Ariadna H. Ochnio, Hanna Kuczyńska (eds),
Current Issues of EU Criminal Law
(Publishing House of ILS PAS 2022)
DOI: 10.5281/zenodo.6856185
pp. 89–106

Data retention obligations in the context of CJEU case law

Michalina Marcia

Abstract

The aim of the article is to present the position of the CJEU on the conditions provided for data retention provisions, and to confront them with the regulations adopted in the national legal systems. The first part discusses the case law of the CJEU regarding data retention, the admissibility of retention as such, data categories covered by retention, duration, which authorities can require access to the retained data, judicial review, and the exceptions to the main principles. In the next part, the solutions adopted in the legal orders of Member States are briefly analysed, with particular focus on Poland, in the context of the above mentioned conditions. Finally, the article addresses the issue of the procedural status of service providers and their rights in criminal proceedings.

Keywords

data retention, digital evidence, traffic data, Directive 2006/24/EC, CJEU case law, right to a fair trial

Introduction

Data retention can be defined as an obligation imposed on providers of publicly available electronic communications services or of public communications networks (service providers) to collect and store, for a defined period of time, certain data which is generated or processed by them. This is done in order to ensure that the data is available

for the purpose of the investigation, detection and prosecution of serious crime.[1] This retention applies to traffic and location data concerning both legal entities and natural persons and to the related data necessary to identify a subscriber or registered user but it does not apply to the content of electronic communications.

Definitions of traffic data can be found across a wide range of legislation. One of them is provided by Article 1 of the Convention on Cybercrime (hereinafter the Budapest Convention).[2] According to this Convention, 'traffic data' is:

> *any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service* (Article 1(d)).

The CJEU has indicated that retention can, in particular, cover the data necessary for the location of the source of a communication and its destination. Additionally, to determine the date, time, duration and type of communication, identify the communication equipment used, locate the terminal equipment and communication data which comprises, for example, the name and address of the user, the telephone numbers of the caller, the person called and the IP address for Internet services. Despite the fact that retention manifestly does not allow for the collection of communications content, it can certainly be described as a surveillance measure.

The issue of data retention moreover seems to have come to the interest of the CJEU and EU legislative bodies.[3] In one respect, recent judgments of the CJEU have significantly restricted the possible scope and grounds for retention itself, whilst in another, the European Commission introduced a proposal for a regulation concerning,

1 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 [2006] OJ L105/54, (Article 1(1)).On the invalidation of this directive see Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, EU:C:2014:238.

2 Council of Europe Convention on Cybercrime, Budapest, 23 November 2001, ETS 185.

3 See more Lilian Mitrou, 'The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive' in Kevin D. Haggerty and Minas Samatas (eds), *Surveillance and Democracy* (Routledge-Cavendish 2010) 127; Mark Taylor, 'The EU Data Retention Directive' (2006) 22 Computer Law & Security Review 309-312, Marie-Helen Maras, 'From targeted to mass surveillance: is the EU Data Retention Directive a necessary measure or an unjustified threat to privacy?' in Benjamin J. Goold, Daniel Neyland (eds), *New Directions in Surveillance and Privacy* (Routledge 2009) 74; Adam Juszczak, Elisa Sason, 'Recalibrating Data Retention in the EU. The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?' [2021] (4) EUCRIM 238-266, Thomas Wahl, 'CJEU: Data Retention Allowed in Exceptional Cases' [2020] (3) EUCRIM 184-186, Sophia Rovelli, 'Case Prokuratuur: Proportionality and the Independence of Authorities in Data Retention' (2021) 6 European Papers 199-210.

inter alia, the issue of data collection from other Member States by directly addressing the service providers which would execute the retention. This was in addition to a proposal for a directive regulating the appointment of legal representatives for service providers in connection with gathering evidence in criminal proceedings.[4] As a result, data retention creates a number of specific issues. The case law of the CJEU calls into question the compatibility of national regulations with the conditions set by this Court together with the future admissibility of evidence collected through data retention in the EU. Furthermore, the proposal for regulation mentioned above raises some doubts connected with the status of the service providers to which the requests for data will be filed.

The aim of the article is to indicate that data retention still remains one of the main problematic issues of EU criminal matters and judicial cooperation, due to the lack of legal conformity among the Member States. First, to support this thesis, the article will present the requirements established by the CJEU to identify the model data retention regulation that would be considered compliant with EU law. In the next part, the diversity of legal solutions in the Member States will be outlined in the context of the above-mentioned conditions with particular focus on the Polish legal system. The general scope of data retention, periods of retention and access to judicial review will be presented. Finally, the issue of the status of service providers will be discussed as another emerging issue connected with data retention. All these elements will make it possible to identify the current state, the future of data retention in the EU and to determine if amendments are needed at a national level to bring all the Member States into compliance with their commitments.

1. CJEU CONDITIONS ON DATA RETENTION

Data retention became an interest of the CJEU after its adoption in the European Parliament and Council Directive 2006/24/EC 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 (hereinafter Directive 2006/24/EC).[5] This directive itself caused a number of contro-

4 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters', Strasbourg, 17 April 2018, COM(2018) 225 final. See also Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters' [2018] OJ C 367/88; Commission, 'Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings', Strasbourg, 17 April 2018, COM(2018) 226 final.

5 Directive 2006/24/EC (n 1).

versies among the European national courts.[6] Finally, in the judgment of 8 April 2014, the CJEU declared Directive 2006/24/EC invalid.[7] The CJEU has referred again to this issue *inter alia* in the cases: 1) *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*,[8] 2) *La Quadrature du Net and Others v Premier ministre and Others*,[9] 3) *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*,[10] 4) *Criminal proceedings against H. K.*[11]

In its recent rulings, the CJEU has adopted a much more protective approach towards fundamental rights, especially the right to privacy, and has formulated several conditions connected with retention itself and with the use of collected data in criminal proceedings. The CJEU underlined in *La Quadrature du Net and Others v Premier ministre and Others* (para 117)[12] that data may reveal information about a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health. Given that such data, specifically, enjoys special protection under EU law, said data 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. In particular, this 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.[13]

---

6 See for example Czech Constitutional Court, Decision of 22 March 2011, Pl. ÚS 24/10, <https://www.usoud.cz/en/decisions/2011-03-22-pl-us-24-10-data-retention-in-telecommunications-services> accessed 9 January 2022; Czech Constitutional Court, Decision of 22 December 2011, Pl. ÚS 24/11, <https://www.usoud.cz/en/decisions/2011-12-20-pl-us-24-11-telecommunication-services> accessed 9 January 2022; Alexander Kashumov, 'Data Retention in Bulgaria' in Marek Zubik, Jan Podkowik, Robert Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer 2021) 75-83; Cian Murphy, 'Romanian Constitutional Court, Decision No. 1258 of 8 October 2009' (2010) 47 Common Market Law Review 933-941; Niklas Vainio, Samuli Miettinen, 'Telecommunications data retention after *Digital Rights Ireland*: legislative and judicial reactions in the Member States' (2015) 23 International Journal of Law and Information Technology 290 <https://doi.org/10.1093/ijlit/eav010>; Ludovica Benedizione, Eleonora Paris 'Preliminary Reference and Dialogue Between Courts as Tools for Reflection on the EU System of Multilevel Protection of Rights: The Case of the *Data Retention Directive*' (2015) 16 German Law Journal 1727, <https://doi.org/10.1017/S2071832200021325>.

7 Joined Cases C-293/12 and C-594/12 (n 1).

8 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.

9 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.

10 Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, EU:C:2020:790.

11 Case C-746/18 *Criminal proceedings against H. K.,* EU:C:2021:152.

12 Joined Cases C-511/18, C-512/18 and C-520/18 (n 9).

13 Case C-623/17 (n 10) para 71.

In its rulings, the CJEU referred to the regulations covering all electronic communications systems and that apply to all users of such systems, without distinction or exception, with no restriction to a particular time period, geographical area, including or instead to suspects of serious crimes. The CJEU declared in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (para 72) that mass, unrestricted retention cannot be perceived as compliant with the general principles of EU law, including the principle of proportionality, nor with the fundamental rights guaranteed in the Charter, especially the right to privacy.[14] According to the position expressed by the CJEU, in order to satisfy the requirement of proportionality, the individual regulations present in national legal systems must stipulate the clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, in order for the persons, whose personal data is affected, to have sufficient guarantees that data will be effectively protected against the risk of abuse (para 68).

Moreover, the CJEU underlined that the regulation in question must be 'legally binding under domestic law and, in particular, it must indicate in what circumstances, under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.'[15] In *La Quadrature du Net and Others v Premier ministre and Others*[16] the CJEU indicated that these safeguards are especially needed when personal data is subjected to automated processing, particularly where there is a significant risk of unlawful access to that data and when the protection of the particular category of personal data that is sensitive data is at risk (para 132). In addition, the CJEU stressed the importance of identifying a particular situation and circumstances that give rise to criminal proceedings against a particular person, prior to imposing any obligations connected with executing retention (para 143). In the view of the CJEU, as expressed in *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*,[17] retention cannot be applied to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with the objective of countering serious crime and, in particular, without there being any relationship between the data whose retention is requested and a threat to public security.[18] Such a measure would be unjustified, disproportionate and incompatible with EU principles (para 105).

One of the most important aspects stipulated by the CJEU is an adequate review of access to retained data. In *European Commission v Federal Republic of Germany*, the CJEU gave a clear outline for the shape of this review. First, it should be carried out either by a court or by an independent administrative body. To be perceived as independent, that body must have a status enabling it to act objectively and impartially when carry-

14 Case C-623/17 (n 10).

15 Ibid, para 68.

16 Joined Cases C-511/18, C-512/18 and C-520/18 (n 9).

17 Joined Cases C-203/15 and C-698/15 (n 8).

18 Joined Cases C-293/12 and C-594/12 (n 1) paras 57-58; C-203/15 and C-698/15 (n 8), para 105.

ing out its duties and must, for that purpose, be free from any external influence (para 25).[19] Moreover, according to the position of the CJEU expressed in *Criminal proceedings against H. K*, that body must be a third party in relation to the authority which requests access to the data, in order that it be able to carry out the review objectively and impartially and free from any external influence.[20] In particular, in the criminal field, the requirement of independence entails that the authority entrusted with prior review must not be involved in the conduct of the criminal investigation in question and must have a neutral stance relative to the parties to the criminal proceedings (para 54).[21] Secondly, as a rule, the review should be executed prior to the access. In cases of duly justified urgency, the review must be conducted within a brief period of the data being accessed (para 51).[22] Finally, the decision of the court or competent body should refer not only to the strict procedural aspects, but must be able to strike a fair balance between, in one respect, the interests relating to the needs of the investigation in the context of combating crime and in the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access (para 52).[23]

However, the CJEU, in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*,[24] indicated that the importance of the objective of safeguarding national security, read in the light of Article 4(2) of the TEU goes beyond that of the other objectives justifying data retention, *inter alia,* the objectives of countering crime in general, even serious crime, and of safeguarding public security. Such threats can be distinguished by their nature and particular seriousness (para 135). According to the CJEU, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives (para 136). In such cases, the Charter does not preclude a legislative measure which permits the competent authorities to order providers of electronic communications services to retain the traffic and location data of all users of their electronic communications systems for a limited period of time, on the proviso that there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat to national security which is shown to be genuine and present or foreseeable (para 138).[25] It does, however, remain unclear how the need for the collection of the data could be foreseen and, if this 'follow-up' procedure based on the exclusion of mass data retention and applicable

19 Case C-518/07 *European Commission v Federal Republic of Germany*, EU:C:2010:125, para 25; Opinion of the CJEU 1/15, 'Draft agreement between Canada and the European Union – Transfer of Passenger Name Record data from the European Union to Canada', EU:C:2017:592, paras 229-230; Case C-746/18 (n 11), para 53.

20 Case C-746/18 (n 11) paras 51-54.

21 Ibid, para 54; Opinion of AG Pitruzzella, EU:C:2020:18, para 126.

22 Case C-746/18 (n 11), para 51; Joined Cases C-511/18, C-512/18 and C-520/18 (n 9), para 189.

23 Case C-746/18 (n 11), para 52.

24 Case C-623/17 (n 10).

25 Case C-623/17 (n 10), paras 135-136.

only after the threat to national security is detected, can always be a sufficient measure to ensure the interests of the State in the face of such a threat.

Finally, in *Criminal proceedings against H. K*[26] the CJEU also addressed the issue of admitting evidence as grounds for a potential conviction. As a result, addressing the issue of the influence of data retention, not only on the right to privacy, but also on the right to a fair trial (paras 41-44). The CJEU indicated that the final evidential use of materials obtained through disproportionate and illegal electronic evidence gathering has a particular impact on the respect of the standard to a fair trial. The CJEU pointed out, *inter alia,* that the need to exclude information and evidence obtained in breach of Union law must be assessed, in particular, in the light of the risk, which the admissibility of such information and evidence presents, to respect for the adversarial principle and thus the right to a fair trial (para 44). Therefore, in the view of the CJEU, the principle of effectiveness imposes an obligation on the national criminal courts to disregard information and evidence obtained via the generalised and indiscriminate retention of traffic and location data, which is incompatible with EU law, or by means of unlawful access to those data sources by a competent authority (para 43). Especially if, in the framework of criminal proceedings instituted against persons suspected of committing a crime, these persons are not able to effectively respond to information and evidence belonging to an area not examined by the court and which may have a decisive influence on the assessment of the facts. Otherwise, the court would permit, to some extent, the possibility of violating the right to a fair trial by failing to ensure the right to active participation in the trial (para 44).

The issue of admissibility is one of the major factors connected with data retention that reflects the importance of compliance with some common standards developed among EU Member States. Research conducted by Eurojust shows a considerable amount of doubt connected with the future of admitting evidence, obtained by means of retention, inconsistent with the conditions imposed by the CJEU.[27] The literature on the subject indicates that, whilst in the Member States, during EU surveys, such evidence was still generally considered admissible for the purposes of the trial, its future, in the light of CJEU case law, remains uncertain.[28] Certainty among national legal systems is, however, one of the most important aspects of effective, judicial cooperation in criminal matters in the Union, based on the principle of mutual recognition of judgments and judicial decisions. Judicial cooperation must be grounded in mutual trust between

26 Case C-746/18 (n 11).

27 Eurojust, 'Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15 – Report, 2017' <https://www.statewatch.org/media/documents/news/2017/nov/eu-eurojust-data-retention-MS-report-10098-17.pdf> accessed 9 January 2022; European Digital Rights, 'Eurojust: No progress to comply with CJEU data retention judgments' <https://edri.org/our-work/eurojust-no-progress-to-comply-with-cjeu-data-retention-judgements> accessed 9 January 2022.

28 Marcin Rojszczak,'The uncertain future of data retention laws in the EU: Is a legislative reset possible?' (2021) 41 Computer Law & Security Review <https://doi.org/10.1016/j.clsr.2021.105572>.

Member States.[29] If procedural rights, or the standards of human rights protection differ significantly in individual states, issues regarding the mutual admissibility of evidence will appear. If these disparities and uncertainties continue despite the judgments of CJEU, perhaps it will become necessary for the European Parliament and the Council to create an act harmonising data retention provisions in order to ensure efficient, judicial cooperation.

2. Data retention in Member States

According to the studies conducted by Eurojust and the European Commission and despite the recent rulings, a majority of Member States still include mass retention provisions[30] in their legal system and there are almost no examples of targeted retention of data linked to specific persons or geographical locations.[31] As the study conducted by the European Commission showed, non-content data is also retained by service providers for purposes other than law enforcement. These purposes include national security and internal and commercial purposes, such as invoicing, marketing, network security and taxation.[32] The average maximum time period for which data can be retained is twelve months. There are, however, some exceptions.[33] Additional 'freeze periods' are also recognised, which may be requested by law enforcement agencies for investigation purposes.[34] One of the positive aspects that can be found in the existing research is that the majority of the States that were subjected to research provide for some sort of control prior to access.[35] In some of the States, in the case of an urgent situation, an *ex post* review can be executed.[36]

Data retention regulations adopted in Member States generally differ from the strict conditions of the CJEU and there appear to be signals that some of the States have, for instance, relied on the national security threat exception to reintroduce mass data retention. *Inter alia,* the French government recently declared a systematic state of emergency in France, stating, therefore, that national security is under constant threat. On this basis, the Council of State [*Conseil d'État*] rendered a decision readopting

29 Agnieszka Grzelak, 'Komentarz do Artykułu 82' in Dawid Miąsik, Nina Półtorak, Andrzej Wróbel (eds), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz (art. 1-89)*, Vol. I (Wolters Kluwer 2012).

30 Exceptions could be found for instance in Austria. See Axel Anderl, Alona Klammer, 'Data Retention in Austria' in Marek Zubik, Jan Podkowik, Robert Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer 2021) 39-52.

31 Eurojust (n 27); European Commission, Directorate General for Migration and Home Affairs, Claire Dupont, Valentina Cilli, Ela Omersa and others, 'Study on the retention of electronic communications non-content data for law enforcement purposes: final report' (2020) Publications Office, 39-48 <https://data.europa.eu/doi/10.2837/384802>.

32 European Commission (n 31), 54-57.

33 Ibid, 16.

34 The maximum period of the freeze generally oscillate around three months, ibid, 94-96.

35 Ibid, 18, 78-81.

36 Ibid, 79-80.

previous data retention provisions. This can be viewed as an attempt to circumvent the CJEU judgment and its ban on non-targeted data retention.[37]

However, whilst many of the countries commenced work on amendments to the existing provisions, numerous requests for preliminary rulings were also issued by the national courts to check their compliance with EU law. One key example of a State, in which the CJEU case law seems to have had a strong impact, is Germany. Their existing data retention provisions are currently under suspension due to administrative court decisions. In the debate on the future of data retention, maintaining 'freeze periods' as the basis of data collection has been proposed.[38] Nevertheless, the suspended regulations still provided some important guarantees that were mentioned by the CJEU in the context of proportionality.

According to Section 100g of the German Code of Criminal Procedure,[39] for example, if certain facts give rise to the suspicion that someone has, as an offender or participant, committed one of the especially serious crimes or, in cases where there is criminal liability for attempting, has attempted to commit such a crime and the act weighs particularly heavily in the individual case as well, then traffic data stored in accordance with Section 113b of the Telecommunications Act may be captured, insofar as establishing the facts or determining the whereabouts of the accused would be considerably difficult in some other way or would be futile and the data capture is appropriate in relation to the importance of the matter. The second sentence of this Section clearly defines the term of 'especially serious crimes', leaving, as a result, very little up to the discretionary power of the law enforcement agencies. These provisions, therefore, include specific terms and conditions on which data can be accessed by law enforcement agencies and, as a result, reduce the risk of unnecessary interference with citizens' right to privacy, and give a sense of legal certainty.[40]

Conversely, the Polish regulations on data retention leave much to be desired. The general basis for the measure was included in the Telecommunications Act (2004),[41]

37 European Digital Rights, 'Data retention? Advocate General says *Asked and answered!*' <https://edri.org/our-work/data-retention-advocate-general-says-asked-and-answered> accessed 9 January 2022. Proposal for maintaining mass retention was also made in Denmark. Here, targeted retention was perceived only as an emergency plan in case the general data retention regime is brought down by courts.

38 Tutanota, 'Germany: Data retention to be abolished once and for all' <https://tutanota.com/blog/posts/data-retention-germany/> accessed 9 January 2022. Currently Federal Administrative Court in Leipzig filed the request for preliminary ruling to the CJEU to clarify if the data retention provisions outlined in Germany's Telecommunications Act comply with EU law.

39 German Code of Criminal Procedure, in the version published on April 7, 1987, BGBl. I, 1074, 1319 with subsequent amendments.

40 European Digital Rights, 'Digitalcourage fights back against data retention in Germany' <https://edri.org/our-work/digitalcourage-fights-back-against-data-retention-in-germany> accessed 9 January 2022; Bundesverwaltungsgericht, Press Release No 66/2019, 'EuGH soll Vereinbarkeit der deutschen Regelung zur Vorratsdatenspeicherung mit dem Unionsrecht klären' <https://www.bverwg.de/pm/2019/66> accessed 9 January 2022.

41 Telecommunications Act (2004), Dz.U. (2021), item 576.

which *de facto* provides for indiscriminate, general, non-targeted data retention. According to Article 180a of the Telecommunications Act, an operator of a public telecommunications network and a provider of publicly available telecommunications services are obliged, at their expense, to retain and store the data generated in the telecommunications network or processed by them within the territory of The Republic of Poland for a period of 12 months from the date of the merger or unsuccessful connection attempt. This data, according to Articles 180c and 180d of the Telecommunications Act, includes *inter alia* necessary data for tracing the network termination point, telecommunications terminal equipment, the end user originating the call or being called, in addition to identifying the date and time of a call and its duration, the type of the call, and the location of telecommunications terminal equipment.

The Telecommunications Act gives legal grounds for retention obligations that can be attributed to service providers. The powers of law enforcement agencies are determined by the provisions of the Polish Code of Criminal Procedure (1997), (hereinafter the CCP).[42] The already mentioned 'freeze period' is included in Article 218a of the CCP. According to the content of this Article, offices, institutions and entities conducting telecommunications activities or providing services by electronic means, and digital service providers, are obliged to immediately secure, at the request of the court or the prosecutor, contained in the decision, for a specified period, but not exceeding 90 days, IT data stored in devices containing this data on a carrier or in the IT system. In certain cases, this measure may be combined with an obligation to prevent access to this data. The legislator also provides for a right to appeal for persons whose rights have been violated in the course of proceedings. In addition, Article 218 para 1 of the CCP provides for the general possibility of requests for correspondence and parcels and the data referred to in Articles 180c and 180d of the Telecommunications Act, if they are relevant to the proceedings. Requests, as a rule, can be ordered by the court or the public prosecutor. Nevertheless, the system of gathering evidence by means of various surveillance measures is not uniform and, in fact, its dualistic nature can be identified as a potential source of fundamental rights infringement.

The Act on the Police (1990),[43] also provides for access to the retained data but with much fewer safeguards. First, it enables access by police officers, therefore broadening the scope of authorities competent to gather data (still limited to non-content data). Moreover, according to Article 20c of the Act on the Police, there is no need for either a reasonable suspicion that a crime was committed, nor that the person in question is in any way connected with any criminal activity. In addition, no clear time frames for applying the measure are set. Finally, and of particular importance, the regulation provides for no type of direct control over the actions taken by the Police. After the

42 Polish Code of Criminal Procedure (1997), Dz.U. (1997), No 89, item 555 with subsequent amendments.

43 Act on the Police (1990), Dz.U. (2021), items 1882, 2333, 2447, 2448.

constitutionality of the regulation was questioned,[44] the legislator added Article 20ca, according to which, control over the obtaining of telecommunications, postal or internet data by the Police is within the competence of the circuit court. Furthermore, every six months the competent authorities must submit a report to the circuit court covering the number of cases in which there was the obtaining of telecommunications, postal or internet data in the reporting period, the type of such data and legal classification of offences in relation to which telecommunications, postal or internet data has been requested, or information on obtaining data in order to save human life or health or to support search or rescue activities. In addition, the circuit court may request materials that justify the disclosure of data to the Police.

However, this type of review cannot be seen as a proper procedural guarantee compatible with the requirements set out by the CJEU. It does not have the *a priori* character, does not give an insight into the individual cases and makes it impossible to assess the legality and proportionality of the measure and whether it satisfies the standards of the right to privacy and to a fair trial. As a result, Poland not only allows for indiscriminate data retention, but is one of the few EU countries that does not require a review by a court or other independent body in the process of gathering retained data for criminal trial purposes.[45]

3. The status of service providers

A further issue that should be mentioned in connection with data retention, is the status of service providers. For the reason that data collection, including both the content of communication and traffic data, becomes more widespread in criminal proceedings, opinions have been expressed that service providers should be granted special status in a trial.[46] The question arises, if the prosecution orders the disclosure of information which is, to a certain degree, private in nature, is there the possibility of contesting it in any way, invoking the right to defence? Should service providers merely be treated as witnesses, or should they have a separate procedural status?[47]

The issue in question gains relevance in the light of the proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal

44 Judgment of the Polish Constitutional Tribunal of 30 July 2014, K 23/11, [2014] (7) Orzecznictwo Trybunału Konstytucyjnego, Series A, item 80. See also Małgorzata Tomkiewicz, 'Sądowa kontrola pozyskiwania danych telekomunikacyjnych, internetowych i pocztowych' [2018] (4) Państwo i Prawo 67.

45 See also European Commission (n 31) 80.

46 Michele Simonato, 'Defence rights and the use of information technology in criminal procedure' (2014) 85 Revue Internationale de Droit Pénal 261-310 <https://www.cairn.info/revue-internationale-de-droit-penal-2014-1-page-261.html> accessed 9 January 2022.

47 Ibid, 289.

matters (hereinafter the proposal for a Regulation).[48] The proposal for a Regulation provides the possibility for competent authorities of Member States to order that a service provider,[49] offering services in the Union, produces or preserves electronic evidence, regardless of the location of the data. A European Production or Preservation Order will be transmitted to the addressee, via a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR) (Article 8 (1)). According to Article 7(1) of the proposal for a Regulation, a European Production Order and a European Preservation Order may be addressed directly to a legal representative, designated by the service provider, for the purpose of gathering evidence in criminal proceedings.

The most important issue, connected with the status of service providers contained in the provisions of the proposal for a Regulation, is reflected in Articles 9 and 15. Article 9 generally provides the premises to decline to execute an EPOC. Firstly, it addresses the more technical and formal issues. Pursuant to Article 9(3), if an EPOC is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC and the addressee cannot comply with it, he or she will inform the issuing authority referred to in the EPOC without undue delay and ask for clarification. The grounds for denial are based on the impossibility of complying with an obligation imposed by *force majeure* or the fact that this obligation is not attributable to the addressee, or, if different, the service provider, due to the fact that the data subject is not their customer, or the data has already been deleted prior to receiving the EPOC. If the relevant conditions are fulfilled, the issuing authority shall withdraw the EPOC (Article 9 (4)).

However, according to Article 9(5) of the proposal for a Regulation, in cases where the addressee considers that an EPOC cannot be executed for reasons based solely on the information contained in the EPOC, it is apparent that it manifestly violates the Charter, or that it is manifestly abusive, the addressee shall also inform the competent enforcement authority in the Member State of the addressee. In cases such as these, the competent enforcement authority may seek clarification of the European Production Order from the issuing authority, either directly or via Eurojust or the European Judicial Network. In addition, Article 10 of the proposal for a Regulation contains provisions on executing an EPOC-PR, including those relating, *inter alia*, to *force majeure*. Furthermore, Article 15 of the proposal for a Regulation provides:

> *If the addressee considers that compliance with the European Production Order would conflict with applicable laws of a third country prohibiting disclosure of the data concerned on the grounds that this is necessary to either protect the fundamental rights of the individuals concerned or the fundamental interests*

48 Commission, Proposal for a Regulation (n 4). See Stanisław Tosza 'All evidence is equal, but electronic evidence is more equal than any other: the relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law 161 <https://doi.org/10.1177/2032284420919802>.

49 See definition of 'service provider' provided in Article 2 (3) of the proposal for a Regulation.

of the third country related to national security or defence, it shall inform the issuing authority of its reasons for not executing the European Production Order in accordance with the procedure referred to in Article 9(5).

The proposal for a Regulation, in fact, gives significant, procedural powers to service providers, including the ability to influence the fundamental rights guarantees. It would seem that these powers are, in fact, of a dual nature. Firstly, service providers have gained a number of review competences with regard to the individual acts. As a result, their decisions can influence the situation of the person whose data is the subject of the order. Secondly, it can be perceived as the manifestation of a separate procedural status for service providers, including rights directly attributable to them in the EU legal system. If the proposed regulation comes into force containing wording similar to the present draft, it will significantly influence the procedural situation of service providers within the EU Member States.

Conclusions

The issues connected with data retention remain one of the major issues of EU criminal law. The regulations of Member States on data retention continue to differ from the conditions established by the CJEU and not all of those involved are willing to adjust to them to comply with the CJEU decisions on this matter. One of the most common issues is clearly demonstrated by the continuation of indiscriminate, general and mass retention being allowed. Conversely, a number of the States have started to adapt their provisions, or at least elements of them, to the standards presented in CJEU case law. The variety of legal solutions that exist across Member States may affect the standards of human rights protection during the process of evidence collection. If this issue is not resolved in the near future, one possible consequence may be the hindrance of judicial cooperation and mutual admissibility of evidence.

With regard to the Polish legal system, the provisions on data retention and access of law enforcement agencies to retained data clearly need to be amended. The most urgently required change is connected with judicial review. Introducing a review, executed by an independent body, will secure fundamental rights and allow for a proportionality assessment in every individual case. An added change that could be considered by the legislator is the introduction of a catalogue of offences and cases in which access to data may be requested.

Finally, a matter that additionally needs reconsideration, at a national level, is the status of service providers. It would seem that this should occur irrespective of whether the proposed regulation is adopted by the European Parliament and the Council. The role of service providers is not only restricted to data retention, but can also have

a significant impact in the context of other surveillance measures.[50] Therefore, it would seem that they should at least be granted the right to file an appeal against a decision in which data is requested from them.

To conclude, amendments to the existing data retention provisions in most Member States seem to be necessary in the context of the CJEU case law. In cases of a lack of common willingness to comply with existing requirements, it may appear inevitable that a proposal will be filed for a harmonising act on the means of collecting digital evidence, including data retention, and formulating a number of common standards in this regard.[51] However, as some EU countries have expressed concern over the strict conditions of the CJEU and consider the retention of traffic data necessary to sustain an effective law enforcement system, it is uncertain whether a consensus can be achieved on this matter across the entire Union.

BIBLIOGRAPHY

Legal acts

German Code of Criminal Procedure, in the version published on April 7, 1987, BGBl. I, 1074, 1319 with subsequent amendments

Act on the Police (1990), Dz.U. (2021), items 1882, 2333, 2447, 2448

Polish Code of Criminal Procedure (1997), Dz.U. (1997), No 89, item 555 with subsequent amendments

Council of Europe Convention on Cybercrime, Budapest, 23 November 2001, ETS 185

Telecommunications Act (2004), Dz.U. (2021), item 576

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 [2006] OJ L 105/54

Treaty on European Union, consolidated version [2016] OJ C 202/1

Charter of Fundamental Rights of the European Union [2016] OJ C 202/389

50 The literature also points to the problem of privilege against self-incrimination – the actions of law enforcement agencies can be perceived as an attempt to bypass the requirements of fundamental rights guarantees. See Sarah Wilson 'Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals When Third Parties Are Forced to Hand Over Passwords' (2015) 30 Berkeley Technology Law Journal 1-38 <http://www.jstor.org/stable/43917626> accessed 9 January 2022.

51 Especially taking into account that the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (n 4) clearly does not eliminate all discrepancies among national regulations and does not apply to all the problematic issues that the CJEU has referred to.

Case law

CJEU

Case C-518/07 *European Commission v Federal Republic of Germany*, EU:C:2010:125
Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, EU:C:2014:238
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
Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, EU:C:2020:790
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
Case C-746/18 *Criminal proceedings against H. K.,* EU:C:2021:152

Czech Constitutional Court

Decision of 22 March 2011, Pl. ÚS 24/10 <https://www.usoud.cz/en/decisions/2011-03-22-pl-us-24-10-data-retention-in-telecommunications-services> accessed 9 January 2022
Decision of 22 December 2011, Pl. ÚS 24/11 <https://www.usoud.cz/en/decisions/2011-12-20-pl-us-24-11-telecommunication-services> accessed 9 January 2022

Polish Constitutional Tribunal

K 23/11, 30 July 2014 [2014] (7) Orzecznictwo Trybunału Konstytucyjnego, Series A, item 80

Official documents

Opinion of the CJEU 1/15 'Draft agreement between Canada and the European Union – Transfer of Passenger Name Record data from the European Union to Canada', EU:C:2017:592
Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters' [2018] OJ C 367/88
Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters', Strasbourg, 17 April 2018, COM(2018) 225 final

Commission, 'Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings', Strasbourg, 17 April 2018, COM(2018) 226 final

Case C-746/18 *Criminal proceedings against H. K.*, EU:C:2020:18, Opinion of AG Pitruzzella

Scientific publications

Anderl A, Klammer A, 'Data Retention in Austria' in M Zubik, J Podkowik, R Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer 2021)

Benedizione L, Paris E, 'Preliminary Reference and Dialogue Between Courts as Tools for Reflection on the EU System of Multilevel Protection of Rights: The Case of the *Data Retention Directive*' (2015) 16 German Law Journal <https://doi.org/10.1017/S2071832200021325>

Juszczak A, Sason E, 'Recalibrating Data Retention in the EU. The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?' [2021] (4) EUCRIM

Kashumov A, 'Data Retention in Bulgaria' in M Zubik, J Podkowik, R Rybski (eds) *European Constitutional Courts towards Data Retention Laws* (Springer 2021)

Maras M-H, 'From targeted to mass surveillance: is the EU Data Retention Directive a necessary measure or an unjustified threat to privacy?' in B J Goold and D Neyland (eds), *New Directions in Surveillance and Privacy* (Routledge 2009)

Miąsik D, Półtorak N, Wróbel A (eds), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz (art. 1-89)*, Vol. I (Wolters Kluwer 2012)

Mitrou L, 'The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive' in K D Haggerty and M Samatas (eds), *Surveillance and Democracy* (Routledge – Cavendish 2010)

Murphy C, 'Romanian Constitutional Court, Decision No. 1258 of 8 October 2009' (2010) 47 Common Market Law Review

Rojszczak M, 'The uncertain future of data retention laws in the EU: Is a legislative reset possible?' (2021) 41 Computer Law & Security Review <https://doi.org/10.1016/j.clsr.2021.105572>

Rovelli S, 'Case Prokuratuur: Proportionality and the Independence of Authorities in Data Retention' (2021) 6 European Papers

Simonato M, 'Defence rights and the use of information technology in criminal procedure', (2014) 85 Revue Internationale de Droit Penal <https://www.cairn.info/revue-internationale-de-droit-penal-2014-1-page-261.html> accessed 9 January 2022

Taylor M, 'The EU Data Retention Directive' (2006) 22 Computer Law & Security Review

Tomkiewicz M, 'Sądowa kontrola pozyskiwania danych telekomunikacyjnych, internetowych i pocztowych' [2018] (4) Państwo i Prawo

Tosza S, 'All evidence is equal, but electronic evidence is more equal than any other: the relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law <https://doi.org/10.1177/2032284420919802>

Vainio N, Miettinen S, 'Telecommunications data retention after *Digital Rights Ireland*: legislative and judicial reactions in the Member States' (2015) 23 International Journal of Law and Information Technology <https://doi.org/10.1093/ijlit/eav010>

Wahl T, 'CJEU: Data Retention Allowed in Exceptional Cases' [2020] (3) EUCRIM

Wilson S, 'Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals When Third Parties Are Forced to Hand Over Passwords' (2015) 30 Berkeley Technology Law Journal <http://www.jstor.org/stable/43917626> accessed 9 January 2022

Online sources

Bundesverwaltungsgericht, Press Release No 66/2019, 'EuGH soll Vereinbarkeit der deutschen Regelung zur Vorratsdatenspeicherung mit dem Unionsrecht klären', <https://www.bverwg.de/pm/2019/66> accessed 9 January 2022

Eurojust, 'Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15 – Report, 2017' <https://www.statewatch.org/media/documents/news/2017/nov/eu-eurojust-data-retention-MS-report-10098-17.pdf> accessed 9 January 2022

European Commission, Directorate-General for Migration and Home Affairs, Dupont C, Cilli V, Omersa E and others, 'Study on the retention of electronic communications non-content data for law enforcement purposes: final report' (2020) Publications Office <https://data.europa.eu/doi/10.2837/384802>

European Digital Rights, 'Data retention? Advocate General says *Asked and answered!*' <https://edri.org/our-work/data-retention-advocate-general-says-asked-and-answered> accessed 9 January 2022

European Digital Rights, 'Digitalcourage fights back against data retention in Germany' <https://edri.org/our-work/digitalcourage-fights-back-against-data-retention-in-germany> accessed 9 January 2022

European Digital Rights, 'Eurojust: No progress to comply with CJEU data retention judgments' <https://edri.org/our-work/eurojust-no-progress-to-comply-with-cjeu-data-retention-judgements> accessed 9 January 2022

Tutanota, 'Germany: Data retention to be abolished once and for all' <https://tutanota.com/blog/posts/data-retention-germany/> accessed 9 January 2022

Information about the Author

Michalina Marcia is a Ph.D. candidate at the Chair of Constitutional Law, Faculty of Law, Administration and Economics, University of Wroclaw. She is, additionally, a Research Assistant at the Digital Justice Center (Academic Excellence Hub – Digital Justice). ORCID 0000-0002-7872-8507. E-mail: michalina.marcia@uwr.edu.pl.