UDC 343.985(497.11); 351.746.2(497.11)
CERIF: S 149
DOI: 10.51204/Anali_PFBU_25104A

Milana M. PISARIĆ, PhD*

Ostoja S. KALABA, LL.M.**

*DATA RETENTION AND CRIMINAL PROCEDURE IN SERBIA****

The use of information technology enables state authorities to prosecute perpetrators and process personal data on an unprecedented scale and in an unimaginable way, in the course of taking measures and actions to prevent, detect and investigate criminal acts. One of the disputed processing is the nonselective mass monitoring of electronic communications in the form of retention of communication data, which, given the technological development and social importance of electronic communications, can on occasion reveal more about an individual than the content of the communication itself. This form of data processing represents interference with guaranteed human rights and freedoms, and need to be legally regulated in order to prevent their violation. The authors analyze the legal framework for retention of communication data and access to retained data for the purposes of criminal proceedings in Serbia, especially in light of the relevant practices of the CJEU and ECtHR.

Key words: *Electronic communications*. – *Data retention*. – *Criminal procedure*. – *Personal data protection*. – *Privacy*.

---

* Assistant Professor, University of Novi Sad Faculty of Law, Serbia, *mpisaric@pf.uns.ac.rs*, ORCID iD: 0000–0001–8344–3349.

** Advisor in the Office of the Commissioner for Information of Public Importance and Personal Data Protection, PhD student, Serbia, *kalaba.ostoja@gmail.com*.

*** Certain parts of this research were presented as an oral communication titled "Data Retention and Access to Retained Data for the Purpose of Criminal Procedure in Serbia", at the conference SSN2024: Surveillance in an Age of Crisis: the 10th Biennial Surveillance Studies Network / Surveillance & Society Conference 2024, hosted by the Institute of Criminology at the Faculty of Law and the University of Ljubljana Faculty of Law, Slovenia, held 28–31 May 2024, at the University of Ljubljana Faculty of Law.

1. INTRODUCTION

When Edward Snowden revealed that the NSA had been extensively collecting call detail records, a large portion of the world was shocked and surprised. Although the sitting President of the United States stated in a speech early 2014, among other things, that such a system does not collect the content of phone calls or the identities of the people involved (*Washington Post* 2014), the academic and professional community also understood what had been left unsaid – that this involved the mass collection of metadata, and that such surveillance encroached on privacy without the appropriate strict criteria for its application and effective oversight by independent supervisory authorities, which was potentially also a violation of certain fundamental human rights and freedoms, steering society towards an Orwellian reality.[1] At the time this "practice" was not unique to the United States, nor is it at the present; for years, it has justifiably been the subject of public and academic discourse,[2] (inadequate) regulation, and the consequent judicial review in many countries.

EU law has influenced the legal framework for electronic communications in Serbia, including in terms of data retention and access to such data. With the adoption of the Data Retention Directives (Directive 2006/24/EC)[3] at the Union level, an obligation was created for providers of publicly available electronic communication services and public communication networks to retain certain data they collect or process in connection with these services, in order to ensure their availability to competent authorities for the purpose of detecting and proving serious criminal offences, as well as for the detection and prosecution of perpetrators of such offences. However, the Serbian legislator has not sufficiently and appropriately followed the further development of Directive 2006/24/EC and data retention regulations of EU member states, especially considering the rulings of the Court of Justice of the EU (CJEU). Furthermore, the relevant decisions of the European Court of Human Rights (ECtHR), establishing violations of the rights under the European Convention on Human Rights (ECHR) related to data retention, were also not taken into account. In this paper, the authors analyze the

[1] For more on this, see Pisarić (2019, 156).

[2] For more on this, see, e.g., Rojszczak 2021a; Rojszczak 2021b.

[3] 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, OJ L 105/54 of 13/4/2006.

domestic legal framework for data retention and the access of competent authorities to retained data for the purpose of criminal proceedings, particularly examining it through the lens of the decisions of the CJEU and the ECtHR.

2. LEGAL FRAMEWORK IN SERBIA

In Serbia, data retention of electronic communications, following the example of Directive 2006/24/EC, was regulated in 2010 with the adoption of the Law on Electronic Communications (LEC),[4] within Chapter XVII: Confidentiality of Electronic Communications, Lawful Interception, and Data Retention. Some provisions from this chapter were declared unconstitutional in 2013 by the Decision of the Constitutional Court of the Republic of Serbia (Decision of the CC),[5] while some were amended in 2014.[6] Following these interventions, the provisions from Chapter XVII remain in effect, despite the adoption of the new Law on Electronic Communications[7] in 2023 (LEC 2023). Namely, Article 180, para. 1 LEC 2023 stipulates that with the entry into force of this law, the previous Law on Electronic Communications ceased to apply, and at the same time, for inexplicable and legislatively unjustified reasons, establishes that certain provisions of the LEC remain in force, including the provisions on data retention. As the new regulation governing electronic communications failed (or avoided) to address data retention, the relevant provisions have unnaturally and incoherently remained outside the core text of the systemic law. For a comprehensive understanding of the legal framework for data retention, it is important to note that the general rules are contained in several articles of the LEC and are more specifically regulated in bylaws (adopted based on the law that is no longer in force). In the following sections, we will analyze data retention and access to retained data as two steps of a single mechanism.

[4] Law on Electronic Communications, *Official Gazette of the Republic of Serbia* 44/10.

[5] Constitutional Court of the Republic of Serbia, Iuz 1245/2010, 13 June 2013, *Official Gazette of the Republic of Serbia* 60/13.

[6] Law on Amendments to the Law on Electronic Communications, *Official Gazette of the Republic of Serbia* 62/2014.

[7] Law on Electronic Communications, *Official Gazette of the Republic of Serbia* 35/23.

2.1. Data Retention

2.1.1. Purpose of Retention

In the text of the original LEC, Article 128, para. 1 stipulated that the operator was obliged to retain data on electronic communications for the purposes of conducting investigations, detecting criminal offenses, and carrying out criminal proceedings, in accordance with the law regulating criminal procedure, as well as for the purposes of protecting national and public security of the Republic of Serbia, in accordance with the laws regulating the work of the security services of the Republic of Serbia and the Ministry of the Interior. The part of the provision referring to these other laws was declared unconstitutional in 2013 by the Decision of the CC.[8] The following year, Article 128 was amended, and the purpose of data retention was completely omitted. The currently LEC currently in effect simply stipulates the operator's obligation to retain data on electronic communications (Article 128, para. 1) and to keep the retained data for 12 months from the date of the communication (Article 128, para. 6), without specifying the purpose for which these obligations are established.

2.1.2. Retained Data

With regard to the data for which operators have obligations, Article 128, para. 1 LEC refers to Article 129, para. 1, which establishes the categories of data that is to be retained to meet specific needs. The answer to the question of which data is specifically retained is provided by the bylaw – the Rulebook on the Requirements for Devices and Software Support for Lawful Interception of Electronic Communications and Technical Requirements for Fulfilling the Obligation of Data Retention on Electronic Communications[9]

[8] The Constitutional Court found that the phrase "in accordance with the law regulating criminal procedure" and the phrase "in accordance with the laws regulating the work of the security services of the Republic of Serbia and the work of law enforcement authorities" are not in compliance with Article 41 para. 2 of the Constitution, as only a court is competent to permit (approve) a deviation from the constitutionally guaranteed inviolability of the secrecy of letters and other means of communication, "and not that this right is determined in accordance with the law." Translation by author. See Decision of the CC, p. 79.

[9] Rulebook on the Requirements for Devices and Software Support for Lawful Interception of Electronic Communications and Technical Requirements for Fulfilling the Obligation of Data Retention on Electronic Communications, *Official Gazette of the Republic of Serbia* 88/2015.

(Rulebook[10]) – which, in Articles 11–16, exhaustively specifies the data that operators are required to retain. The data retained is necessary for: 1) monitoring and determining the source of the communication,[11] 2) determining the destination of the communication,[12] 3) determining

[10] Originally, Article 129, para. 4 LEC stipulated that the ministry responsible for telecommunications would prescribe in more detail the requirements related to the retention of data referred to in Article 129, para. 1, having previously obtained opinions from the ministry responsible for justice, the ministry in charge of internal affairs, the ministry in charge of defense, the Security Information Agency, and the authority in charge of personal data protection,. When the CC of Serbia declared Article 128, para. 5 unconstitutional, it also invalidated Article 129, para. 4 – thus eliminating the legal basis for regulating the obligation to retain data through subordinate legislation. However, such a regulation was adopted nonetheless. Specifically, Article 127, which governs the lawful interception of electronic communications, was amended in 2014 to include, in paragraph 5, a provision that the ministry shall also prescribe technical requirements for fulfilling the data retention obligations under Articles 128 and 129 of the law. The Rulebook in question was adopted based on this provision.

[11] According to Article 11 of the Rulebook, the following data is specified: A. with regard to publicly available telephone service at a fixed location and publicly available telephone service in a public mobile communications network: the number from which the communication was initiated, as well as the name and surname of the individual, or the name of the legal entity, and the address of the subscriber or registered user; B. with regard to internet access, electronic mail, voice transmission services using the internet, and other forms of packet-switched exchange: the assigned user identifier or telephone number for each communication in the public electronic communications network; the name and surname of the individual, or the name of the legal entity, and the address of the subscriber or registered user to whom the IP address, user identification, or telephone number was assigned at the time of the communication; the dynamic or static IP address assigned by the service provider or access provider and the user identification of the subscriber or registered user; the identification of the digital subscriber line or other communication source point.

[12] According to Article 12 of the Rulebook, the following data is specified: A. with regard to publicly available telephone service at a fixed location and publicly available telephone service in a public mobile communications network: the dialed number (the number called), and in the case of additional services (call forwarding, call transfer, and conference call), the number to which the communication was forwarded, or the numbers involved in the conference call; the name and surname and address of the subscriber or registered user; B. with regard to internet access, electronic mail, voice transmission services using the internet, and other forms of packet-switched communication: the dynamic or static IP address assigned by the service provider or access provider and the user identification of the subscriber or registered user at the time of the communication; the user identification or telephone number of the voice transmission service counterpart; the name and surname and address of the subscriber or registered user, as well as the user identification of the communication counterpart; the identification of the digital subscriber line or other communication destination point; communication data (according to Article 2, para. 1, it. 8, this is the data representing signaling related to the targeted electronic

the start, duration, and end of the communication,[13] 4) determining the type of communication,[14] 5) identifying the user's terminal equipment,[15] and 6) determining the location of the user's mobile terminal equipment.[16]

communication service, network, or other user, including signaling used for establishing communication, controlling the flow of communication (for example, communication accepted, communication transferred), whose content and data are available to electronic communication operators (e.g., communication duration).

[13] According to Article 13 of the Rulebook, the following data are specified: A. with regard to publicly available telephone service at a fixed location and publicly available telephone service in a public mobile communications network: the date, time of the beginning, duration, and end of the communication; B. with regard to internet access, electronic mail, voice transmission services using the internet, and other forms of packet-switched communication: the date and time of logging in and out when using the access service, within the corresponding time zone, as well as the date and time of sending and receiving electronic mail and calls via the voice transmission service using the internet, within the corresponding time zone, for services provided by the operator.

[14] According to Article 14 of the Rulebook, the following data are specified: A. with regard to publicly available telephone service at a fixed location and publicly available telephone service in a public mobile communications network: data on the used telephone service; B. with regard to electronic mail, voice transmission services using the internet, and other forms of packet-switched communication: data on the used internet service.

[15] According to Article 15 of the Rulebook, the following data is specified: A. with regard to publicly available telephone service in a public mobile communications network: the IMSI number from which the communication was initiated and the IMSI number to which the communication was directed, as well as the IMEI number of the device used to initiate the communication and the IMEI number of the device to which the communication was directed; B. with regard to prepaid services for publicly available telephone service at a fixed location and publicly available telephone service in a public mobile communications network: the serial number of the card (for publicly available telephone service at a fixed location) and the serial number of the prepaid card, as well as the location from which the electronic top-up was made, if possible, for publicly available telephone service in a public mobile communications network; C. with regard to prepaid services for internet access, electronic mail, voice transmission services using the internet, and other forms of packet-switched communication: the serial number of the card; D. with regard to publicly available telephone service at a fixed location, internet access, electronic mail, voice transmission services using the internet, and other forms of packet-switched communication: the serial number of the device, MAC address, dynamic and static IP addresses assigned by the service or access provider, in the appropriate time zone, and other data that uniquely identifies the user's terminal device.

[16] The Rulebook in Article 16 does not specify which data is retained but rather imposes an obligation on operators to ensure the technical connection of their equipment with the equipment of the relevant state authorities, using an appropriate

Additionally, the LEC stipulates that the obligation of retention also includes data on established calls that were not answered, but not data on calls that failed to connect (Article 129, para. 2), nor data that the operator did not produce or process (Article 129, para. 5). The retention of data revealing the content of communications is explicitly prohibited (Article 129, para. 3).

2.2. Access to Retained Data

2.2.1. Purpose of Obtaining Access

The original LEC (2010) did not state the purpose of accessing retained data, and after Article 128 was amended in 2014, the current LEC (2023) first stipulates that access to retained data is not allowed without the user's consent, and then, as an exception, foresees such a possibility (Article 128, para. 2). Namely, access to retained data is exceptionally allowed "for a specific period and based on a court decision." At the same time, the LEC (2023) clearly defines the purpose of accessing retained data, which is necessary for conducting criminal proceedings or protecting the security of the Republic of Serbia,[17] while referring another law regarding the method.

The regulation that should govern access to retained data when necessary for criminal proceedings is the Criminal Procedure Code[18] (CPC). Article 286 CPC ("Police Powers") stipulates that if there are grounds to suspect that a criminal offense prosecutable ex officio has been committed, it is the duty of the police to take necessary measures and actions to locate the perpetrator, ensure the perpetrator or accomplice does not hide or flee, to uncover and secure traces of the criminal offense and items that may serve

technical interface through which data about all mobile terminal devices appearing at a specific geographical, physical, or logical location are transmitted, in accordance with the technical standards or capabilities of the particular mobile electronic communication technology.

[17] In the original LEC, the legislator defined the protection of national and public security of the Republic of Serbia as the purpose of retaining data (in Article 128, para. 1, before amendments). However, when formulating the amended Article 128 and determining the purpose of accessing retained data (Art. 128, para. 2), the legislator consistently followed the text of Article 41, para. 2 of the Constitution (which states "protection of the security of the Republic of Serbia").

[18] Criminal Procedure Code, *Official Gazette of the Republic of Serbia* 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 – Decision of the CC, and 62/21 – Decision of the CC.

as evidence, as well as collect any information that could be useful for the successful conduct of the criminal proceeding. In order to fulfill this duty, the police may, upon the order of the preliminary procedure judge and at the proposal of the public prosecutor, 1) obtain the records of already conducted telephone communications, 2) obtain records of the base stations used, and 3) perform location tracking of the place "from which the communication is conducted" (Article 286, para. 3).

2.2.2. Manner of Access

The operator is obliged to retain data in such a way that it can be accessed without delay, or that it can be promptly provided based on a court decision (Article 128, para. 7). By analyzing the LEC and subordinate regulations, it can be noted that the competent state authorities access retained data in two ways: a) directly – by accessing the premises, electronic communication network, associated equipment, or electronic communication equipment of the operator; or b) indirectly – by having the operators provide the requested data.[19]

A clearer answer to what this means can be found in the Rulebook. The Rulebook contains a general provision stating that all data retained in accordance with the LEC must be made available to the competent state authorities, via the appropriate technical interface, for a period of the last 12 months from the date of communication, in accordance with the law (Article 9, para. 2 of the Rulebook). Regarding location data, the Rulebook, in Articles 16 and 21, requires operators to enable technical connection of their equipment with the equipment of the competent state authorities by using the appropriate technical interface, facilitating the transfer of certain communication data.[20]

[19] The clear distinction between the two access regimes to retained data also arises from the obligation to maintain records (Art. 128, paras. 8 and 9 LEC, Article 10 of the Rulebook), as well as the obligation to create a technical interface through which the retained data is made accessible to the competent authorities, as required by the Rulebook.

[20] This applies to: a) data about all mobile terminal devices that appeared at a specific geographical, physical, or logical location, in accordance with Article 16, para. 1; b) data about the current geographical, physical, or logical location of an individual electronic communication device, in accordance with Article 21, para. 1 of the Rulebook.

2.3. Data Retention, Access to Retained Data, and the Constitution

When regulating the retention of data, one important aspect was not sufficiently and appropriately considered, namely the justification for such interference with guaranteed human rights and freedoms. The LEC generally foresees, and bylaws specifically regulate, the retention of a large amount of data, which, when accessed and processed by the competent authorities – even if done for legitimate purposes – can enable the drawing of very precise conclusions about the private life of the individuals whose data is retained. This includes their daily habits, permanent or temporary places of residence, daily or other movements, activities, social relations, and the social environments they visited. All of this can have significant and potentially comprehensive effects on both the right to privacy and data protection, as well as on the right to freedom of expression and movement.

In this regard, it is necessary to consider the alignment of the relevant provisions of the LEC and the CPC with Article 41 of the Constitution of the Republic of Serbia (Constitution),[21] which guarantees the inviolability of the secrecy of correspondence and other means of communication (para. 1),[22] and permits exceptions only for a limited time and based on a court decision, if necessary for conducting criminal proceedings or protecting the security of the Republic of Serbia, in the manner prescribed by law (para. 2).

The decision of the Constitutional Court (CC), from more than 10 years ago, emphasized that constitutional protection encompasses not only the content but also the formal characteristics of communication,[23] which means that deviation from the inviolability of communication data may be permitted only if it is in accordance with the Constitution.

By itself, the general mass retention and storage of data on all communications of all users, based on the LEC, undoubtedly represents a deviation from the guaranteed secrecy of communications and can only be allowed if the conditions prescribed by the Constitution are met. However, it

[21] Constitution of the Republic of Serbia, *Official Gazette of the Republic of Serbia* 98/06, 115/21 – amendments I-XXIX and 16/22.

[22] It is interesting to note that both the LEC and the LEC 2023 contain a rule on the confidentiality of communications. However, while Chapter XVII LEC, which contains provisions on data retention, links confidentiality only to the content of electronic communications (Art. 126), the LEC 2023 clearly recognizes both the confidentiality of the content and the confidentiality of traffic data related to electronic communications (Art. 160).

[23] Decision of the CC, p. 78.

seems that the legislator does not treat data retention as a deviation from the constitutional guarantee; it did not specify the purpose for which operators are required to retain and store data (conducting criminal proceedings or protecting the security of the Republic of Serbia). The purpose of data retention cannot be derived from the purpose of accessing retained data, as prescribed in Article 128, para. 2, because retention and access to retained data are two forms of deviation from the guaranteed rights, and each requires separate justification. Additionally, citing certain "needs" for which specific categories of data are retained, in Article 129, para. 1, is not the same as determining the purpose of data retention. Moreover, the requirements that the deviation is allowed "based on a court decision" and "for a limited period" are not considered when prescribing the obligation to retain and store data.

When regulating access to retained data, in Article 128, para. 2 LEC, the legislator consistently followed the formulation from the Constitution.[24] However, it cannot be said that the CPC, which should regulate the deviation from the guaranteed secrecy of communication for the purpose of conducting criminal proceedings, does so in a proper manner, for at least two reasons: a) deviation can only be authorized by a court decision – but a warrant is not a court decision (the CPC recognizes three types of decisions in criminal proceedings: orders, rulings, and judgments – Article 269); b) deviation is allowed only "for a limited time" – but Article 286, para. 3 CPC does not impose such a requirement.

Additionally, the authorization in Article 286, para. 3 CPC relates to the obtaining of certain retained data, specifically data on telephone communication, but not on other types of electronic communication.

[24] It is possible that the legislator, when amending Article 128, took into account the arguments from the Decision of the Constitutional Court. Namely, the Constitutional Court found that although the disputed provision (from the original Article 128, para. 1) established only a general obligation for operators to retain data and determined the purpose for which the retention is prescribed, but not the manner of using the retained data, what is controversial is that the introduction of this obligation is carried out in accordance with other relevant laws. This method establishes an obligation for operators, which may indirectly lead to a violation of the confidentiality of communication, if the retained data is not used in accordance with Article 41, para. 2 of the Constitution. This means that the data would be used without a court decision and without specifying the time frame during which it can be used, but based on resolutions from the mentioned laws. The Constitutional Court emphasized that "[t]he conditions and purpose of the allowed deviation from the confidentiality of communication are determined by the Constitution and, as such, cannot be subject to legal provisions, as the manner of exercising this right can only be prescribed by law" (Decision of the CC, p. 78, translated by author).

Accordingly, this article could not be used to gain access to all the categories and types of data that are retained based on the LEC and the Rulebook, which are not covered by it[25] – in other words, the CPC does not regulate the method of access to this data. Furthermore, a request for the delivery of such retained data, which may be directed to operators by the police or public prosecution based on the general provisions of the CPC, would be questionable from the standpoint of constitutionality.

The issue of the constitutionality of the provisions on data retention was also addressed by the Commissioner for Information of Public Importance and Personal Data Protection (Commissioner), when, more than a decade ago, they conducted oversight of the implementation of the Personal Data Protection Act[26] (PDPA) by the operators of mobile and fixed telephony in the Republic of Serbia (Commissioner 2012).[27] Based on the results of this oversight, the Commissioner and the Ombudsman prepared a Proposal of Recommendations for improving the situation in this area, containing 14 items. Our analysis cannot state with certainty that these recommendations have been fully and adequately applied to this day. The situation is similar when it comes to electronic communications operators providing internet access and internet services (Commissioner 2015).

In addition to the alignment of the legal framework on data retention and access to retained data with the Constitution being questionable, its compliance with EU law and the ECHR is uncertain, due to the failure to take into account the human rights protection standards established in the CJEU's and ECtHR's case law.

---

[25] For example, Article 286, para. 3 CPC could not be used for obtaining data about a dynamic or static IP address assigned by the service provider or access provider, which is retained under Article 12 of the Regulation, or data about the date, time of login and logout during the use of access services, within the appropriate time zone, as well as the date and time of sending and receiving emails and calls via the internet voice service, within the appropriate time zone, for services provided by the operator, which is retained under Article 13 of the Regulation – even if the court issues an order to obtain such data.

[26] Personal Data Protection Act, *Official Gazette of the Republic of Serbia* 87/18.

[27] The subject of the oversight was access to retained communication data, and based on the established facts during the oversight, it was concluded that the processing of this data, individually and especially when considered together, over a period of 12 months, constitutes a serious intrusion into the privacy of citizens. It was found that this violates the constitutional guarantee of the inviolability of communication secrecy, as well as the provision that deviations are allowed only for a specific time and based on a court decision, for the purpose of conducting criminal procedure or protecting national security.

3. STANDARDS OF HUMAN RIGHTS PROTECTION

3.1. The CJEU Case Law

Although Directive 2006/24/EC was repealed more than a decade ago because it broadly and especially severely interfered with fundamental human rights, and such interference was not precisely limited to what was strictly necessary,[28] communication data is still retained in EU member states, and national regulations and the actions of competent authorities in several countries have been subject to review by the CJEU.[29] The decisions in the *SpaceNet AG*,[30] *Tele2 Sverige*,[31] *La Quadrature du Net*,[32] *Privacy International*,[33] and *Prokuratuur*[34] cases were analyzed in order to determine the position of the CJEU on data retention and access to retained data by competent authorities in member states.

3.1.1. Data Retention

The CJEU particularly addressed the purpose of data retention in its decision in the *SpaceNet AG* case. First and foremost, regarding the justification for restricting rights, the Court held that the objectives outlined in the first sentence of Article 15, para. 1 of Directive 2002/58/EC[35] are exhaustively listed. Consequently, any legislative measure adopted under this

[28] CJEU, joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238, 8 April 2014.

[29] For more on this, see Podkowik, Rybski, Zubik 2021, 1608–1609.

[30] CJEU, joined cases C-793/19 and C-794/19, *SpaceNet AG*, ECLI:EU:C:2022:854, 27 October 2022.

[31] CJEU, joined cases C-203/15 and C-698/15, *Tele2 Sverige*, ECLI:EU:C:2016:970, 21 December 2016.

[32] CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, ECLI:EU:C:2020:791, 6 October 2020.

[33] CJEU, case C-623/17, *Privacy International*, ECLI:EU:C:2020:790, 6 October 2020.

[34] CJEU, case C-746/18, *Prokuratuur*, ECLI:EU:C:2021:152, 2 March 2021.

[35] 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), OJ L 201/37 of 12/07/2002.; 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

provision must effectively and strictly correspond to one of these objectives. The existence of potential difficulties in precisely determining the cases and conditions under which targeted retention should be implemented cannot justify a member state prescribing general and indiscriminate retention of traffic and location data in such a way that an exception becomes the rule.[36] Namely, the CJEU has taken a clear stance that national legislation providing for data retention must meet objective criteria, establishing a link between the data to be retained and the objective being pursued. The Court found that, according to its case law and the principle of proportionality, there is a hierarchy among these objectives, based on their importance. The significance of the objective sought by such a measure must be proportionate to the severity of the interference, with the guaranteed rights resulting from it. Accordingly, the Court emphasized that EU law is opposed to national legislation which, for the purpose of combating serious crime, provides as a rule for general and indiscriminate retention of traffic and location data, as it exceeds what is strictly necessary and cannot be considered justified in a democratic society. It is highlighted that crimes, even particularly serious ones, cannot be equated with a threat to national security. Such an equivalence would create an intermediate category between national and public security, allowing for the requirements specific to the former[37] to be applied to the latter. This is neither justified nor permissible.

The CJEU has provided member states with clear guidelines on how to regulate data retention in their national laws in a manner consistent with EU law. In its decision in the *Tele2 Sverige* case, the Court left member states the option to provide for targeted retention of traffic and location data in their national legislation, for the purpose of combating crime. However, this must be subject to appropriate authorization and effective oversight during the implementation of such measures, which should be conducted by a court or an independent body, while respecting the principles of time limitation and necessity, and ensuring that the retention is strictly required for a specifically determined and justified purpose.[38] Furthermore, in its decision

communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337/11, of 18/12/2009.

36 *SpaceNet AG*, paras. 104–113.

37 *SpaceNet AG*, paras. 70–74, 92–94 and 117–124.

38 *Tele2 Sverige*, paras. 108–112, 116–125. It should also be noted that in this decision, the CJEU expressed the view that when it comes to the objectives that may justify a national regulation that deviates from the principle of confidentiality of electronic communications, it should be noted that, as established in paras. 90 and 102 of this judgment, the enumeration of objectives in the first sentence

in the *La Quadrature du Net* case, the CJEU provided guidance on certain forms of data retention. It held that specific measures are not contrary to EU law, provided that they are prescribed by clear and precise legal rules, particularly if certain substantive and formal conditions are met. Notably, affected individuals must have access to effective safeguards against risks and the possibility of misuse.[39]

---

of Article 15(1) of Directive 2002/58 is exhaustive, and access to retained data must effectively and strictly fulfill one of those objectives. Furthermore, since the aim of this regulation must be linked to the seriousness of the interference with fundamental rights caused by that access, it follows that in the area of preventing, investigating, detecting, and prosecuting criminal offenses, only the fight against serious crimes can justify such access to retained data (see *Tele2 Sverige*, para. 115).

[39] These are measures that allow for: a) general and indiscriminate retention of traffic and location data for the purpose of protecting national security in situations where the member state concerned is faced with a serious threat to national security that is real and present (imminent) or foreseeable, if the decision providing for the retention of data is subject to effective review by a court or an independent administrative body, the decision of which has a binding character, which seeks to verify whether one of those situations exists and whether the conditions and guarantees that must be provided for are respected, and if the said decision may be issued only for a period limited in time to what is strictly necessary, but may be extended in the event of the persistence of that threat, b) targeted retention of traffic and location data for the purpose of protecting national security, combating serious crime and preventing serious threats to public security, which is limited on the basis of objective and nondiscriminatory criteria, depending on the category of persons concerned or by means of a geolocation criterion, and which is determined for a period limited in time to what is strictly necessary, but which may be extended; c) general and indiscriminate retention of IP addresses assigned to the source of the connection for a period limited in time to what is strictly necessary, for the purpose of protecting national security, combating serious crime and preventing serious threats to public security; d) general and indiscriminate retention of data on the civil identity of users of electronic communication means for the purpose of protecting national security, combating crime and protecting public security; e) urgent retention of traffic and location data for a limited period of time held by those service providers for the purpose of combating serious crime and protecting national security, based on a decision of a competent authority subject to effective judicial review, respecting the limits of what is strictly necessary; f) the automatic analysis and real-time collection of traffic and location data in the event that it is limited to situations in which the State is faced with a serious threat to national security that has proven to be real and present (imminent) or foreseeable, if the use of such analysis can be subject to effective supervision by a court or an independent administrative body whose decision has a binding character, which seeks to verify whether there is a situation justifying the said measure and whether the conditions and guarantees that must be foreseen are respected, and g) the real-time collection of technical data on the location of the terminal equipment used, if it is limited to persons in relation to whom there are reasonable and clear grounds for suspecting that they are involved in any way in terrorist activities, and is subject to prior supervision by a court or an independent administrative body whose decision has

3.1.2. Access to Retained Data

In its decision in the *Privacy International* case, the CJEU concluded that EU law is opposed to national legislation allowing a state authority to require providers of electronic communication services to engage in general and indiscriminate transmission of traffic and location data for the purpose of protecting national security. Such a measure exceeds the limits of what is strictly necessary and cannot be considered justified in a democratic society.

Even in cases of specific threats to national security, the Court emphasized that the regulation must not merely stipulate that a request for access to retained data aligns with achieving the stated objective. Instead, it must prescribe substantive and formal conditions governing access to data, based on objective criteria, to define the circumstances and conditions under which the competent authorities may be granted access. Special attention must be paid to whether there is a connection between the data to be transmitted and the threat to national security, as well as whether there is a clear link between the individuals whose retained data would be accessed and the specific threat to national security.[40] This requirement applies even more strongly when access to retained data is granted for the purposes of criminal proceedings.

Furthermore, in its decision in the *Prokuratuur* case, the CJEU took the position that only the objectives of combating serious crimes or preventing serious threats to public safety can justify granting state authorities access to a set of traffic or location data. Such data may provide information about communications conducted by a user via electronic communication devices or the location of terminal equipment used, which could allow for precise conclusions to be drawn about the private lives of the individuals concerned. Other factors cannot justify such access for the purposes of preventing, investigating, or detecting crimes in general.[41] Additionally, in light of the

a binding character, in order to ensure that such real-time collection is authorized only within the limits of what is strictly necessary (*La Quadrature du Net*, paras. 168, 192). For more on this issue, see Bugarski, Pisarić 2020.

[40] *Privacy International*, paras. 74–82.

[41] In this regard, the CJEU has stated that even access to a limited amount of data or access to data from a short period of time may provide precise information about the private life of the user of the means of electronic communication. This is because the amount of data available and the specific information about the private life of the person concerned that emerges from them are circumstances that can be assessed only after access to that data. However, the authorization of a court or a competent independent authority must be given before access to the data and the information that emerges from it can be granted, so that the assessment of the seriousness of the interference that access entails is carried out in the light of the risk generally

goal of combating serious crime, access may, in principle, only be granted in relation to the data of individuals for whom there is a clear suspicion that they intend to commit, are committing, or have committed a serious crime, or have otherwise participated in such an offense.[42] To ensure full compliance with these conditions in practice, it is essential that judicial or independent oversight be conducted before the national authorities access retained data, based on a substantiated request as part of a criminal proceeding. The requirement of independence, which must be met by the body responsible for conducting prior oversight, mandates that the body act as a third party in relation to the authority requesting access to the data. This ensures that it can perform oversight objectively, impartially, and without external influence. Specifically, the requirement of independence in criminal proceedings means that the body responsible for such prior oversight must, on the one hand, not be involved in conducting the criminal investigation in question and, on the other hand, maintain a neutral position in relation to the parties in the criminal proceeding. It must have a status capable of ensuring a fair balance between, on the one hand, the interests associated with the investigative needs of crime-fighting and, on the other hand, the fundamental rights to respect for private life and the protection of personal data of the individuals whose data is accessed.

In conclusion, the CJEU stated that the public prosecutor's office, as a state body responsible for conducting investigations and, where applicable, representing the prosecution, cannot fulfill these criteria. Consequently, the public prosecutor's office is not in a position to conduct prior oversight regarding the application of measures for accessing retained data.[43] In cases of justified urgency, subsequent oversight may be carried out, provided it follows shortly after the access to data has been granted.[44]

---

inherent in the category of data sought for the private life of the persons concerned, without it being important to know whether the information about the private life that emerges from it is sensitive in a particular case (*Prokuratuur*, paras. 35–45).

[42] However, in special circumstances, such as those in which terrorist activities pose a threat to essential national security, defense or public safety interests, access to data of other persons may be authorized, in cases where there are objective elements allowing the conclusion that the data in the specific case can make a real and unequivocal contribution to the fight against such activities (*Prokuratuur*, paras. 49–58).

[43] *Prokuratuur*, paras. 51–59. For more on the application of the principle of proportionality and independence of authorities regarding access to retained data, see Rovelli 2021.

[44] Regarding the question of whether the absence of prior supervision by an independent authority can be compensated for by subsequent judicial supervision of the lawfulness of access to retained data, the CJEU has pointed out that subsequent

3.2. The ECtHR's case law

To examine the compliance of domestic legal frameworks with the ECHR, the judgments of the ECtHR in the cases of *Ekimdzhiev and Others v. Bulgaria*,[45] *Škoberne v. Slovenia*,[46] and *Podchasov v. Russia*,[47] were analyzed. These cases involved complaints where applicants claimed that the retention of communication data by service providers and access to that data by competent authorities violated their rights under Article 8 of the ECHR.

3.2.1. Ekimdzhiev and Others v. Bulgaria

In the *Ekimdzhiev and Oothers v. Bulgaria* case, the ECtHR determined that, under Bulgarian law, all communication service providers are required to retain and store all subscriber, traffic, and location data of all users for six months after the end of communication, with the aim of making such data available to various competent authorities for specific purposes. Since providers are required to retain data that can, individually or in combination with other data, relate to "private life", such legally mandated retention constitutes an interference with the right to respect for private life and correspondence, regardless of whether competent authorities subsequently access the retained data.[48] Such interference is attributable to the Bulgarian state, even though it is carried out by private entities, as they are obliged by law.[49] The ECtHR further found that Bulgarian authorities may access retained communication data if it is necessary to achieve one or more legally defined purposes. In the Court's view, since any individual's communication

supervision does not enable the objective of prior supervision, which consists in preventing access to the data in question from being granted in cases that exceed the limits of what is strictly necessary (*Prokuratuur*, paras. 49–58).

45 ECtHR, *Ekimdzhiev and Others v. Bulgaria* (Application No. 70078/12), 11 January 2022.

46 ECtHR, *Škoberne v. Slovenia* (Application No. 19920/20), 15 February 2024.

47 ECtHR, *Podchasov v. Russia* (Application No. 33696/19), 13 February 2024.

48 *Ekimdzhiev and Others v. Bulgaria*, para. 372.

49 *Ekimdzhiev and Others v. Bulgaria*, para. 375. The ECtHR took an identical position in *Podchasov v. Russia* concerning the legal obligation of an internet communications service provider to retain all communications data for one year and the content of all communications for six months, and to provide access to and provide them to law enforcement or security services, in circumstances specified by law, together with the information necessary to decrypt electronic messages if they are encrypted (paras. 50–52); and in *Škoberne v. Slovenia*, which concerned the obligation of telecommunications service providers to retain and store traffic and location data relating to fixed and mobile telephony of all users

data could theoretically become necessary for one or more of these purposes, the applicants could also be affected by the contested legislation. Therefore, the Court concluded that access by competent authorities to retained communication data constitutes further interference with the right under Article 8 ECHR.[50] Regarding the justification for this interference, the ECtHR emphasized that the retention of communication data by service providers and subsequent access by state authorities in individual cases must be accompanied, *mutatis mutandis*, by the same safeguards as those required for the secret surveillance of communications.[51]

Although Bulgarian law prescribes certain safeguards aimed at ensuring that competent authorities access retained communication data only when justified (as prior court approval is required), the ECtHR concluded that this falls below the required standard of effective protection.[52] As for the

of telecommunications services for a period of 14 months and to provide it to competent authorities upon request, for certain law enforcement purposes, with various authorities being able to access such data (paras. 125–128).

50 *Ekimdzhiev and Others v. Bulgaria*, para. 376.

51 The Court pointed out that, given the technological and social developments in the field of electronic communications over the past two decades, communications data can reveal a large amount of personal data and, if collected en masse by the competent authorities, can be used to create an intimate picture of a person, through social network mapping, location tracking, internet browsing, mapping of communication patterns, insight into who the person has communicated with and when, etc. The collection of such data through mass and general retention and access to the retained data can therefore be as intrusive as the mass collection of the content of communications, which is why their interception, retention and use by the competent authorities should be analyzed in the context of the protection measures relating to the content of the communications (*Ekimdzhiev and Others v. Bulgaria*, paras. 394–395).

52 The Court found that requests for access submitted outside the framework of criminal proceedings already initiated must state the grounds and purpose for which access to the retained data is sought, as well as a full account of the circumstances showing that the data is necessary for a specific and relevant purpose. In contrast, although requests for access related to criminal proceedings should contain information on the alleged criminal offence for which access is sought, the competent authorities are not expressly required to explain in the request why the data is actually necessary (it need only contain a description of the circumstances underlying the request), nor to disclose to the judge "fully and honestly" all issues relevant for the assessment of the merits of the request for access, including issues that may "weaken" the justification of the request, nor to provide supporting materials – which may prevent the judge from properly assessing whether the request for access is valid. Furthermore, the law does not oblige the judge examining the request for access to state in the decision granting access the reasons explaining why they decided that the granting was indeed necessary and proportionate, or that less invasive measures could not have achieved the same purpose (*Ekimdzhiev and Others v. Bulgaria*, paras. 400–407).

"fate" of the retained data accessed by competent authorities, the ECtHR found that such data is simply stored in criminal case files, follows the fate of those files, and can be accessed by anyone with access to the file itself. This fails to provide an adequate level of data protection, as there are no provisions adequately regulating the storage, access, review, use, disclosure, and destruction of the data.[53] Regarding the notification of individuals whose retained data was accessed, the ECtHR found that the prescribed notification is inconsistent with established case law,[54] as notification is required in all cases, not only when the data was accessed unlawfully, and should occur as soon as possible without jeopardizing the purpose of the measure.[55] Furthermore, the ECtHR established that neither the Bulgarian Electronic Communications Act nor the Criminal Procedure Code provides a legal remedy concerning the retention or access to communication data.[56]

---

[53] The relevant Bulgarian legislation provides that all communications data not used for the initiation of criminal proceedings must be destroyed within three months of receipt by the competent authorities, and that all data accessed under an urgent procedure must be destroyed immediately in the same manner, unless such access has been retrospectively confirmed by the competent judge. By contrast, no such time limit is defined for accessed data in cases where criminal proceedings have been initiated. The ECtHR noted that, although this issue appears to be covered by internal rules issued by the Chief Prosecutor, those rules have not been made publicly available, and it is unclear what they provide. Furthermore, there is nothing to suggest that the provisions of the relevant law transposing Directive (EU) 2016/680 have so far been used to fill this gap (*Ekimdzhiev and Others v. Bulgaria*, paras. 408–409).

[54] Although the Bulgarian Law on Electronic Communications requires a special parliamentary committee to notify an individual in the event that their retained communications data has been unlawfully accessed or access has been unlawfully requested, provided that such notification would not undermine the purpose for which the data was accessed – the ECtHR found such a solution unsatisfactory.

[55] The Court found that there was no indication that such notification system had been made so far on the basis of the amendments to the law transposing Directive (EU) 2016/680, which provided for the possibility for individuals to obtain such information in relation to retained and accessed communications data, nor did it appear that there had been any cases in which individuals had been able to obtain information on the retention or access to their communications data in accordance with the relevant provisions of that law. In the absence of further details, it cannot be accepted that the data protection provisions related to retained communications data are effective in that regard (*Ekimdzhiev and Others v. Bulgaria*, paras. 416–417).

[56] Also, for the newly introduced remedies, in the absence of reported decisions of Bulgarian courts, it was pointed out that, due to the lack of details on the "actual functioning" of the system of remedies related to communications data, it cannot be accepted that they are currently effective, nor is there any evidence that a remedy is available. It follows that public concerns regarding the threat of misuse of access to and use of communications data by state authorities cannot be sufficiently

Finally, in terms of oversight of access to retained data, the ECtHR concluded that existing mechanisms are inadequate to ensure that the power to access data is not abused.[57]

3.2.2. Škoberne v. Slovenia

In the *Škoberne v. Slovenia* case, the ECtHR determined that the (amended) Slovenian Law on Electronic Communications from 2004 specified various purposes for which communication data was to be retained. However, it did not include provisions limiting the scope and application of this measure solely to what was necessary for achieving those purposes, and the state failed to demonstrate that another legislative act contained such provisions. The ECtHR first emphasized that, based on established case law, as part of minimum requirements and in a manner appropriate to the specific surveillance measure, the national law must define the scope of application of the surveillance measure and ensure appropriate procedures

addressed by the present effective remedies in this regard. Namely, it is up to the State to explain that the effectiveness of the remedies it claims to be effective has been ensured and to substantiate the explanations provided, as far as possible, with concrete examples, which was lacking in the case of Bulgaria (*Ekimdzhiev and Others v. Bulgaria*, paras. 376–382).

[57] Namely, the Personal Data Protection Commission is competent to supervise the conduct of communication service providers, but it has no explicit powers in relation to the state authorities that may access retained data. However, through the relevant amendments to the legislation transposing Directive (EU) 2016/680, the Commission and the Inspectorate of the Supreme Judicial Council are tasked with supervising the manner in which state authorities process personal data for law enforcement purposes; there is nothing to suggest that these bodies have so far used these powers in relation to retained communication data. Also, the judge who grants access to retained data is not in a position to ensure effective control, because, although the competent authorities provide them with a report on the implemented measure, they have no authority to supervise or order corrective measures, are not authorized or expected to conduct on-site inspections, and perform their supervisory duties solely on the basis of reports from the competent authorities. Furthermore, although the main oversight body (a special parliamentary committee) can supervise both communication service providers and competent authorities, and has broad powers of information gathering and supervision, and annual reports show that it regularly carries out inspections through officials it employs. The shortcoming is that its members do not have to be persons with legal qualifications or experience in this field, and the committee has no power to order corrective measures in specific cases, but can only issue instructions designed to improve the relevant procedures, and if it discovers irregularities, it can only draw the attention of the competent authorities or inform the heads of the relevant authorities and communication service providers (*Ekimdzhiev and Others v. Bulgaria*, paras. 410–415).

for authorization and/or review, aimed at keeping the measure within the necessary limits. In this context, the minimum requirements also applied to the retention of communication data, considering the nature of the contested interference. The ECtHR highlighted that the clarity of a law prescribing the general and indiscriminate retention of communication data cannot in itself be considered sufficient to ensure compliance with the principles of the rule of law and proportionality. The absence of provisions or mechanisms ensuring that the measure is genuinely restricted to what is "necessary in a democratic society" for specific purposes set forth in the (amended) 2004 Act, along with the requirement to retain the data for a period of fourteen months, rendered such a regime incompatible with the state's obligations under Article 8 ECHR.[58]

To support its findings, the ECtHR referred to the case law of the CJEU and noted that a regime of mandatory, general, and indiscriminate retention of communication data for combating serious crime is inconsistent with the requirement of proportionality. Such retention cannot be systemic in nature and must be subject to independent oversight in specific cases, even in the context of protecting national security, where data retention could be mandated as a general and indiscriminate measure under strict conditions.[59]

When considering the use of data collected under such a retention regime, the ECtHR observed that, even though the CJEU and the Slovenian Constitutional Court had invalidated the retention regime, the relevant factors for assessing compliance with Article 8 ECHR in the specific case was the moment when the data was retained and accessed (prior to the invalidation of the regime) and whether the applicant had adequate legal protection at that time under the Convention – which the Court found was not the case. Furthermore, the ECtHR underlined that, although the applicant's data access was accompanied by certain safeguards (i.e., judicial approval), those safeguards alone were insufficient to render the retention regime compliant with Article 8 ECHR.[60]

---

58 *Škoberne v. Slovenia*, paras. 138–139.

59 *Škoberne v. Slovenia*, paras. 140, 68.

60 *Škoberne v. Slovenia*, paras. 142–143. Furthermore, the ECtHR noted that the CJEU had similarly found, in the *SpaceNet* and *Telekom Deutschland* cases, that national legislation, which ensured full compliance with the conditions laid down by the law implementing Directive 2006/24/EC concerning access to retained data, by its very nature could not limit or even remedy the serious interferences resulting from the general retention of data – the retention and access to such data being separate interferences requiring specific justifications (*Škoberne v. Slovenia*, para. 87).

In conclusion, the ECtHR stated that, irrespective of the amount of data retained, what matters under Article 8 ECHR is that the data was retained under a general and indiscriminate regime that was found to be in violation of Article 8 ECHR.[61] In other words, when the retention of communication data is determined to breach Article 8 ECHR due to noncompliance with the "quality of law" requirement and/or the principle of proportionality, the same applies to the access to and the subsequent processing of the retained data by state authorities.[62]

3.2.3. Podchasov v. Russia

In its decision in the *Podchasov v. Russia* case, the ECtHR found, among other things, that the mere existence of a law requiring the continuous and automatic retention and storage of all internet communication data and related metadata by electronic communication providers, as well as the storage of the content of all internet communication services (used for transmitting voice, text, visual, audio, video, or other electronic communications), along with the potential access by authorities to such data and the obligation for the Telegram instant messaging and social media platform to decrypt encrypted data, constituted an exceptionally serious and unacceptable interference with the applicant's rights under Article 8 ECHR. The Court emphasized that this practice effectively impacts all users of internet communications, particularly in situations where there is no reasonable suspicion of their involvement in criminal activities or activities threatening national security, nor any other reason to believe that data retention might contribute to combating serious crime or protecting national

[61] The Court stated that it was not of any particular significance that, in convicting the applicant, the domestic courts had used a limited amount of retained data relating to a (limited) period of one month, since the application concerned a whole range of data retained and stored over a period of fourteen months, which had been obtained by the competent authorities and then processed, stored and examined for the purposes of the criminal proceedings in question (*Škoberne v. Slovenia*, paras. 145, 147).

[62] *Škoberne v. Slovenia*, para. 144. In this regard, the ECtHR referred to the position expressed by the CJEU in the *An Garda Siochana* case, where the CJEU found that communications data cannot be subject to general and indiscriminate retention for the purpose of combating serious crime and that access to such data therefore cannot be justified for that same purpose, and accordingly the ECtHR sees no reason to find otherwise in the applicant's case.

security.[63] Such a broadly prescribed obligation to retain data, without any limitations in terms of territorial or temporal scope or the categories of individuals whose personal data is retained and stored, significantly infringes upon rights protected under Article 8 ECHR.[64]

Moreover, the ECtHR highlighted as particularly invasive the obligation imposed on electronic communication service providers to install equipment providing authorities direct remote access to all retained internet communication data, as well as to the content of the communications. This allows authorities to bypass authorization procedures and access the retained communication data and content without prior judicial approval. According to the ECtHR, such a practice is unacceptable, given that requiring judicial approval before a service provider grants access to retained data constitutes an essential safeguard against abuse by authorities. The absence of such judicial oversight significantly increases the risk of arbitrariness and the likelihood of abuse, thus failing to meet the minimum requirements for protective measures.[65]

---

[63] It has been pointed out that the protection provided for in Article 8 of the ECHR would be unacceptably weakened if the use of modern technologies were permitted in the criminal justice system at any cost and without a careful balancing of the potential benefits of the extensive use of such technologies against the important interests of protecting private life, i.e., protecting personal data (*Podchasov v. Russia*, para. 62).

[64] *Podchasov v. Russia*, para. 70.

[65] *Podchasov v. Russia*, paras. 72–75. It is also important to note that in the same decision, regarding the requirement to provide security services with the information necessary to decrypt encrypted electronic communications, the ECtHR notes that encryption provides strong technical guarantees against unlawful access to the content of communications and is therefore widely used as a means of protecting the right to respect for private life and the privacy of online correspondence. In the digital age, technical solutions for securing and protecting the privacy of electronic communications, including encryption measures, contribute to ensuring the enjoyment of other fundamental rights, such as freedom of expression. Moreover, encryption appears to help citizens and businesses defend themselves against misuse of information technologies, such as hacking, identity and personal data theft, fraud and inappropriate disclosure of confidential information. In accordance with the abovementioned, the ECtHR takes into account the dangers of limiting encryption described by many experts in this field, bearing in mind that it would be necessary to weaken the encryption for everyone in order to enable the decryption of communications protected by end-to-end encryption. The measures therefore cannot be limited to certain individuals and would indiscriminately affect everyone, including individuals who do not pose a threat to a legitimate government interest. Weakening the encryption by creating a backdoor would clearly make it technically possible to carry out routine, general and indiscriminate surveillance of personal electronic communications, but criminal networks could also exploit the backdoor and seriously undermine the security of electronic communications of all users. The

4. COMPLIANCE OF THE SERBIAN LEGAL FRAMEWORK WITH HUMAN RIGHTS PROTECTION STANDARDS

Certain positions expressed by the CJEU and the ECtHR in the decisions of the aforementioned cases are potentially applicable to the Serbian legal framework.

4.1. Compliance with EU Law

The Serbian LEC of 2010 was modeled after Directive 2006/24/EC, with certain provisions directly translated and incorporated into the law, adopted uncritically and without the necessary legislative adjustments (considering the legal nature of directives). Subsequent legislative interventions failed to take into account the views of the CJEU, clearly expressed in the decision annulling Directive 2006/24/EC,[66] as well as the positions outlined in several rulings concerning national regulations,[67] which was also not addressed during the adoption of the new law in 2023.

Regarding data retention, the arguments that led to the annulment of Directive 2006/24/EC – specifically its broad and particularly severe interference with fundamental human rights, without such interference being precisely limited to what is strictly necessary – can easily also be applied to Serbian law.[68] The CJEU deemed national legislation that mandates the general and indiscriminate retention of all traffic and location data for all users of electronic communication services to be impermissible and excessive, in its 2016 decision in *Tele2 Sverige*. This position was further reaffirmed in decisions such as in the *La Quadrature du Net* case in 2020 and the *SpaceNet AG* case in 2022. Accordingly, it is not difficult to conclude whether the LEC, which prescribes the obligation for general and indiscriminate retention of electronic communication data without specifying the purpose for which such data is retained, aligns with EU law. In this regard, it is essential to note

Court accordingly concluded that the legal obligation of internet communication providers to decrypt end-to-end encrypted communications poses a risk that providers of such services would weaken the encryption mechanism for all users and that the existence of such an obligation cannot be considered proportionate and legitimate (*Podchasov v. Russia*, paras. 76–79).

66 For more on this, see Pisarić (2019, 187–188).

67 For more on this, see Mitsilegas *et al.* (2023, 182–183).

68 See especially paras. 25–29, as well as paras. 54–69.

that the CJEU has taken a clear stance that both data retention and access to retained data constitute separate interferences with guaranteed rights, each requiring specific justifications.

In this regard, and concerning access to retained data for the purposes of criminal proceedings, it is questionable whether and to what extent the provisions of the CPC meet the requirements established in the case law of the CJEU. The purpose of granting access is derived from Article 286, para. 3 CPC, which states that the police are authorized to access retained data "for the purpose of fulfilling the duty referred to in paragraph 1 of this Article."[69] Such a formulation cannot be said to define the purpose of access in a specific case with sufficient precision, as it is insufficient to merely prescribe that the police may access retained data to achieve a certain goal (i.e., duties outlined in Article 286, para. 1).[70] Although the CPC prescribes conditions for accessing retained data – both material ("If there are grounds for suspicion that a criminal offence which is prosecutable ex officio has been committed") and formal (that the public prosecutor has submitted a request and the pre-trial judge has approved the collection of data by order) – the case law of the CJEU unequivocally indicates that these conditions must be based on objective criteria that more precisely define the circumstances under which access may be granted to the competent authorities in a particular case, which the CPC fails to provide. Regarding the material condition that there must be the lowest level of suspicion that any criminal offense prosecutable ex officio has been committed, it should be noted that the CJEU has taken the position that a regime of general and indiscriminate transfer of retained data to competent authorities, even for the purpose of combating serious crime, does not comply with the requirement of legal quality and/or proportionality. This applies even more strongly to access to retained data for the general purpose of combating crime, as provided for by the CPC. Furthermore, the measure under Article 286, para. 3 CPC can be applied to any individual (including those for whom there is no indication that their behavior might have any connection, even indirect or remote, to the objective of conducting criminal proceedings). The CJEU has emphasized that access should be granted only for data related to individuals for whom there is clear suspicion that they have committed a serious criminal offense,

[69] That is, "to locate the perpetrator of the criminal offence, for the perpetrator or accomplice not to go into hiding or abscond, to detect and secure traces of the criminal offence and objects which may serve as evidence, as well as to collect all information which could be of benefit for the successful conduct of criminal proceedings."

[70] See *Privacy International*, paras 74–81.

while access to the data of other individuals should only be permitted under restrictive conditions.[71] Regarding the formal condition, the case law of the CJEU suggests that particular attention should be paid to whether a connection exists between the data requested and the criminal offense, as well as whether there is a clear link between the individuals whose retained data would be accessed and the specific criminal proceedings,[72] which should be justified both in the request made by the competent authority for access and in the court's decision granting access in a specific case,[73] while the CPC does not impose such a requirement regarding either the proposal or the order.

Furthermore, it appears that Serbia has not yet considered the possibility of regulating targeted data retention and access to such data, as suggested in the decisions of the CJEU, which provide clear guidelines and criteria for a more balanced approach to resolving the relationship between protecting the public interest and interfering with fundamental human rights (for example, as determined in the *La Quadrature du Net* case). Given all of the above, and following the analysis of the relevant case law of the CJEU, it cannot be asserted that Serbia's national regulations are aligned with EU law. As a candidate country for EU membership, Serbia should take into account the positions and guidelines established in the rulings of the Union's highest court. The gravity of the (in)adequacy of the legislative solutions is further evaluated through the (non)alignment with the case law of the ECtHR.

4.2. Compliance With the ECHR

Based on the case law of the ECtHR, it could be stated that all users of electronic communication services in Serbia are victims of interference with their rights under Article 8 ECHR, due to the way regulations obligate operators to retain and store a large amount of data about the electronic communications of all their users (regardless of whether competent authorities later access it), and regulate access to retained data by competent authorities for the purposes of criminal proceedings.[74]

---

71 See *Prokuratuur*, paras. 49–58.

72 See *Privacy International*, paras. 74–81.

73 For more on this, see 4.2.1.

74 See *Ekimdzhiev and Others v. Bulgaria*, paras. 372, 376; *Podchasov v. Russia*, paras. 50–52; *Škoberne v. Slovenia*, paras. 125–128.

Furthermore, since the purpose of data retention is not defined in the LEC, and there are no provisions limiting the scope and application of retention to what is necessary to achieve the purpose (instead there is a general and nonselective data retention regime), it could be concluded that such retention is in violation of Article 8 ECHR, as it does not respect the "quality of law" requirement and/or the principle of proportionality. The same would apply to access to retained data and its subsequent processing by competent state authorities for the purposes of criminal proceedings, as regulated in the CPC.[75]

Regarding the justification of such interference with the right under Article 8 ECHR, we will analyze: the provisions of the LEC, as the regulation governing data retention and access to retained data in general; the provisions of the CPC, as the regulation governing access to retained data for criminal proceedings; and the provisions of other regulations. The analysis will be conducted in light of the ECtHR's stance that, considering the importance of communication data, retention by service providers and subsequent access by state authorities in individual cases must be accompanied by the same protective measures as secret surveillance of communications.[76]

4.2.1. Request/Decision

In terms of prior authorization for access to retained data, as a protective measure that should ensure that competent authorities access retained communication data only when justified, the question arises whether the CPC regulates this issue adequately. The CPC does not stipulate what should be contained in the public prosecutor's proposal, as a request for authorization of access by the competent authority, or the judge's order for preliminary proceedings, as a decision granting access.[77] It does not require the provision of any reasoning at all, let alone showing that the condition that less intrusive measures could not achieve the same purpose has been

[75] See *Škoberne v. Slovenia*, para. 144.

[76] See *Ekimdzhiev and Others v. Bulgaria*, paras. 394–395; *Podchasov v. Russia*, para. 72; *Škoberne v. Slovenia*, paras. 119, 133–134, 137.

[77] According to the existing legal solution, it would be sufficient for the request to contain a statement that there are grounds for suspicion that a certain criminal offense has been committed and that access to the retained data is necessary in order to locate the perpetrator of the criminal offense, to prevent the perpetrator or accomplice from going into hiding or absconding, to discover and secure traces of the criminal offense and objects that can serve as evidence, or to collect all the information that could be useful for the successful conduct of criminal proceedings.

met. This implies that the procedure for authorizing competent authorities to access retained communication data does not effectively guarantee that such access will be authorized only when it is truly necessary and proportional in the specific case.[78] Based on the above, it could be said that Article 286, para. 3 CPC does not meet the quality of law standard in relation to access to retained data, as established in the practice of the ECtHR.

Also, since the ECtHR has reacted negatively to the requirement for electronic communication providers to install equipment that allows competent authorities direct, remote access to retained data, it is necessary to consider domestic regulations. Although the LEC clearly states that a judicial decision is a necessary precondition for both methods of obtaining retained data (Article 128, para. 7 LEC), the obligations of operators concerning the technical interface need to be examined carefully.[79] Furthermore, although the data pertaining to the judicial decision that serves as the basis for accessing retained data is entered into the records maintained by operators and the competent authorities that access the retained data (Articles 128, paras. 8–9 LEC), their obligation to keep these records confidential, in accordance with the Data Secrecy Law[80] (DSL), does not eliminate the potential suspicion that competent authorities could effectively bypass the authorization procedure and access the retained data directly, without prior judicial approval.[81]

4.2.2. Notification of Individuals

Regarding the notification of individuals whose retained data has been accessed by the authorities, the ECtHR emphasized that notification is required in all cases as soon as it can be carried out without jeopardizing the purpose for which the measure was taken.[82] However, in Serbia, individuals

[78] See *Ekimdzhiev and Others v. Bulgaria*, paras. 400–407; *Škoberne v. Slovenia*, paras. 142–143.

[79] Operators are obliged to make the retained data available via an appropriate technical interface (Art. 9, para. 2 of the Regulation), i.e., to enable the technical connection of their equipment with the equipment of the competent state authorities by using an appropriate technical interface that enables the transfer of certain communication data (Arts. 16 and 21 of the Regulation).

[80] Data Secrecy Law, *Official Gazette of the Republic of Serbia* 104/09.

[81] See *Podchasov v. Russia*, paras. 72–75.

[82] See *Ekimdzhiev and Others v. Bulgaria*, paras. 416–417.

are not notified that their data has been accessed based on the Article 286, para. 3 CPC,[83] instead, they have the right to file a complaint with the relevant judge for the preliminary procedure (Article 286, para. 5 CPC).[84]

The accused may only learn of the access to their retained data indirectly by reviewing the case files, but only after the court hearing (Article 251, para. 1 CPC). In this regard, it should be noted that, alongside the prosecutor's proposal and the judge's order for the preliminary procedure, the retained data accessed by the authorities should be included in the case files – even though the police are not required to submit a report on the obtained data to the judge for the preliminary procedure or to the prosecutor (there is only a general obligation to notify the prosecutor about the measures taken, as stated in Article 286, paras. 2 and 3).

For the exercise of the rights of individuals whose retained data has been accessed for criminal procedure purposes, including the right to be informed, provisions in the PDPA[85] may be relevant, particularly the provision on the right to access data (Article 27) and the provision restricting this right (Article 28).[86] Regarding submitting a request to the controller to exercise rights related to the processing of personal data (Article 27 PDPA), a question arises: if an individual has no information, or even indirect knowledge, about the retention and access to the data that concerns them, would it be realistic

[83] The CPC regulates the issue of informing persons only in relation to special evidentiary actions (Art. 163 CPC), but it is questionable whether it does so in an adequate manner, i.e., in accordance with the practice of the ECtHR.

[84] In this regard, see 4.2.3.

[85] In particular, the provisions regulating the provision of information and the methods of exercising the rights of data subjects is carried out by competent authorities for specific purposes (Art. 21), the right of the data subject to have certain information made available to them or to provide it (Art. 25), the right to access data (Art. 27), the right to erasure or restriction of processing (Art. 32), and the right to be informed of the correction or erasure of data, as well as the restriction of processing (Art. 34). For more information on the methods of exercising the rights of natural persons in relation to the processing of personal data, see Kalaba, 2023.

[86] These restrictions cannot last forever and indefinitely, but only to the extent and for such duration as is necessary and proportionate in a democratic society in relation to respect for the fundamental rights and legitimate interests of the individuals whose data are processed, and the authorities would have to justify their decision with clear reasons based on law. Further consideration of these issues is beyond the scope of this paper.

to expect them to submit such a request in order to find out whether and how their data has been collected and processed by the relevant authorities for criminal proceedings?[87]

4.2.3. Legal Remedy

The notification of individuals whose retained data has been accessed is a necessary prerequisite for exercising the right to an effective legal remedy concerning access to retained data for the purposes of criminal proceedings. Considering that the individual is unaware that the measure under Article 286, para. 3 has been applied to them – since they are not notified about the access to retained data concerning them – the question arises regarding their right to file a complaint to the investigating judge (Article 286, para. 5). Even if the individual were notified or became aware by inspecting the case files, questions arise about what circumstances the complaint would address, what it would seek, etc. Moreover, it is questionable whether the complaint constitutes an effective legal remedy against the order, partly because the investigating judge to whom the complaint is addressed is the one who issued the order in the first place, and it is unclear what the judge could do in response to the complaint. For all these reasons, it cannot be said that the CPC adequately regulates the right to an effective legal remedy concerning access to retained data for criminal proceedings.[88]

The provisions of the PDPA may also potentially be relevant regarding access to retained data for criminal proceedings. These provisions allow individuals whose data are being processed by competent authorities for specific purposes[89] to exercise their rights through the Commissioner, in accordance with their powers prescribed by that law (Article 35). Individuals whose retained data is concerned may address a complaint to

[87] It should also be noted that the Personal Data Protection Act provides for two regimes for the processing of personal data – general and specific. For more information on the general and specific processing regimes, see Milić, Kalaba 2023.

[88] See *Ekimdzhiev and Others v. Bulgaria*, paras. 376–382.

[89] On the difficulties of determining the entities that can be considered the competent authority that processes personal data for specific purposes, see Milić, Kalaba 2024.

the Commissioner for the protection of their rights under this law (Article 82), with the decision subject to review by the Administrative Court (Article 83) or by filing a lawsuit in court (Article 84). The extent to which these legal remedies can be considered effective is beyond the scope of this paper.

4.2.4. The "Fate" of Retained Data

The ECtHR has examined how the fate of the retained data accessed by competent authorities is regulated in situations where criminal proceedings have not been initiated and where the collected data has been included in criminal case files.[90] Regarding the storage, access, examination, use, disclosure, and destruction of retained data accessed by competent authorities for criminal proceedings, determining whether Serbia ensures an adequate level of protection requires consideration of several legal provisions.

The LEC obliges operators to undertake specific protective measures to ensure that retained data is safeguarded against accidental or unauthorized destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access, or disclosure (in accordance with the PDPA Article 130, para. 1, it. 3), and destroyed after 12 months from the date of communication (Article 130, para. 1, it. 4).[91] Concerning the data preserved and submitted to competent authorities, the LEC also requires operators (not the authorities receiving the data) to protect such data against accidental or unauthorized destruction, loss, alteration, unlawful storage, processing, access, or disclosure. However, in this case, the obligations align with the DSL.[92] Although the 12-month destruction period does not apply, the LEC provides no further rules, with the issue being regulated by other laws. Unfortunately, Serbia still lacks comprehensive regulation governing the processing of

[90] See *Ekimdzhiev and Others v. Bulgaria*, paras. 408–409.

[91] Supervision of the implementation of these obligations is carried out by the Commissioner (Art. 130, para. 3 LEC).

[92] Supervision of the implementation of these obligations is also carried out by the Ministry of Justice, as the body in charge of supervising the implementation of the DSL (Art. 130, para. 3 LEC).

personal data by judicial authorities. Regarding retained data accessed by the police, protective measures are outlined in the Law on Records and Data Processing in Internal Affairs[93] (Law on Records[94]).

The CPC does not contain provisions on the fate of accessed retained data where criminal proceedings are not initiated (e.g., it does not mandate its destruction within a specific timeframe or under certain conditions),[95] However, we should have in mind that under the Law on Records[96] the police maintain records of access to retained telecommunications data,[97] that such data is classified as secret and is stored permanently (Article 42, para. 2),[98] i.e., regardless of whether criminal proceedings are initiated or

[93] Law on Records and Data Processing in Internal Affairs, *Official Gazette of the Republic of Serbia* 24/2018.

[94] Article 42, which regulates the recording of applied operational and operational-technical means, methods and actions, stipulates that the Ministry collects and processes data in accordance with the regulations governing criminal procedure (CPC) and electronic communication (LEC).

[95] As it does so by an explicit provision on the handling of material collected through the conduct of special evidentiary actions (Art. 163 CPC).

[96] Article 42, which regulates the recording of applied operational and operational-technical means, methods and actions, stipulates that the Ministry collects and processes data in accordance with the regulations governing criminal procedure (CPC) and electronic communication (LEC).

[97] The records contain data from the judge's order for the previous proceedings of the competent court, on the basis of which access to the retained data is granted, which may relate to: the person's name and surname, the name of one of the parents, nickname, personal identification number, date, place, municipality and country of birth, the person's address of permanent/temporary residence, nationality, place of work, telephone number or IMEI number of the phone, user number, e-mail address, type of vehicle and device, vehicle registration plate, which are covered by the court order, i.e., data necessary for monitoring and determining the source of communication, determining the destination of communication, determining the beginning, duration and end of communication, determining the type of communication, identifying the user's terminal equipment, and determining the location of the user's mobile terminal equipment (Art. 42, para. 1).

[98] Although Article 42, paras. 3 and 4 CPC that the Ministry shall retain data processed in accordance with This law until the statute of limitations for criminal prosecution expires, as part of its duty to take the necessary measures and actions to locate the perpetrator of the criminal offense, to prevent the perpetrator or accomplice from hiding or absconding, to discover and secure traces of the criminal offense and objects that may serve as evidence, and to collect all information that could be useful for the successful conduct of criminal proceedings – that is, in accordance with Article 286 CPC, including obtaining records from Article 286, paras. 3–5 CPC – para. 2 of the same article specifically and in a significantly different manner regulates the retention period for records of access to retained data (and thus the retention period for retained data entered into the records).

their outcome. This raises questions about compliance with the PDPA as well as Directive 2016/680. Further analysis of this issue falls outside the scope of this paper.

Regarding the fate of retained data accessed when criminal proceedings are initiated, the CPC stipulates that case files may be reviewed, copied, and recorded by anyone with a justified interest: during the proceedings (including the preliminary investigation),[99] with permission from the prosecutor[100] or the court; and after the conclusion of the proceeding, with approval from the court president or an authorized official (Article 250 CPC).[101] Access to case files is restricted only if classified – however, unlike special evidentiary actions, data regarding the proposal, decision, and execution of the measure under Article 286, para. 3 is not classified. Additionally, the CPC does not explicitly mandate that the prosecutor's proposal, investigating judge's order, or report on collected data be classified in accordance with regulations on secret data,[102] considering the ECtHR's position that an adequate level of protection for retained data cannot be ensured when it is included in case files and follows their trajectory – thus allowing access to anyone with access to the case file. It is necessary to review how this issue is addressed in Serbia.

---

[99] Given the meaning of the term "proceedings" within the meaning of Art. 2, para. 2, item 14 CPC.

[100] In this regard, it should be emphasized that when granting permission to review a document or case, or to issue a photocopy of a document, even to persons with a justified interest, the public prosecutor takes into account the stage of the proceedings in the case and the interests of the regular conduct of the proceedings, in accordance with Article 65 of the Rules of Procedure in Public Prosecutor's Offices (Pravilniku o upravi u javnim tužilaštvima, *Official Gazette of the Republic of Serbia* 110/2009, 87/2010, 5/2012, 54/2017, 14/2018 and 57/2019). The CPC also stipulates that the review of a document may be denied by decision or conditioned by a ban on the public use of the names of participants in the proceedings, if the right to privacy could be seriously violated (Art. 250, para. 3 CPC).

[101] In addition, the documents of a legally concluded criminal proceeding are kept in accordance with the Court Rules (Court Rules, *Official Gazette of the Republic of Serbia* 110/2009, 70/2011, 19/2012, 89/2013, 96/2015, 104/2015, 113/2015, 39/2016, 56/2016, 77/2016, 16/2018, 78/2018, 43/2019, 93/2019 and 18/2022), which regulates the method of archiving and the periods for storing archived cases in criminal proceedings, counting from the date of the legal validity of the proceeding, and depending on the outcome of the proceeding (in particular, considering the type and amount of the imposed sanction).

[102] See *Ekimdzhiev and Others v. Bulgaria*, paras. 408–409.

4.2.5. Supervision

When it comes to overseeing access to retained data, it is questionable whether and to what extent the existing mechanisms in Serbia can ensure that the access powers are not misused.

The Ministry of Information and Telecommunications is responsible for inspecting the implementation of the LEC and related regulations governing electronic communications activities, carried out through telecommunications inspectors (Article 163 LEC 2023).[103] However, inspectors are not authorized to supervise the exercise of access by competent authorities, let alone assess the justification for accessing retained data in specific cases. Moreover, the supervision of compliance with obligations to implement data protection measures (Article 130, para. 3 LEC) does not include oversight of how competent authorities handle such data.

As for monitoring access based on records kept by operators and competent authorities, the records maintained under Article 128, paras. 8 and 9 LEC are classified as secret. Consequently, the declassification of such data or documents containing classified information would be possible only under conditions prescribed by the DSL. Regarding the records of requests for access to retained data (Article 130a LEC), which are submitted annually to the Commissioner for Information of Public Importance and Personal Data Protection, they include only summary statistics on requests and granted access. Importantly, they explicitly do not contain personal data related to the accessed information (Article 130a, para. 3 LEC).[104] This approach limits

[103] In addition to the authority under the law governing the performance of inspection tasks, the inspector is authorized, among other things, to inspect the actions of a business entity in relation to the implementation of measures to protect personal data and privacy (Art. 166, para. 1, it. 6 LEC 2023), and the actions of operators in relation to providing access to retained data (Art. 166, para. 1, it. 7 LEC 2023). If illegalities in the application of regulations are identified during the course of inspection, the inspector is authorized to impose certain measures.

[104] The problem of submitting the aforementioned records to the Commissioner has been the subject of analysis for several years by several nongovernmental organizations dealing with data privacy, digital security and transparency of the work of government bodies. In their reports and analyses, they indicate that in addition to a significant decline in transparency in reporting by operators and competent authorities regarding their practices of accessing retained data, which is most evident in the failure to provide information on independent access to data, the problem is also manifested in visible differences in the reports. It is also emphasized that since Article 130a of the Law on Electronic Communications does not regulate the content of the records to be submitted to the Commissioner with sufficient precision, the scope for arbitrary interpretation of this legal obligation is quite wide and seems to depend on the goodwill or, at best, on the

(but does not exclude) the Commissioner's ability to perform effective oversight in individual cases, considering the powers conferred by the PDPA. Whether these powers are adequately defined and can be efficiently applied in practice is another matter.

Regarding the CPC "oversight mechanism", the investigative judge who issues an access order is not in a position to supervise how the access is exercised or how the retained data is used. Access to retained data must be reported to the public prosecutor immediately, and no later than 24 hours after the action is taken (Article 286, para. 4 CPC) – but not to the issuing judge. Given the jurisprudence of the CJEU and the ECtHR, where a public prosecutor cannot be considered an independent body for supervising data access, the adequacy of Serbia's solution is debatable. The CPC does not require any report on data access to be submitted to the judge, nor that the judge be notified of the destruction of irrelevant or useless accessed communication data. Regarding a judge's potential reaction to a complaint filed by a data subject (Article 286, para. 5), it remains unclear what powers the judge would have in such cases.

5. CONCLUSION

In Serbia, operators are required to engage in mass retention and storage of a vast amount of data on all the electronic communications of their users, for 12 months from the time of communication. This obligation, prescribed by the LEC, lacks a clear purpose and justification. On the other hand, the LEC allows access to such data only in exceptional cases – "for a specific period" and "based on a court decision" if it is "necessary" for conducting criminal proceedings or protecting the security of the Republic of Serbia, as stipulated by other laws. Access to retained data, mandated by the LEC, is exercised for criminal proceedings under the CPC, however, this regulation does not address the issue adequately.

procedures established at the corporate level of a particular provider of electronic communications services. The practice could change if amendments to the law or appropriate secondary legislation (e.g., regulations) were to prescribe a mandatory form for submitting records of retained data, the elements of which would have to contain uniform information. The current practices of operators and competent authorities represent more of a formal fulfillment of the obligation than the substantive intention of the law to prescribe a mechanism for transparency in the retention of electronic communications data and access to that data (SHARE Foundation 2021; 2019; 2018).

The domestic legal framework has thus faced criticism due to potential inconsistencies with the Constitution and misalignment with the ECHR and EU law. It is important to note that Serbia, as a member of the Council of Europe and a candidate for EU membership, is obligated to harmonize its regulations and their implementation with the laws of these international organizations, a task that, so far, appears to have been inadequately or insufficiently addressed. In this paper, the authors clearly identify these inconsistencies, referencing relevant rulings of the CJEU and the ECtHR.

The case law of the CJEU unequivocally indicates that general and indiscriminate retention of communication data, as prescribed by the LEC, cannot be justified in itself and is contrary to EU law. Regarding access to retained data by competent authorities for criminal proceedings, the legal framework in the CPC cannot be considered limited to what is strictly necessary "in a democratic society". Consequently, based on the analysis of the relevant case law of the CJEU presented in this paper, it cannot be stated that the positions and guidelines established in the rulings of the Union's highest court have been considered so far, although it would be desirable for the legislator to address them.

As for the compliance of domestic regulations with the ECHR, the ECtHR's case law suggests that, considering that obtaining communication data through mass and general retention and access to retained data can be as intrusive as the mass collection of communication content, the general retention of communication data by communication service providers and access to such data by competent authorities in individual cases must, *mutatis mutandis*, be accompanied by the same safeguards as secret surveillance of communications. Should proceedings be initiated before the ECtHR against Serbia for violations of rights under the ECHR concerning data retention and access to retained data for criminal proceedings, it is likely that the ECtHR, as in the case of Slovenia, would find that the existing provisions forming the basis for data retention and storage fail to meet the "quality of law" requirement and cannot limit "interference" with the rights under Article 8 ECHR to what is "necessary in a democratic society." Furthermore, the retention, subsequent access, and processing of communication data under such a legal framework would be deemed incompatible with the Convention.

It can also be reasonably assumed that the ECtHR would undoubtedly point out, as it did in the case of Bulgaria, that Serbia must make necessary amendments to its domestic legal framework to end the violation of rights and ensure that its regulations are compatible with the Convention.

REFERENCES

[1] Bugarski, Tatjana, Milana Pisarić. 4/2020. Zadržavanje podataka u praksi Suda Evropske Unije. *Zbornik Pravnog fakulteta u Novom Sadu* 54: 1231–1252.

[2] Kalaba, Ostoja. 2023. Obrada podataka o ličnosti od strane crkava i verskih zajednica u pravu i praksi EU i Republike Srbije. 867–896 in *Tematski zbornik radova Savremeno državno-crkveno pravo*, edited by Vladimir Đurić, Dalibor Đukić. Belgrade: Institut za uporedno pravo; Budva: Mitropolija crnogorsko-primorska SPC.

[3] Milić, Ivan, Ostoja Kalaba. 2023. Savremeni "pametni" sistemi za regulisanje saobraćaja u gradovima Republike Srbije – (ne) usklađenost pozitivnopravnih propisa ("pazi, snima se"). 253–275 in *Tematski zbornik radova Pravo između ideala i stvarnosti*, edited by Strahinja Miljković. Kosovska Mitrovica: Pravni fakultet Univerziteta u Prištini sa privremenim sedištem u Kosovskoj Mitrovici; Belgrade: Institut za uporedno pravo.

[4] Milić, Ivan, Ostoja Kalaba. 2024. Prekršajna odgovornost i kazne za kršenje zakona o zaštiti podataka o ličnosti. 237–267 in *Tematski zbornik radova Dinamika savremenog pravnog poretka*, edited by Srđan Radulović. Kosovska Mitrovica: Pravni fakultet Univerziteta u Prištini sa privremenim sedištem u Kosovskoj Mitrovici; Belgrade: Institut za uporedno pravo; Belgrade: Institut za kriminološka i sociološka istraživanja.

[5] Mitsilegas, Valsamis, Elspeth Guild, Elif Kuskonmaz, Niovi Vavoula. 1–2/2023. Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal* 29: 176–211.

[6] Pisarić, Milana. 2019. *Elektronski dokazi u krivičnom postupku*. Novi Sad: Pravni fakultet u Novom Sadu.

[7] Podkowik, Jan, Robert Rybski, Marek Zubik. 5/2021. Judicial dialogue on data retention laws: A breakthrough for European constitutional courts? *International Journal of Constitutional Law* 19: 1597–1631.

[8] Commissioner for Information of Public Importance and Personal Data Protection. 2012. Izveštaj o izvršenom nadzoru nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti od strane operatora mobilne i fiksne telefonije u Republici Srbiji. *https://labs.rs/Documents/PoverenikovIzvestaj.pdf*, last visited April 9, 2024.

[9] Commissioner for Information of Public Importance and Personal Data Protection. 2013. Izveštaj o sprovođenju Zakona o slobodnom pristupu informacijama od javnog značaja i Zakona o zaštiti podataka o ličnosti za 2012. godinu. *https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2012/latizvestaj2012final.pdf*, last visited April 9, 2024.

[10] Commissioner for Information of Public Importance and Personal Data Protection. 2015. Izveštaj o izvršenom nadzoru nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti od strane operatora elektronskih komunikacija koji pružaju usluge pristupa internetu i internet usluge. *https://www.poverenik.rs/sr-yu/saopstenja/2128-nuzno-je-popravljati-nivo-zastite-licnih-podataka-u-oblasti-elektronskih-komunikacija.html*, last visited April 9, 2024.

[11] SHARE Foundation. 2018. *Pregled evidencije pristupa zadržanim podacima u Srbiji za 2017. godinu*. *https://resursi.sharefoundation.info/sr/resource/zadrzavanje-podataka-o-komunikaciji-u-srbiji-koliko-smo-pod-nadzorom/*, last visited April 9, 2024.

[12] SHARE Foundation. 2019. Pregled evidencije pristupa zadržanim podacima u Srbiji za 2018. godinu. *https://www.sharefoundation.info/sr/pristup-bez-transparentnosti-praksa-zadrzavanja-podataka-u-2018/*, last visited April 9, 2024.

[13] SHARE Foundation. 2021. *Pregled evidencije pristupa zadržanim podacima u Srbiji za 2020*. godinu. *https://www.sharefoundation.info/wp-content/uploads/Zadrzani-podaci-2020_izvestaj.pdf*, last visited April 9, 2024.

[14] *Washington Post.* 2014. Transcript of President Obama's Jan. 17 speech on NSA reforms. January 17. *https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3–9556–4a4bf7bcbd84_story.html*, last visited December 24, 2023.

[15] Rojszczak, Marcin. 4/2021a. National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts. *European Constitutional Law Review* 17: 607–35.

[16] Rojszczak, Marcin. 2021b. The uncertain future of data retention laws in the EU: Is a legislative reset possible?, *Computer Law & Security Review* 41.

[17] Rovelli, Sophia. 2021. Case *Prokuratuur*: Proportionality and the Independence of Authorities in Data Retention. *European Papers-A Journal on Law and Integration* 1: 199–210.

Article history:
Received: 10. 4. 2024.
Accepted: 29. 11. 2024.