P-ISSN 2233-3746 / E-ISSN 2720-782X
https://doi.org/10.60131/jlaw.2.2024.8331

Ketevani Kukava*

Privacy and Personal Data Protection v. the Protection of National Security and the Fight Against Crime: An Analysis of EU Law and Judicial Practice

Considering the risks that accompany technological progress, the need for personal data protection has significantly increased in today's world. While digital technology offers many benefits, it has also created unprecedented opportunities for surveillance, posing a threat to human rights and democratic values.

Fighting against crime and safeguarding national security are important legitimate aims, and processing data related to electronic communications is one of the means for their achievement. At the same time, the state's extensive power can create a sense of constant surveillance and give rise to a chilling effect. The wide discretion of state authorities and the covert nature of implemented measures generate a high risk of human rights violations. Therefore, one of the main challenges in human rights law is finding a balance between combating crime and protecting national security, on the one hand, and safeguarding human rights, on the other.

Over the past few years, the Court of Justice of the European Union has delivered significant judgments on the compliance of legal regimes governing the retention and transmission of electronic communications data with EU law. When ensuring a fair balance between different interests, the CJEU appropriately considers both the threats present in the modern world and the importance of human rights protection.

The present article discusses the processing of personal data in the electronic communications sector under EU law and analyses the development of the case law of the Court of Justice of the European Union.

Keywords: *Electronic Communications, Data Retention, National Security, Court of Justice of the European Union*

1. Introduction

The right to privacy enables individuals to freely develop their own personality, opinions, and relationships. At the same time, this right is a precondition for exercising other human rights and is one of the vital values of a democratic society.

Digital technology has created an unprecedented opportunity for surveillance, which poses a serious threat to privacy and the right to personal data protection. In today's world, vast amounts of personal information are collected and processed through increasingly sophisticated methods.

Modern technology is an integral part of people's daily lives. While individuals voluntarily disclose personal information in exchange for access to services and information, given the present

* Ph.D. student of Ivane Javakhishvili Tbilisi State University Faculty of Law.

state of technological dependency, refusing to use electronic means of communication would mean foregoing significant social interaction to such an extent that it can hardly be considered an option.[1] In a digitally interconnected society, it makes less sense to refuse the use of technologies and still fully participate in society.[2]

Considering the risks that accompany technological progress, the need for personal data protection has significantly increased. The Charter of Fundamental Rights of the European Union (hereinafter "Charter") guarantees the right to the protection of personal data[3] alongside the right to respect for private and family life.[4] Moreover, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law, respect the essence of those rights and freedoms, and comply with the principle of proportionality.[5]

The protection of national security and the fight against crime are important legitimate aims, and processing data related to electronic communications is one of the means for their achievement. At the same time, robust safeguards against state authorities' arbitrariness and abuse of power are essential for protecting democratic values.

The legal regime governing the retention of data related to electronic communications and state authorities' access to that data has often been the subject of broad discussion and debate. The standard developed in the case law of the Court of Justice of the European Union (hereinafter "CJEU") is of particular significance in this regard, as it aims to balance the objectives of combating crime and safeguarding national security, on the one hand, with the protection of human rights, on the other.

The present article aims to discuss the processing of personal data in the electronic communications sector under EU law and to analyse the development of the CJEU's case law.

2. Directive 2002/58/EC on Privacy and Electronic Communications

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter "Directive 2002/58" or "Directive on privacy and electronic communications") aims to ensure the protection of fundamental rights and freedoms and in particular, the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and electronic communication equipment and services in the EU.[6]

---

1 *Ronen Y.,* Big Brother's Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers, Utrecht Journal of International and European Law, Vol. 31, Nº 80, 2015, 73.

2 *Karaboga M., Matzner T., Obersteller H., Ochs C.,* Is there a Right to Offline Alternatives in a Digital World? in Data Protection and Privacy: (In)visibilities and Infrastructures, *Leenes R., Brakel R.v., Gutwirth S., Hert P.D.,* (eds.), Springer International Publishing AG, 2017, 54.

3 Charter of Fundamental Rights of the European Union, 07/12/2000, Article 8.

4 Ibid, Article 7.

5 Ibid, Article 52 (1).

6 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 (Directive on privacy and electronic communications), Article 1 (1).

Directive 2002/58 deals with the processing of the following three categories of data by the providers of electronic communications services: traffic data,[7] location data[8], and the content of the communication. This Directive enshrines the principle of confidentiality of both the electronic communications and the related traffic data.[9] By adopting the Directive on privacy and electronic communications, the EU legislature established important safeguards to respect private and family life and to protect personal data.

Article 15 of Directive 2002/58 enables Member States to determine the exceptions when the restriction of the scope of the rights and obligations constitutes a necessary, appropriate, and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection, and prosecution of criminal offences.[10] To this end, Member States may adopt legislation regarding the retention of data for a limited period.[11] That being said, the possibility to derogate from the rights and obligations provided for by Directive 2002/58 cannot permit the exception to become the rule.[12]

It is important to note that Directive 2002/58 does not apply to activities concerning public security, defence, state security, and the activities of the state in areas of criminal law.[13] In addition, according to the Treaty on European Union, national security remains the sole responsibility of each Member State.[14] Nevertheless, according to the CJEU's interpretation, national legislation enabling a state authority to require providers of electronic communications services to retain and transmit traffic and location data to the security and intelligence agencies falls within the scope of Directive 2002/58.[15]

It is also worth noting that the 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, which is intended to replace the 2002/58 Directive, is still under consideration. As of today, this Regulations has not yet been adopted. Further information is available here: <https://eur-lex.europa.eu/procedure/EN/2017_3> [10.08.2024].

7 "Traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Directive 2002/58, Article 2 (b).

8 "Location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. Directive 2002/58, Article 2 (c).

9 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 (Directive on privacy and electronic communications), Article 5.

10 Ibid, Article 15 (1).

11 Ibid.

12 C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, [2020], CJEU, § 59.

13 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 (Directive on privacy and electronic communications), Article 1 (3).

14 Treaty on European Union, 07/02/1992, Article 4 (2).

15 Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, [2020], CJEU, § 104. C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, [2020], CJEU, § 49.

3. Invalidation of the Data Retention Directive 2006/24/EC

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 (hereinafter "Data Retention Directive" or "Directive 2006/24") obliged the providers of publicly available electronic communications services and of public communications networks to retain certain data and ensure that those data are available to competent authorities for the investigation, detection, and prosecution of serious crime. The Data Retention Directive covered in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation, or exception.[16] Even though Directive 2006/24 did not permit the retention of the content of the communication, the retained data, taken as a whole, might allow drawing very precise conclusions concerning the individuals' private lives, such as the habits of everyday life, permanent or temporary residences, daily or other movements, social relationships they maintained and the social environments they frequented.[17]

In 2014, the Grand Chamber of the CJEU invalidated the Data Retention Directive. According to the Court, the fight against serious crime, in particular, organized crime and terrorism, is critical for ensuring public security, and its effectiveness may largely depend on the use of modern investigation techniques.[18] However, such an objective does not in itself justify a retention measure established by Directive 2006/24.[19]

The Data Retention Directive applied to everyone, who used electronic communications services. It applied even to persons for whom there was no evidence suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.[20] Moreover, it did not lay down any objective criterion to limit the number of persons authorised to access and subsequently use the retained data strictly by necessity.[21] The access to the retained data by the competent national authorities was not dependent on a prior review by a court or an independent administrative body.[22] Directive 2006/24 set the retention period at a minimum of 6 months and a maximum of 24 months but did not specify that the determination of the retention period must be based on objective criteria.[23] Overall, according to the CJEU, the Data Retention Directive did not comply with the principle of proportionality.

4. The Rules for Retention and Transmission of Data Related to Electronic Communications Based on the Case Law of the CJEU

Following the invalidation of Directive 2006/24, the validity of national data retention regimes was called into question. Consequently, two references for a preliminary ruling were submitted to the

16 C-293/12, C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, [2014], CJEU, §§ 57-59.
17 Ibid, § 27.
18 Ibid, § 51.
19 Ibid.
20 Ibid, § 58.
21 Ibid, § 62.
22 Ibid.
23 Ibid, § 64.

CJEU, which served as the basis for assessing the compliance of Swedish and UK legislation with Directive 2002/58 and the Charter. In its 2016 judgment, the CJEU ruled that the national legislation allowing authorities, for the purpose of combating crime, to impose on the providers of electronic communications services the obligation of general and indiscriminate retention of traffic and location data did not comply with Directive 2002/58, read in the light of the Charter.[24]

At the same time, according to the CJEU, Member States may adopt legislation permitting the targeted retention of data for the purpose of fighting serious crime, provided that sufficient safeguards are in place to ensure the effective protection of personal data against the risk of misuse.[25] Access by the competent national authorities to retained data should, as a general rule, except in cases of duly justified urgency, be subject to a prior review carried out either by a court or by an independent administrative body,[26] and the data must be retained within the European Union.[27]

Following the 2016 judgment, legal discussions concerning the retention and transmission of data persisted. The CJEU's ruling of 6 October 2020 related to the processing of data for national security purposes is noteworthy in this regard. The CJEU assessed the UK legislation that permitted the Secretary of State to require providers of electronic communications services, in the interests of national security, to transmit traffic and location data to the security and intelligence agencies. According to the Court's assessment, such a regulation has the effect of making an exception to the principle of confidentiality the rule[28] and is likely to generate the feeling of constant surveillance.[29] The CJEU regarded the transmission of data to the security and intelligence agencies as a particularly serious interference with the right to privacy.[30]

The regime for the transmission of traffic and location data affected all persons using electronic communications services, regardless of whether they had a link, even an indirect one, with a threat to national security.[31] According to the CJEU's interpretation, EU law precludes national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic and location data to the security and intelligence agencies for the purpose of safeguarding national security.[32]

On 6 October 2020, the CJEU delivered another important judgment determining the rules for the retention of traffic and location data, IP addresses, and data relating to the civil identity of users of electronic communications systems.[33] In this case, the CJEU assessed the compliance of the legislation

---

24 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, [2016], CJEU.

25 Ibid, §§ 108-109.

26 Ibid, § 120.

27 Ibid, § 122.

28 C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, [2020], CJEU, § 69.

29 Ibid, § 71

30 Ibid.

31 Ibid, § 80.

32 Ibid, § 82.

33 Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, [2020], CJEU.

of France and Belgium with Article 15(1) of Directive 2002/58, as read in light of the Charter. The standards established by this judgment can be summarised as follows:

1) EU law does not preclude blanket retention of traffic and location data by providers of electronic communications services for national security purposes provided that the following conditions are met: a) This measure can be used when the state concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable;[34] b) The instruction for the preventive retention of data of all users must be limited in time to what is strictly necessary and be subject to robust safeguards to protect effectively the personal data against the risk of abuse. Therefore, data retention cannot be systematic in nature.[35] The instruction for data retention may be renewed if that threat persists.[36] c) Decisions instructing providers of electronic communications services to retain data must be subject to effective review by a court or an independent administrative body whose decisions are binding.[37] Such a review aims to verify the existence of a serious threat and to ensure that appropriate safeguards are in place.[38]
2) EU law precludes blanket retention of traffic and location data by providers of electronic communications services for the purposes of combating crime and safeguarding public security.[39]
3) EU law does not preclude targeted retention of traffic and location data by providers of electronic communications services for the purposes of combating serious crime, preventing serious attacks on public security and, a fortiori, safeguarding national security, provided that such retention is limited, with respect to the categories of data, the means of communication, the persons concerned and the retention period, to what is strictly necessary.[40]
4) EU law does not preclude blanket retention of IP addresses by providers of electronic communications services for the purposes of combating serious crime, preventing serious threats to public security, and safeguarding national security, provided that such retention complies with the substantive and procedural conditions regulating the use of that data.[41]
5) EU law does not preclude a legislative measure that requires providers of electronic communications services to retain data relating to the civil identity of all users of electronic communications systems for the purposes of preventing, investigating, detecting, and prosecuting criminal offences and safeguarding public and national security.[42]
6) EU law does not preclude expedited retention of traffic and location data by providers of electronic communications services for a specified period for the purposes of combating serious

34 Ibid, § 137.
35 Ibid, § 138.
36 Ibid, § 138.
37 Ibid, § 139.
38 Ibid.
39 Ibid, §§ 141-143.
40 Ibid, §§ 146-147.
41 Ibid, §§ 155-156.
42 Ibid, § 159.

crime and safeguarding national security.[43] A decision of the competent authority should be subject to effective judicial review.[44]

7) EU law permits automated analysis of the traffic and location data of all users of electronic communications systems, for a strictly limited period, for the purpose of safeguarding national security.[45] Such a measure is subject to the conditions related to the blanket retention of data for the purpose of safeguarding national security.[46]

8) EU law permits national legislation obliging providers of electronic communications services to ensure the real-time targeted collection of traffic and location data.[47] A decision authorising the real-time collection of data must be based on objective and non-discriminatory criteria provided for in national legislation, must be subject to a prior review by a court or an independent administrative body, and in case of duly justified urgency, its lawfulness must be examined within a short time.[48]

These judgments provide useful guidance with respect to achieving a balance between the right to privacy and personal data protection, on the one hand, and national security interests, on the other. The CJEU considers both the threats present in the modern world and the importance of human rights protection. At the same time, it is important to analyse the 2020 judgments in light of the standards established by previous rulings.

In contrast to the judgments delivered in 2014 and 2016, which dealt with relatively simple data retention regimes aimed at combating crime,[49] the 2020 ruling weighed national security interests against personal data protection.[50] Furthermore, the CJEU discussed broader categories of data: in addition to traffic and location data, IP addresses and data related to the civil identity of users were also considered. The categories of data, data processing operations, and their purposes made the 2020 judgment more complex than its predecessors.[51]

Where in its 2014 judgment, the CJEU invalidated the Data Retention Directive, and in 2016, it prohibited blanket and indiscriminate data retention for the purpose of combating crime, in its 2020 ruling, the Court examined the exceptional circumstances under which EU law permits blanket data retention. At the same time, the CJEU established strict conditions for such measures.[52]

It is worth noting that in its 2020 judgment, the CJEU emphasized the importance of a review by the court or an independent administrative body. However, such a review is not mentioned with

---

43 Ibid, §§ 163-164.
44 Ibid, § 163.
45 Ibid, § 178.
46 Ibid, §§ 176-179.
47 Ibid, § 188.
48 Ibid, § 189.
49 *Eskens S.,* The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-depth Review of La Quadrature du Net and Others and Privacy International, Vol. 8, Issue 1, 2022, 143.
50 Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, [2020], CJEU.
51 *Eskens S.,* The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-depth Review of La Quadrature du Net and Others and Privacy International, Vol. 8, Issue 1, 2022, 143.
52 Ibid.

regard to targeted retention of data, retention of IP addresses, or identifying data.[53] This may be due to the CJEU viewing these forms of data retention as relatively mild interference with fundamental rights; however, it has been pointed out that this might give rise to some questions in the future.[54]

The judgments discussed above underscore the importance of protecting traffic and location data. According to the CJEU's assessment, such data may reveal a wide range of information about an individual's private life, including sensitive information.[55] These data may enable very precise conclusions about the private lives of individuals and provide a means to establish profiles of those concerned – information that is no less sensitive, with respect to the right to privacy, than the actual content of communications.[56] The CJEU's discussion is grounded in a proper understanding of the significant challenges present in the digital age. Considering the increasing capabilities of modern technologies, linking and extracting entirely new information has become easier.[57] Therefore, the protection of any type of personal data gains crucial importance.

It is worth noting that the retention of data related to electronic communications affects not only privacy and the right to personal data protection but also freedom of expression, as guaranteed by Article 11 of the Charter. Mass collection of such data can result in a chilling effect, as the mere feeling of surveillance prompts people to restrict their freedom of expression.[58] The CJEU explicitly highlights that the retention of traffic and location data can impact the use of means of electronic communication and, consequently, the exercise of freedom of expression, as such measures may lead individuals to feel that their private lives are under constant surveillance.[59]

The CJEU adopts a more lenient approach towards blanket data retention for the purpose of safeguarding national security, as opposed to its stance on combating serious crime and protecting public safety. To ensure a robust national security regime states employ sophisticated technologies and implement significant measures, and the CJEU largely supports this approach. The aforementioned judgments illustrate that the Court adopts a pragmatic approach when ensuring a fair balance between competing interests.

At the same time, the CJEU's discussion gave rise to criticism for different reasons. Several states deemed the proportionality test on data retention to be excessively stringent and the suggested

---

53 Ibid, 154.

54 Ibid.

55 Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, [2020], CJEU, § 117.

56 Ibid.
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, [2016], CJEU, § 99.
C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, [2020], CJEU, § 71.

57 *Karaboga M., Matzner T., Obersteller H., Ochs C.,* Is there a Right to Offline Alternatives in a Digital World? in Data Protection and Privacy: (In)visibilities and Infrastructures, *Leenes R., Brakel R.v., Gutwirth S., Hert P.D.,* (eds), Springer International Publishing AG, 2017, 45.

58 *Buono I., & Taylor A.,* Mass Surveillance in the CJEU: Forging European Consensus, Cambridge Law Journal, Vol. 76, No. 2, 2017, 251.

59 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, [2016], CJEU, §§ 100-101.

solutions, such as the targeted data retention, impractical or ineffective.[60] On the other hand, human rights defenders, who advocate for a total ban on mass surveillance instruments, view the CJEU's recent judgments "as a form of legalizing unlimited surveillance methods for national security purposes."[61]

5. Conclusion

Considering the threats present in the modern world, states process electronic communications data to prevent serious crimes and to safeguard national security, which may pose a risk to privacy and the right to personal data protection. Therefore, striking a fair balance between combating crime and protecting national security, on the one hand, and safeguarding human rights, on the other, is one of the main challenges in human rights law.

According to the Treaty on European Union, national security remains the sole responsibility of each Member State.[62] Nevertheless, the judgments of the CJEU clarify that national legislation obliging providers of electronic communications services to retain and transmit data for national security purposes falls within the scope of Directive 2002/58.

Notably, EU law prohibits the blanket transmission of traffic and location data to security and intelligence services for national security purposes, as such practices create a sense of constant surveillance and transform the exception to the principle of confidentiality into the rule.

Furthermore, the CJEU has clearly determined the rule for the retention of data related to electronic communications. In contrast to targeted data retention, blanket retention affects everyone, regardless of whether they have any connection to a specific threat or crime. The CJEU ruled that blanket retention of data cannot be justified by the interest of combating serious crime; however, this measure can be employed for the purpose of safeguarding national security. At the same, in this case, data retention cannot be systematic and this measure can only be applied when the state is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable. Furthermore, one of the key safeguards for the protection of human rights is review by a court or an independent administrative body. Therefore, instead of fully prohibiting the blanket retention regime, the judges opted to establish clear limits and a strict proportionality test.

In summary, EU law and judicial practice appropriately consider both the threats present in the modern world and the importance of protecting human rights. At the same time, ensuring robust safeguards against abuse at the national level and their effectiveness is essential for protecting democratic values.

Bibliography:

1. Charter of Fundamental Rights of the European Union, 2000.
2. Treaty on European Union, 1992.

60 *Celeste E., Formici G.,* Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia, German Law Journal, 2024, 18.

61 Ibid.

62 Treaty on European Union, 07/02/1992, Article 4 (2).

3. 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 (Directive on privacy and electronic communications).
4. *Buono I., & Taylor A.,* Mass Surveillance in the CJEU: Forging European Consensus, Cambridge Law Journal, Vol. 76, No. 2, 2017, 251-253.
5. *Celeste E., Formici G.,* Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia, German Law Journal, 2024, 13, 18.
6. *Eskens S.,* The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-depth Review of La Quadrature du Net and Others and Privacy International, European Data Protection Law Review (EDPL), Vol. 8, No. 1, 143.
7. *Karaboga M., Matzner T., Obersteller H., Ochs C.,* Is there a Right to Offline Alternatives in a Digital World? in Data Protection and Privacy: (In)visibilities and Infrastructures, *Leenes R., Brakel R.v., Gutwirth S., Hert P.D.,* (eds), Springer International Publishing AG, 2017, 45, 54.
8. *Ronen Y.,* Big Brother's Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers, Utrecht Journal of International and European Law, Vol. 31, Nº80, 2015, 73.
9. Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others, [2020], CJEU.
10. C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, [2020], CJEU.
11. 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, [2016], CJEU.
12. C-293/12, C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, [2014], CJEU.