

[37] Recital 26 of the General Data Protection Regulation: „To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, *either by the controller or by another person to identify the natural person directly or indirectly*. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". (Emphasis added by author).

[38] *Personal data* concept under the General Data Protection Regulation encompasses all information relating to an identified or identifiable natural person ('data subject'), and the *processing* thereof signifies any operation or set of operations performed on personal data, whether or not by automated means (e.g. the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction). An 'identifiable' natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity. Emphasis added by author. Article 4, paras 1-2 of the General Data Protection Regulation. Important here are also additional explanations in recital 30 of the General Data Protection Regulation, according to which: „Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them".

[39] Recital 73 of the General Data Protection Regulation.

[40] Recital 26 of the ePrivacy Directive.

date, time, duration and type of a communication, to identify users' communication device and to establish the location of mobile communication device) and which data, when taken as a whole: "is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, 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." "In particular that data provides 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." „The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance". „Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights […], the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter […]."[41]

The three categories of data regulated by the current ePrivacy Directive, which are processed by providers of electronic communication services, include: (1) traffic data, (2) location data and (3) communication (content). Data processed in the context of providing publicly available electronic communications services in public communications networks (apart from contractual personal data provided, e.g. upon subscription to the service such as a name, surname and address) include the data generated in the course of usage of such service, and in particular the traffic data and location data. Both data categories are defined in the ePrivacy Directive, as follows. The term *traffic data* stands for any data processed for the purpose of conveyance of a communication on an electronic communications network or for billing thereof (in this sense, traffic data would also include location data). Such data can *inter alia* consist of data referring to routing, duration, time or volume of a communication, used protocol, location of sender's or recipient's terminal equipment, the network on which the communication originates or terminates, beginning, end or duration of a connection, and such data may also consist of the format in which a communication is conveyed by the network.[42] *Location data* are defined as data processed in the electronic communications network as well as by an electronic communications service, which indicate the geographic position of the terminal equipment of a user of a publicly available electronic communications service. Those data may refer to latitude, longitude and altitude of user's terminal equipment, direction of travel, level of accuracy of location information, identification of the network cell in which terminal equipment is located at a certain point in time and to the time when location information was recorded.[43] The most sensitive category of data is (*content of a)*

[41] C-203/15 and C-698/15, *supra* note 17, points 98-101; C-293/12 and C-594/12, *supra* note 12, points 26-28, 37.
[42] Article 2b and recital 15 of ePrivacy Directive.
[43] Article 2c and recital 14 of ePrivacy Directive.

communication (with related traffic data). *Communication* is defined as any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service, which may include any naming, numbering or addressing information provided by the sender of a communication or user of a connection to carry out the communication (and traffic data may include any translation of this information by the network over which communication is transmitted for the purpose of carrying out transmission).[44]

In order to establish if traffic and/or location data processed by the provider of the relevant electronic communication service are also personal data[45], it is necessary to establish in each case if there is a possibility to identify the subscriber or user (natural person) to whom this data relate, as supported by reference to applicable ePrivacy and general data protection rules with respect to a specific service provider and service at hand, and relevant interpretations thereof. With respect to location data, however, the standpoint should be noted that such data will always be personal data, owing to the above stated definition of location data under the ePrivacy Directive as data indicating geographical position of terminal equipment of a user of a publicly available electronic communications service and with taking into account the definition of personal data as data relating to identified or identifiable users (natural persons).[46] Also, such data have been considered sensitive as they also involve the users' freedom to come and go anonymously.[47]

3.2 Relevant rights and obligations in the ePrivacy Directive

Where following invalidation of the Data Retention Directive, national retention measures have been reviewed before the CJEU that were adopted for law

[44] A communication does not include information conveyed as part of broadcasting service to the public over electronic communications network except to the extent that the information can be related to identifiable subscriber or user receiving the information. Article 2d, recital 15 of ePrivacy Directive.

[45] Earlier excellent examples demonstrating the complexity of this task and also various possible types of connections between the data are provided in: Arnold Roosendaal, Bert-Jaap Koop and Colette Cuijpers, "The legal framework for location-based services in Europe," FIDIS (Future of Identity in the Information Society), Deliverable D 11.5. June 12, 2007, http://www.fidis.net/fileadmin/ fidis/deliverables/fidis-WP11-del11.5-legal_framework_ for_LBS.pdf, especially at 27-28 (this work is also referenced in: Denis Royer, André Deuker and Kai Rannenberg, "Mobility and Identity," in *The Future of Identity in the Information Society: Challenges and Opportunities*, ed. Kai Rannenberg, Denis Royer and André Deuker (Berlin: Springer, 2009), 217-219. Also see: Christoph Schnabel, "Privacy and Data Protection in EC Telecommunications Law," in *EC Competition and Telecommunications Law*, 2nd edition. International Competition Law Series 6, ed. Christian Koenig, Andreas Bartosch, Jens-Daniel Braun and Marion Romes (Alphen aan den Rijn: Kluwer Law International B.V., 2009), 530-531.

[46] Article 29 Data Protection Working Party, "Opinion on the use of location data with a view to providing value-added services", WP 115, 2130/05/EN, November 2005, 3. See also Article 29 Data Protection Working Party, "Opinion 13/2011 on Geolocation services on smart mobile devices", WP 185, 881/11/EN, May 16, 2011, 8. (point 4.1. especially as to base station data processing by operators within the scope of ePrivacy Directive)

[47] Article 29 Data Protection Working Party, "Opinion on the use of location data with a view to providing value-added services", *ibid*.

enforcement purposes such as combatting crime and for the protection of public but also national security, and which measures are pertinent to communications data retention by providers of electronic communication services as well as to the access to such data by competent authorities, that Court affirmed its competence and applicability of ePrivacy Directive and relevant requirements (including, in particular, all requirements of Article 15 para. 1 of ePrivacy Directive) in relation to such national measures.

Namely, national legislation requiring operators to retain electronic communications data constitutes one possible measure that may be adopted under conditions of Article 15, para. 1 of ePrivacy Directive, since that is a national measure restricting the scope of certain rights and obligations provided for in that Directive of which most pertinent for this area are its Article 5 on confidentiality of communications and Articles 6 and 9 on traffic and location data processing.[48]

Article 5 of the ePrivacy Directive stipulates the duty of Member States to ensure through national legislation the *confidentiality of communications and related traffic data* by means of a public communications network and publicly available electronic communications services. They must especially prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data *by persons other than users*, without the consent of the users concerned, *except when legally authorised to do so in accordance with the above mentioned Article 15 para. 1 of that Directive.* The stated prohibition does not apply to technical storage necessary to transmit a communication, and to legally authorised recording of communications and related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.[49] The stated general rule on confidentiality of communications applies not only to (content of a) communication but also to the *related traffic data*. Furthermore, the rule applies *erga omnes*, *i.e.*, it is directed toward all persons (or bodies) other than users to whom the communication and traffic data relate to. Consequently, as confirmed by the CJEU in its data retention case law, this rule addresses also any measures (including data retention) that are taken by State bodies.[50]

According to ePrivacy Directive's general rule on *traffic data processing* (Article 6), traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service (operator) must be erased or made anonymous, when this data is no longer needed to transmit a communication. There are several exceptions to this rule, which include also any national measure adopted in line with Article 15 para. 1 of this Directive, *i.e.*, including data retention.

The first set of exceptions relates to the use of such data by the operators

[48] A full list of rights and obligations that may be restricted includes also the above mentioned Article 9 on the processing of location data without traffic data, and Article 8, paras. 1-4 of ePrivacy Directive on the presentation and restriction of calling and connected line identification.

[49] Article 5, paras. 1-2 of the ePrivacy Directive, see also further explanations in recitals 21-23.

[50] Joined Cases C-203/15 and C-698/15, *supra* note 17, point 77; C-207/16, *supra* note 17, point 36.

themselves, *i.e.*, the private sector.[51] Firstly, in order for the operators to be able to charge for and bill the provided service, the traffic data that is necessary for that purpose will need to be processed and stored by them, but only until expiry of the debt limitation period.[52] Secondly, operators may process and store for a limited time period the traffic data that are normally processed for billing purposes, for fraud detection and cessation purposes (unpaid use of electronic communications), and where necessary and in individual cases, for the detection of technical failure and/or errors in the transmission of communications.[53] Operators are furthermore allowed under the ePrivacy Directive[54] to process and retain users' traffic data where such data is necessary to provide a value-added service[55], or for the purpose of marketing electronic communications services, but only subject to certain conditions.[56] In connection with described uses of traffic data by operators, special safeguards have been included so as to ensure that there is no unlawful access to and/or processing of the data. More specifically, access to the data processing must only be limited to persons acting under operators' authority to carry out activities for which the data may be processed[57], and must be restricted to what is necessary for the purposes of such activities. In connection with this it should here also be noted that the CJEU confirmed the possibility of the operator to subcontract under the ePrivacy Directive the processing of such traffic data to a third party for debt collection purposes, in line with the rules on subcontracted personal data processing that are prescribed by the general data protection framework (in the concrete case, the General Data Protection Directive as *lex generalis*). Taking into account that such processing constitutes an exception to the rule on confidentiality of communications and the related traffic

[51] In the context of mandatory data retention and the retention of traffic data by operators, as regulated by the ePrivacy Directive, it was rightfully observed in the doctrine: „Yet, the victory against mandatory data retention may be largely symbolic, as metadata lives a long life in the private sector (...) Consequently, such data will often be available, even without a mandatory data retention scheme." Marie-Pierre Granger and Kristina Irion, „The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection," *European Law Review* 39, issue 6 (2014): 849.

[52] Users must be informed on the types of traffic data processed for that purpose and on the duration of such processing. For a detailed analysis of requirements with respect to processing for billing purposes, see: Article 29 Data Protection Working Party, "Opinion 1/2003 on the storage of traffic data for billing purposes," WP 69, 12054/02/EN, January 29, 2003.

[53] Recital 29 in connection with Article 6, para. 5 of the ePrivacy Directive.

[54] Additional explanations relating to the general rule and exceptions to it are provided in recitals 26 and 30 of the ePrivacy Directive.

[55] Any service requiring the processing of traffic data or location data other than traffic data beyond that what is necessary to transmit or bill a communication (e.g. services providing route guidance, traffic information and weather forecasts). See Article 2g (now 2f) for the definition, as well as recitals 18, 35 of the ePrivacy Directive.

[56] This is provided that the users gave their prior informed consent (in this sense see especially explanations in recital 30 of the ePrivacy Directive) and that only the necessary data is processed as regards those purposes and for the restricted time period corresponding to the duration of respective service provisioning, and that the (consenting) users were informed on data types and duration of processing.

[57] Billing or traffic management, customer enquiries, fraud detection, marketing communications services or the provision of value-added services.

data, any such subcontracted processing of the data may only be performed under certain strict conditions.[58] The next exception to the general rule on traffic data processing noted above permits the operators to deliver the traffic data to competent bodies in line with applicable legislation for the purpose of settling disputes, in particular interconnection or billing disputes.[59]

With respect to the applicable ePrivacy regime for *location data*, as a rule the processing thereof in mobile networks together with traffic data, in order to convey a communication or charge for the provided electronic communications service, falls under the above noted legal regime for traffic data processing. However, the processing of location data without traffic data, in order to provide a value-added service (*e.g.* location-based service)[60] that normally entails the more precise processing of location data than it is normally necessary to transmit a communication, is subject to special conditions and safeguards provided in Article 9 of the ePrivacy Directive.[61]

[58] The subcontracted third party (data processor) must act, as a person acting under the authority of the operator (data controller), solely on instructions and under control of the operator, and the agreement that they must conclude to that effect must include rules to ensure lawful processing of traffic data by the third party and allow the operator to ensure that those provisions are complied with at all times. C-119/12, *supra* note 31.

[59] According to the CJEU, this option only relates to disputes between the operator (supplier) and user as regards permitted activities and grounds for storing the data (data storage for the purposes of billing or traffic management, customer enquiries, fraud detection, marketing or provisioning of value-added services). C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, EU:C:2008:54, point 48.

[60] See *supra* note 55.

[61] Article 9 specifies: „1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time. 2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication. 3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service."

3.3 National measures restricting relevant rights and obligations under the ePrivacy Directive

Starting from its Tele2 v. Watson judgment[62], the CJEU has following the 2014 ruling established its competence and applicability of EU law requirements, including, in particular, requirements of Article 15, para. 1 of ePrivacy Directive in relation to national data retention measures, considering them as measures restricting relevant rights and obligations in that Directive, such as those on the confidentiality of communications and related traffic data, but also on traffic and location data processing that were examined in previous part of this paper.

Mentioned requirements are, firstly, that (any) such restrictive national measure must be a "*necessary, appropriate and proportionate measure within a democratic society in order to safeguard* one of the following *objectives*: national security (*i.e.,* State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system[63]*,* as referred to in Article 13 para. 1 of the General Data Protection Directive."[64] Since the General Data Protection Directive is currently no longer in force, relevant provision of the General Data Protection

[62] Joined Cases C-203/15 and C-698/15, *supra* note 17. The judgment was appropriately referred to in the doctrine as the "case about the interpretation of Article 15 of the e-Privacy Directive". Anja Møller Pedersen, Henrik Udsen and Søren Sandfeld Jakobsen, „Data retention in Europe—the Tele 2 case and beyond," *International Data Privacy Law* 8, issue 2 (May 2018): 160–174.

[63] „As regards the exception relating to unauthorised use of the electronic communications system, this appears to concern use which calls into question the actual integrity or security of the system, such as the cases referred to in Article 5(1) of Directive 2002/58 of the interception or surveillance of communications without the consent of the users concerned." C-275/06, *supra* note 59, point 52.

[64] Without prejudice to the fact that the here specified list of objectives is exhaustive (Joined Cases C-203/15 and C-698/15, *supra* note 17, points 90 and 115; C-207/16, *supra* note 17, point 52; Joined Cases C-511/18, C-512/18 and C-520/18, *supra* note 17, point 112), the CJEU interpreted in its earlier case law, unrelated to data retention, that the latter reference to the Data Protection Directive means that the objectives for adopting national restrictive measures include also the objectives specified in the mentioned Article 13, para. 1 of that Directive, which are not already listed in mentioned Article 15, para. 1 of the ePrivacy Directive. Article 13, para. 1 of the General Data Protection Directive also specifies the conditions under which Member States may adopt legislative measures to restrict the scope of certain obligations and rights in that Directive, when such a restriction constitutes a necessary measure to safeguard: (1) national security; (2) defence; (3) public security; (4) prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (5) important economic or financial interest of a Member State or of the EU, including monetary, budgetary and taxation matters; (6) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (3), (4) and (5); and (7) the protection of the data subject or of the rights and freedoms of others. As regards objective (7), here it should be noted that in its earlier case law (unrelated to data retention) the CJEU interpreted Article 15, para. 1 of the ePrivacy Directive in light of stated reference to the General Data Protection Directive, holding that since the applicable objective of protecting rights and freedoms of others (as prescribed in the latter Directive) does not specify rights and freedoms, it could *inter alia* include the protection of the right to property, or situations in which authors seek to obtain that protection in civil proceedings. C-275/06, *supra* note 59, point 53.

Regulation (Article 23, para. 1) should here apply[65], to the extent it reflects the same objectives as those specified in Article 13, para. 1 of the earlier General Data Protection Directive.[66]

Next requirement is that any such restrictive measure must comply with the general principles of Community law, including those referred to in Article 6, paras. 1-2 of the Treaty on European Union[67], and it must be in accordance with the European Convention on Human Rights, as interpreted by the rulings of the European Court of Human Rights. Measure must also comply with the general principles and fundamental rights now guaranteed by the Charter (of Fundamental Rights of the European Union). As noted earlier in the paper, of particular relevance as regards data retention measures are the Charter's guarantees of the right to privacy, in particular communications privacy (Article 7), the right to the protection of personal data (Article 8), and also relevant is the freedom of expression (Article 11). Accordingly, Article 15, para. 1 of the ePrivacy Directive is in relevant cases for the topic of this paper interpreted in light of mentioned guarantees of fundamental rights.[68]

Last, but not least, the ePrivacy Directive also regulates specific duties of relevant providers in relation to adopted national restrictive measures. Namely, they must establish internal procedures for responding to requests for access to users' personal data based on any such national provisions adopted under Article 15, para. 1 and they must provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response (Article 15, para. 1 b of ePrivacy Directive). As construed, this provision implies the authority of competent supervisory

---

[65] Comparable provisions of the General Data Protection Regulation are contained in its Article 2, paragraph 2d (material scope) and Article 23, paragraph 1 (restrictions of rights and obligations - related objectives of national/EU legislation). Thus according to the CJEU: "Although that regulation states, in Article 2(2)(d) thereof, that it does not apply to processing operations carried out 'by competent authorities' for the purposes of, inter alia, the prevention and detection of criminal offences, including the safeguarding against and the prevention of threats to public security, it is apparent from Article 23(1)(d) and (h) of that regulation *that the processing of personal data carried out by individuals for those same purposes falls within the scope of that regulation.* It follows that the above interpretation of Article 1(3), Article 3 and Article 15(1) of Directive 2002/58 is consistent with the definition of the scope of Regulation 2016/679, which is supplemented and specified by that directive." Emphasis added by author. C-623/17, *supra* note 17, point 47; Joined Cases C-511/18, C-512/18 and C-520/18, *supra* note 17, point 102.

[66] It should, however, be noted that while in Joined Cases C-203/15 and C-698/15 (Tele2 / Watson judgment) the CJEU made a reference to the entire provision (*i.e.*, which includes objectives specified in Article 13, para. 1 of the General Data Protection Directive), the CJEU, whether intentionally or not, did not include that entire reference, in the context of the comparable provision of the General Data Protection Regulation (Article 23, paragraph 1) in its subsequent data retention judgments. Compare judgments in Joined Cases C-203/15 and C-698/15, *supra* note 17, point 90 with C-623/17, *supra* note 17, point 58 and Joined Cases C-511/18, C-512/18 and C-520/18, point 110.

[67] See also recital 11 of the ePrivacy Directive.

[68] C-293/12 and C-594/12, *supra* note 12, points 25 and 28; Joined Cases C-203/15 and C-698/15, *supra* note 17, points 92-93, 101; C-623/17, *supra* note 17, points 60, 62, 72; Joined Cases C-511/18, C-512/18 and C-520/18, *supra* note 17, points 113-114, 118, 173, 186.

authorities (such as the national data protection authority) to review such procedures carried out pursuant to underlying (restrictive) national measures. It is, however, disputable whether such reviews have been implemented in the majority of Member States where national data retention measures are concerned.

One significant reason for this lays in the lacking clarity of EU *versus* Member State (exclusive) competencies, where retention is concerned, and taking into account that many have (up until the post-2014 CJEU data retention jurisprudence) considered that area to be outside the remit of EU law. In fact, that is one of the most significant drivers for preliminary reference procedures initiated on data retention measures following the 2014 ruling. In those proceedings and before the CJEU, arguments have been raised that the national data retention measures pursuing objectives such as law enforcement (combatting crime) and the safeguarding of public security (taking into account also the subject matter of such measures, *i.e.*, retention and access to retained data) and in particular those pursuing national security objectives[69] would be excluded from the scope of EU law, *i.e.*, ePrivacy Directive requirements. Main reason for this lays in the provision on material scope of ePrivacy Directive, which excludes from its scope activities of the State in criminal law areas, as well as activities concerning public security, defence and State security (*inter alia*).[70] Furthermore, as mentioned earlier in the paper, pursuant to Article 15, para. 1 of ePrivacy Directive the objectives for which Member States may adopt measures such as data retention include the national security (*i.e.*, State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offence. While admitting that „objectives which, under that provision, such measures must pursue, such as safeguarding national security, defence and public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that directive“[71] (*i.e.*, above mentioned activities and objectives that are excluded from the scope of ePrivacy Directive), the CJEU has so far in its case law rejected interpretations suggesting thereby an automatic exclusion of data retention measures adopted for mentioned purposes from the scope of ePrivacy Directive and in particular its Article 15, para. 1.[72] In other

[69] Under Article 4, paragraph 2 of the Treaty on the European Union (TEU), national security in particular remains the sole responsibility of each Member State: "The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."

[70] Article 1, para. 3 of ePrivacy Directive. Other excluded activities are those falling outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union - common foreign and security policy (note: Chapter 2 of Title V of the TEU, Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on European Union, OJ C 326, October 26, 2012, 1-390.

[71] Joined Cases C-203/15 and C-698/15, *supra* note 17, point 72.

[72] "However, having regard to the general structure of Directive 2002/58, the factors identified in the preceding paragraph of this judgment do not permit the conclusion that the legislative measures

words, those EU law requirements do apply to national data retention measures adopted for above specified law enforcement, public security but also national security purposes. It is, however, important to discern whether the data retention measure in question regulates relevant data processing activities of providers of electronic communication services, which are subject to the ePrivacy Directive.[73] As such, to the extent that those measures regulate activities of such operators, which fall within the scope of application of ePrivacy Directive, such activities (*i.e.* retention of data as well as the related granting access/transmitting of the data to law enforcement and/or security and intelligence agencies) cannot according to the Court be regarded as "activities characteristic of the State".[74] Thereby the CJEU also resisted claims of a number of EU Member States' governments on the exclusory character of Article 4 of TEU, *i.e.*, on the automated exclusion of data retention measures pursuing such objectives from the scope of EU law, *i.e.*, the ePrivacy Directive[75].

Finally yet importantly, the CJEU's finding should here be noted on the application of comparable safeguards, exclusively from the point of view of General Data Protection Regulation, for cases when national data retention measures apply to those service providers that might not fall under the scope of the ePrivacy Directive, and where such retention measures concern the personal data relating to users of their services. To be more precise, in such cases, retention is to be assessed in regard to the earlier mentioned Article 23, paragraph 1 of the General Data Protection Regulation (restrictions of rights and obligations - related objectives of national/EU legislation) and in light of relevant Articles 7, 8, 11 and 52, paragraph 1 of the Charter.[76] This corroborates yet again the intrinsic connection between the general data protection and sectoral data and privacy protection legal frameworks.

---

referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met." Joined Cases C-203/15 and C-698/15, *supra* note 17, point 73. (…) an interpretation of that directive under which the legislative measures referred to in Article 15(1) thereof were excluded from the scope of that directive because the objectives which such measures must pursue overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that same directive would deprive Article 15(1) thereof of any practical effect (…)." C-623/17, *supra* note 17, point 42; Joined Cases C-511/18, C-512/18 and C-520/18, *supra* note 17, point 97. Also see C-207/16, *supra* note 17, point 34.

[73] The ePrivacy Directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices (Article 3 of the ePrivacy Directive).

[74] Such activities would, as noted above, otherwise be excluded from Directive's scope of application. Joined Cases C-203/15 and C-698/15, *supra* note 17, points 75-76, 78; C-207/16, *supra* note 17, point 37; Joined Cases C-511/18, C-512/18 and C-520/18, *supra* note 17, point 96; C-623/17, *supra* note 17, point 39.

[75] C-623/17, *supra* note 16, points 44 and 49; Joined Cases C-511/18, C-512/18 and C-520/18, *supra* note 17, points 99, 104.

[76] For more details, see Joined Cases C-511/18, C-512/18 and C-520/18, *supra* note 17, points 193-212 (second question in Case C-512/18).

4. Concluding remarks

Examined legal provisions and CJEU jurisprudence on manifestations of EU-law mandated guarantees largely pertaining to communications and data privacy, in connection with data retention obligations subjecting electronic communications service providers, affirm the applicability of legal safeguards contained in Article 15, para. 1 of ePrivacy Directive both to national measures regulating the duty of electronic communications service providers to retain users' traffic and location data, and to the thereto unavoidably linked[77] measures regulating access to such data (retained by service providers).[78] Such measures regulate providers' data processing activities under EU law, as interpreted by the CJEU and in connection with the here examined *lex specialis/generalis* relationship between the ePrivacy Directive and the general data protection framework. Strictly focusing on application of EU law requirements, most specifically those contained in mentioned Article 15, para. 1 of the ePrivacy Directive, in relation to the different objectives pursued by national data retention measures[79], analysis in this paper has also shown affirmed applicability of EU law requirements not only to measures pursuing law enforcement and public security, but also national security objectives under specified conditions.

[77] More generally speaking: (...) if one accepts the retention-access inter-relationship, it is difficult to see how, the 'data retention' obligation could stand as a justifiable or acceptable restriction upon individual privacy in the absence of rules regulating access to the retained data, thus giving effect to its very purpose." Christiana Markou, „The Cyprus and other EU court rulings on data retention: The Directive as a privacy bomb," *Computer Law & Security Review* 28, issue 4 (August 2012): 474-475.

[78] „By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, *without imposing processing obligations on providers of electronic communications services*, the protection of the data of the persons concerned *is not covered by Directive 2002/58*, but by national law only, subject to the application of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89), with the result that the measures in question must comply with, inter alia, *national constitutional law and the requirements of the ECHR*." Emphasis added by author. C-623/17, *supra* note 17, point 48; Joined Cases C-511/18, C-512/18 and C-520/18, *supra* note 17, point 103.

[79] Already in 2014 it was argued in scientific literature that „it is crucial to precisely identify the type and seriousness of the security threat at stake in order to properly identify the needs of the democratic society implicated. In this line, it becomes necessary to distinguish, to the extent possible, between different, though closely related, concepts and in particular between the concepts of national security, public security and the prevention of crimes. Indeed, when "only" the prevention of crimes is at stake, it should be more difficult to justify interferences to the right to respect of private life." Sophie Stalla-Bourdillon, "Privacy Versus Security…Are We Done Yet?," in: Sophie Stalla-Bourdillon, Joshua Phillips and Mark D. Ryan, *Privacy vs. Security*, SpringerBriefs in Cybersecurity (London: Springer Verlag London Ltd., 2014), 67.

Taking into account in particular the *ex tunc* and *erga omnes* effect of CJEU's interpretation of Article 15, para. 1 of ePrivacy Directive[80], further research into the more extensive topic of compatibility of national data retention measures with the the guarantees of fundamental rights and freedoms and allowed restrictions thereof in the European legal system requires a comparative detailed assessment of relevant CJEU jurisprudence with that of the European Court of Human Rights, *inter alia* for the purposes of establishing consistencies and/or divergences in exercised judicial assessment.[81] In that context it is vital to also closely follow any developments surrounding possible (re-)new(ed) initiative(s) towards EU data retention legislation.[82] In addition, a close eye should be kept on relevant developments toward the Regulation on Privacy and Electronic Communications (ePrivacy Regulation), which is to replace the current ePrivacy Directive.[83] The Proposal for ePrivacy Regulation is currently still in legislative procedure and subject to numerous amendments.[84] However, once adopted, its solutions on the processing of protected data, material scope and restrictions, *i.e.*, possibilities of Member States to restrict rights and obligations under that Regulation (such as by adoption of retention measures) should be carefully assessed in respect of findings examined in this paper, in particular as regards the scope and quality of mandatory requirements ensuring the necessary and proportionate response to the thereby restricted rights and freedoms. Last, but no less important, legal certainty reasons, particularly in today's digital age pervaded by rapid technological development call for a complementary specification and clarification of the intrinsic *lex specialis/generalis* relationship between the relevant new rules, comparable to those discussed in this paper in relation to the current ePrivacy Directive, with those contained in the General Data Protection Regulation.[85]

---

[80] Xavier Tracol, „The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: The need for a harmonised legal framework on the retention of data at EU level," *Computer Law & Security Review* 33, issue 4 (August 2017): 549.

[81] This is so particularly in the context of its latest judgments on national (EU) mass-surveillance regimes. See: Case of Centrum för Rättvisa v. Sweden, Application no. 35252/08, judgment, May 25, 2021 (final); Case of Big Brother Watch and Others v. the United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15, judgment, May 25, 2021 (final).

[82] Council of the EU, „Informal video conference of justice ministers," March 11, 2021, https://www.consilium.europa.eu/en/meetings/jha/2021/03/11/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Informal+video+conference+of+justice+ministers.

[83] Europan Commission, „Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)," COM/2017/010 final - 2017/03 (COD), Brussels, January 10, 2017.

[84] For the latest version in legislative procedure (up until June 2021), see: Council of the EU, „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) - Mandate for negotiations with European Parliament," 6087/21, Brussels, February 10, 2021, https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

[85] See Article 95 of the General Data Protection Regulation.

Bibliography

1. Article 29 Data Protection Working Party, "Opinion 13/2011 on Geolocation services on smart mobile devices." WP 185, 881/11/EN, May 16, 2011.
2. Article 29 Data Protection Working Party. "Opinion on the use of location data with a view to providing value-added services." WP 115, 2130/05/EN, November 2005.
3. Article 29 Data Protection Working Party. "Opinion 1/2003 on the storage of traffic data for billing purposes." WP 69, 12054/02/EN, January 29, 2003.
4. Council of the EU. "Initiative from France, Ireland, Sweden and United Kingdom: 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." 8958/04 EXT 1, Brussels, October 19, 2004.
5. Council of the EU. „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) - Mandate for negotiations with European Parliament." 6087/21, Brussels, February 10, 2021, https://data.consilium.europa.eu /doc/document/ST-6087-2021-INIT/en/pdf.
6. European Commission. "Commission Staff Working Document. Annex to the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment." COM(2005) 438 final. Brussels, September 21, 2005.
7. European Parliament. "Report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks (8958/2004-C6 0198/2004-2004/0813(CNS)." Final A6-0174/2005. May 31, 2005.
8. Granger, Marie-Pierre and Irion Kristina. "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection." *European Law Review* 39, issue 6 (2014): 835-850.
9. Gumzej, Nina. "Evolving Challenges and Legal Safeguards in Processing User Data in Electronic Communications." In *Proceedings of the 12th International Conference on Telecommunications – ConTEL 2013*, *Zagreb, June 26-28, 2013*. Zagreb: IEEE. 271-281.
10. Kosta, Eleni. „The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection." October 15, 2013. Available at SSRN: https://ssrn.com/abstract=2675803 or http://dx.doi.org/10.2139/ssrn.2675803.
11. Kosta, Eleni and Valcke Peggy. "Retaining the data retention directive." *Computer Law & Security Review* 22, issue 5 (2006): 370–380.
12. Markou, Christiana. „The Cyprus and other EU court rulings on data retention: The Directive as a privacy bomb." *Computer Law & Security Review* 28, issue 4 (August 2012): 468-475.

13. Meskic, Zlatan and Samardzic Darko. "The Strict Necessity Test on Data Protection by the CJEU: A Proportionality Test to Face the Challenges at the Beginning of a New Digital Era in the Midst of Security Concerns." *Croatian Yearbook of European Law & Policy* 13, no. 1 (2017): 133-168.
14. Milaj, Jonida. „Invalidation of the data retention directive – Extending the proportionality test." *Computer Law & Security Review* 31, issue 5 (October 2015): 604-617.
15. Møller Pedersen, Anja, Udsen Henrik and Sandfeld Jakobsen, Søren. „Data retention in Europe—the Tele 2 case and beyond." *International Data Privacy Law* 8, issue 2 (May 2018): 160–174.
16. Papakonstantinou, Vagelis and de Hert Paul. "The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implentation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights." *The John Marshall Journal of Information Technology & Privacy Law* 29, issue 1 (2011): 29-74 .
17. Roberts, Andrew J. "Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications." *The Modern Law Review* 78, issue 3 (2015): 535-548.
18. Roosendaal, Arnold, Koop Bert-Jaap and Cuijpers Colette. "The legal framework for location-based services in Europe." FIDIS (Future of Identity in the Information Society), Deliverable D 11.5. June 12, 2007. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP11-del11.5-legal_framework_ for_LBS.pdf.
19. Royer, Denis, Deuker André and Rannenberg Kai. "Mobility and Identity." In *The Future of Identity in the Information Society: Challenges and Opportunities*, edited by Kai Rannenberg, Denis Royer and André Deuker, 195-242. Berlin: Springer, 2009.
20. Schnabel, Christoph. "Privacy and Data Protection in EC Telecommunications Law." In *EC Competition and Telecommunications Law*, 2nd ed. International Competition Law Series 6, edited by Christian Koenig, Andreas Bartosch, Jens-Daniel Braun and Marion Romes, 509-568. Alphen aan den Rijn: Kluwer Law International B.V., 2009.
21. Stalla-Bourdillon, Sophie. "Privacy Versus Security…Are We Done Yet?." In: Stalla-Bourdillon, Sophie, Joshua Phillips and Ryan Mark D., *Privacy vs. Security*. SpringerBriefs in Cybersecurity, 1-90. London: Springer Verlag London Ltd., 2014.
22. Tracol, Xavier. „Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it." *Computer Law & Security Review* 30, Issue 6 (December 2014): 736-746.
23. Tracol, Xavier. „The judgment of the Grand Chamber dated 21 December 2016 in the two joint *Tele2 Sverige* and *Watson* cases: The need for a harmonised legal framework on the retention of data at EU level." *Computer Law & Security Review* 33, issue 4 (August 2017): 541-552.
24. Vainio, Niklas and Miettinen, Samuli. „Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States." *International Journal of Law and Information Technology* 23, issue 3 (Autumn 2015): 290–309.
25. Zubik, Marek, Podkowik Jan and Rybski Robert. „Data Retention in Judgments of National Constitutional Courts." In: *European Constitutional Courts towards Data Retention Laws*. Law, Governance and Technology Series - Issues in Privacy and Data Protection 45, 39-173. Cham: Springer Nature Switzerland AG, 2021.