REVISTA DO CEJUR/TJSC: PRESTAÇÃO JURISDICIONAL
JOURNAL OF ADMINISTRATIVE JUSTICE SYSTEM
E-ISSN: 2319-0884
OPEN ACCESS
PODER JUDICIÁRIO de Santa Catarina

ANALYSIS OF THE ACCESS TO ELECTRONIC COMMUNICATIONS METADATA FOR THE PURPOSES OF CRIMINAL LAW ENFORCEMENT IN BOSNIA AND HERZEGOVINA

Iman Pašić[1]
Manuel David Masseno[2]

ABSTRACT

Objective: This research intended to analyse the adequacy of the legal frameworks of the access to electronic communications metadata in Bosnia and Herzegovina for the purposes of law enforcement with the current Law of the European Union, an essential topic for balancing the effectiveness of criminal investigations with the fundamental rights of citizens in the current connected societies, moreover as the negotiations for accession are currently ongoing.

Methodology: The Comparative Method of Legal Research, in the strict sense, was mostly followed, also taking into consideration the Case Law of the Court of Justice of the European Union and the privacy and data protection policies of the main electronic communications operator in Bosnia and Herzegovina.

Results: After identifying and evaluating in detail the main issues arising from the current national legislation of Bosnia and Herzegovina, this research shows that, in general terms, it is already compatible with the rules and principles in force in the European Union, following the case-law of its Court of Justice.

Contributions: The research puts into evidence the current state of the Sources of Law in Bosnia and Herzegovina and how they are adjusting to the standards of the European Union, especially regarding privacy and data protection in electronic communications, as well as points out the necessary legislative initiatives in order to achieve a full compliance of criminal investigations with such standards, that may serve as guidelines for the other countries also in accession processes.

Keywords: Access to metadata. Bosnia and Herzegovina. Electronic communications. European Union. Privacy and Personal Data Protection.

ARTIGO CONVIDADO
Aceito em: 30 de agosto. 2023
DOI: https://doi.org/10.37497/revistacejur.v12i00.433

[1] Mestranda da *Univerzitet u Sarajevu* (Universidade de Sarajevo), Bósnia e Herzegovina, & do Instituto Politécnico de Beja, Portugal - imanpasic.smss@gmail.com

[2] Professor Adjunto do Instituto Politécnico de Beja e Membro convidado do Centro de estudos e análise da privacidade e proteção de dados da Universidade Europeia, Portugal / https://orcid.org/0000-0001-8861-0337 - masseno@ipbeja.pt

Análise do acesso a metadados de telecomunicações para fins justiça criminal na Bósnia e Herzegovina

RESUMO

Objetivo: Esta pesquisa pretendeu analisar a compatibilidade do regime jurídico aplicável na Bósnia e Herzegovina quanto ao metadados das telecomunicações para de fins de justiça criminal com o Direito da União Europeia, uma questão essencial de equilíbrio entre a eficácia da investigação e os direitos fundamentais dos cidadãos na sociedade conectada atual, mais ainda estando em andamento as negociações com vista à sua adesão.

Metodologia: Foi sobretudo empregue o Método da Comparação de Direitos, em sentido estrito, tendo inclusivamente em consideração a Jurisprudência do Tribunal de Justiça da União Europeia e a politica de privacidade e de proteção de dados da maior operadora de telecomunicações da Bósnia e Herzegovina.

Resultados: Depois de identificar e avaliar detalhadamente as principais questões resultantes da presente legislação nacional da Bósnia e Herzegovina, o estudo evidencia como a mesma é já compatível, em termos gerais, com as regras e princípios vigentes na União Europeia, tal como resultam da jurisprudência do respectivo Tribunal de Justiça.

Contribuições: O estudo evidencia o atul estado das Fontes de Direito na Bósnia e Herzegovina e como estas se têm adequado aos padões da União Europeia, especialmente no que se refere à privacidade e à proteção de dados pessoais nas telecomunicações, assim como assinala as iniciativas legislativas a serem ainda necessárias para alcançar uma plena conformidade das investigações criminais a tais padrões, o que pode servir de referência para o demais países em processos de adesão.

Palavras-chave: Acesso a metadados. Bósnia e Herzegovina. Justiça criminal. Privacidade e Proteção de Dados Pessoais. Telecomunicações. União Europeia.

1. Introduction

Currently, Bosnia and Herzegovina (BiH) is taking a complicated path towards becoming a full European Union (EU) member, requiring the harmonization of its legal framework with stricter EU criteria. One of the crucial areas where such alignment is necessary are the rules governing the processing of personal data by Electronic Communications Service Providers (ECSPs) in BiH such as mobile network operators and Internet Service Providers (ISPs). This essay examines how this information can be accessed by law enforcement agencies, like the Police and the Prosecutors, to effectively fight crime. Through comparative analysis, the purpose of this research is to determine whether BiH's existing legal system is increasingly being brought into line with the principles stipulated by the Court of Justice of the European Union's (CJEU) in landmark cases: *Digital Rights Ireland*, of 2014 (Judgment of the Court (Grand Chamber), of 8 April 2014, Joined Cases C-293/12 and C-594/12 - *Digital Rights Ireland and Seitlinger and Others*), and *Tele2 Sverige*, of 2016 (Judgment of the Court (Grand Chamber) of 21 December 2016, Joined Cases C-203/15 and C-698/15 - *Tele2 Sverige*). This analysis

aims at helping BiH identify any potential adjustments in legislation required for bringing closer to EU norms country's practice on data protection.

As previously mentioned, privacy and data protection became increasingly important in our connected societies. Especially today, both data protection and privacy are top concerns. The growing use of digital technologies has made individuals worry about as they easily get exposed. We will look at a specific aspect of privacy safeguards within the EU and that these safeguards influence the processing of personal data by the law enforcement agencies. Therefore, we will evaluate the structure of the system that the police and the public prosecutor, in their response to crime-fighting, are demanded to obey in order to access personal data and acknowledge the inherent supervising of rights to privacy.

The core subject matter to be dealt in this paper is comparing the BiH legal framework with EU Law, according to the case-law of the Court of Justice of the European Union. Such analysis is important, given the rulings of *Digital Rights Ireland* and *Tele2 Sverige*, which served as major reference points on the topic of data protection and privacy in the EU, even beyond electronic communications. Additionally, we will be able to assess if and how effectively BiH has implemented the core elements embedded in EU standards and what measures need to be put in place to be more consistent with those standards.

First, we will scrutinize the implementation of privacy measures in the EU regarding electronic communications. The basic points and the rules on how personal data is controlled within the Union will be shown in the first section of this paper. After, we will be able to see whether data retention by ECSPs is legal and accurate or else. Namely, to find out if the personal data involved is lawfully processed, as well as purposes limitation and necessity of secondary processing, the latter likely not to be the case, of course.

As proclaimed by the *Charter of Fundamental Rights of the European Union*, specially at articles 7 and 8, privacy and data protection are essential to Democracy and the Rule of Law. Consequently, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) has an essential role in the EU Law.

Following this, the paper starts with BiH data protection laws in electronic communications, particularly analyzing how and if they comply with EU standards, as established after the *Digital Rights Ireland* and *Tele2 Sverige* Judgments. This scrutiny will be performed at a granular level, uncovering the major stumbling blocks and advantages for BiH in the fight for the alignment of its legal framework with EU directives.

Finally, we will recommend a few measures that may upgrade the BiH regulations so they may be in line with the EU regulations in terms of privacy and data protection.

2. The Protection of personal data in electronic communication within the European Union

Data retention policies within EU have been significantly influenced by judgments made by CJEU in *Digital Rights Ireland* and *Tele2 Sverige*. *Digital Rights Ireland* Judgement resulted in striking down a directive that required electronic communications providers to retain all user data on the grounds it violated privacy rights (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). Similarly, in *Tele2 Sverige*, the CJEU ruled that Swedish laws requiring data retention were invalid, reinforcing the stance that indiscriminate data retention is incompatible with EU Law.

In this section, we will delve into the impact of the CJEU rulings and the GDPR on national laws. Both the rulings of the CJEU and the GDPR have had a profound effect on national laws across the EU. EU Member states have had to change their legal systems to comply with EU standards, often necessitating significant changes to their laws. This has included things like the development of more stringent accountability mechanisms, more detailed stipulations regarding time limits for retention of information as well as increased protections offered to the rights of individuals.

In brief, *Digital Rights Ireland* was a breakthrough ruling that fundamentally altered how data retention was carried out within European Union countries. The CJEU emphasized that, according to the standards present at Article 52 of the *Charter of Fundamental Rights of the EU*, data retention legislation must be in proportionate necessity test form. It was held that the Directive at issue, requiring all users' electronic communications data to be retained without any differentiation between them, constituted

a serious infringement on privacy and protection of personal data. In this section, we will analyze the landmark *Tele2 Sverige* case, a pivotal decision concerning data retention and privacy rights in the EU.

Subsequently to *Tele2 Sverige*, the CJEU reiterated and clarified the principles laid down by the Digital Rights Ireland ruling. It ruled that domestic law should thus ensure that only necessary information is kept during the data retention process. Blanket retention rules or policies were found incompatible with EU Law, while relevant safeguards had been put in place for any such retain, subjecting it to a targeted approach which would respect individual's privacy.

These Judgement were followed by a string of decisions (C-207/16, *Ministerio Fiscal*, of 2 October 2018; C-511/18, C-512/18, C-520/18, & C-623/17, *La Quadrature du Net*, of 6 October 2020; C-746/18, *Prokuratuur*, of 2 March 2021; C-140/20, *Commissioner of An Garda Síochána*, of 5 April 2022; and C-793/19 & C-794/19, *SpaceNet*, of 20 September 2022) that consolidated the main purpose of the Court, that the *Charter of Fundamental Rights of the European Union* had to be taken seriously.

3. The access to personal data in electronic communications in Bosnia and Herzegovina

In Bosnia and Herzegovina, under certain conditions, law enforcement agencies may be given access to personal data from telecoms and providers by the *Law on Criminal Procedure* (In full, the "Law on Criminal Procedure of Bosnia and Herzegovina", Official Gazette of BiH, No. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13) Article 116 spells out special investigation methods that include telecommunication surveillance and technical intercepts, computer systems access among others. It requires authorization from a court and must be determined to be necessary for investigating or prosecuting crimes.

Meanwhile, the Regulatory Agency for Communications (RAK, *Regulatorna agencija za komunikacije* <https://www.rak.ba/bs-Latn-BA/>) issues licenses ECSPs, including the ISP, and ensures compliance with data protection laws. Thus, striking a balance between law enforcement's needs with respect to privacy and data protection of individuals is a key role played by RAK.

On the other hand, the procedure for law enforcement agencies to obtain personal information has been designed to ensure that it is legal and proportional. These steps are as follows:

1. Submission of Request: A formal request indicating the purpose and scope of the request is made by law enforcement agencies.

2. Approval by the Judiciary: Within this process, there must be an assessment of the necessity as well as proportionality of measures requested through competent courts; thus, they are supposed to review its advisability thereby bringing it into line with Rule 11(3).

3. Data Provision: Upon approval, ECSPs are required to provide the requested data, ensuring compliance with legal and regulatory requirements.

4. Oversight and Accountability: The entire process is subject to oversight by regulatory bodies and independent authorities to prevent abuse and ensure transparency.

In BiH, as in the European Union, one of the most pressing challenges as to do with observing proportionality in relation to accessing personal data. This principle is important for the protection of individuals' privacy rights and enables law enforcement agencies to carry out their duties effectively. In practice, this implies that security forces must convincingly establish that they require access to personal data under certain circumstances pertaining to investigations. They should also show why less intrusive means cannot be employed in gathering facts about incidents under investigation. Otherwise, the criteria can ensure that access will not be given just upon request from law enforcement agencies, but only when it is proportionate to the legitimate aims such as investigating and preventing serious crimes.

Consequently, ensuring proportionality involves a rigorous assessment process. Law enforcement agencies must provide detailed justifications for their request for accessing data including clear proof of necessity of data for an inquiry. It has required that due caution should be exercised concerning the type of investigation, the nature of information sought and its potential effect on the privacy rights of an individual being investigated. It is a tightrope of balancing between the police's or prosecutors' desires

and the individual's right to privacy, which must be handled with utmost caution to avoid any unnecessary interference in people's lives or power abuse.

This line is held by judicial oversight, which ensures that data access requests are legal as well as justified. The judiciary acts as an important control over law enforcement agencies by checking their demands for accessing personal data independently. This is important in safeguarding privacy rights and ensuring that any data access meets laid down legal requirements.

The judiciary on its part should have the capacity and resources required for effective judicial oversight. To begin with, judges and other members of the judiciary ought to undergo training on laws related to the protection of information and implications of making such requests among others. Besides this, they should have adequate time and resources through which they can read through every request. This entails scrutinizing justifications provided by law enforcers, assessing whether proportionate necessity standards were met with respect to the information sought, as well as being consistent with legal frameworks in place.

In addition, there must be a clear methodology for evaluating data access requests within judicial oversight mechanisms. With these mechanisms, transparency and accountability should be promoted so that individuals are given a proper understanding of how their personal data is accessed and for what purposes. In case access to data is considered unjustifiable or too intrusive, the courts should have powers to reject such requests and provide remedies to the affected individuals.

For example, to effectively address these challenges, BiH must strengthen its legal and institutional frameworks for data protection and judicial oversight. This requires updating existing laws to meet EU standards and best practices by ensuring they offer strong safeguards for personal information while giving clear guidelines on procedures of law enforcement agencies. In addition, it also demands the development of judicial capacity able to handle complexities associated with requests for accessing information.

Consequently, investing in training and resources for both law enforcement and judicial personnel becomes essential. There is the need for law enforcement agencies to evaluate the legal requirements around retrieving data, as well as understand why they must observe privacy rights of citizens. Hence, judicial officers should become better informed about legislation on safeguarding information from misuse besides being equipped enough so that extensive scrutiny can be made regarding how data has been obtained. Furthermore, the establishment of a sense of responsibility and openness within

security agencies and courts is important. This includes putting in place regular audits and reviews of data access practices as well as avenues for challenging unwarranted data access and obtaining remedies.

Equally important is involving citizens in discussions about data protection rights and privacy. Raising awareness about proportionality principle as well as judicial oversight can make individuals better understand how to protect their rights. Previous public information campaigns, seminars with nongovernmental organizations (NGOs) and open talks have helped to create an educated society that now knows its rights.

At last, but not at least, creating a culture that respects privacy and holds accountable the responsible departments will enable BiH earn trust from the public, judiciary, law enforcement agents. This trust shall ensure the effectiveness of law enforcement while protecting individuals' rights in an increasingly digital world.

4. Bosnia and Herzegovina's Compliance with EU Standards

As stated, the above-mentioned Judgments of CJEU set high standards of data protection within the EU regarding electronic communications. They lay down that targeted and proportional data retention measures, as opposed to blanket retention policies, are essential. Also, they address strong oversight mechanisms to ensure that law enforcement's access to data is legitimate and confined.

Bosnia and Herzegovina's legal framework lays the foundation for personal data protection, with the "Law on Protection of Personal Data" (Official Gazette of BIH', nos. 49/06, 76/11 and 89/11) (DP Law). However, there are several areas where it can be further aligned with EU standards. For instance, there is a lack of detailed rules specifying how long certain information can be stored in servers or what circumstances should trigger information sharing among different security departments. Additionally, a transparent mechanism of assessing whether grounds existed to request accessing data is imperative.

Hence, specific regulations should be put in place outlining the period within which information must be held, as well as situations when an individual can claim his record/ deletion rights from search engines would improve legal certainty while enhancing conformity with EU norms. Namely:

- Separate Independent Oversight: Independent oversight authorities need to be established too.

- Improving Transparency and Accountability: A Review of Data Access Requests by an Independent Oversight Body will Ensure that Data Access is Justified and Proportionate

- Transparency and Accountability: Making data collection, retention periods, and user rights clear would bring Bosnia's practices in line with the EU principles; giving better protection to individuals' right to privacy.

Alongside, any sound research has to deal with the realities in place. As a matter of fact, by far, *BH Telecom* <https://www.bhtelecom.ba/> is the leading ECSP in BiH. So, an analysis of its stated privacy and data protection policies is inescapable. According to them, *BH Telecom* processes client's information following both national and EU regulations. Specifically, it collects personal information such as names, contact details or identification credentials necessary for rendering services. Besides, data retention policies are designed to comply with legal requirements.

Indeed, the company does not collect personal data without consent, and the further processing of that data is based on certain legitimate grounds. *BH Telecom* is bound by the country's legal system and the requirements and supervision of the agency. By complying with the DP Law, *BH Telecom* ensures that data collection and processing is legal, fair, and transparent. However, certain modifications in some areas are necessary to ensure compliance with EU standards.

For its part, *BH Telecom* uses defense-in-depth approaches to securing personal data through both technology and work processes. These efforts involve encryption, secure access, and regular security checks. Considering this, *BH Telecom* is aware that it must regularly improve and constantly move with the times to be able to offer a satisfactory level of data security. Such as better transparency, as such it would involve *BH Telecom* complying with the provision of the individual's need of data by being more direct with some information like the period that the data would be stored, and the rights of the users. This way, people would be informed about how their data is processed and protected. The same for more stringent data retention policies: More stringent data retention policies that are in line with the principles of data minimization and data storage limitations.

To conclude, the introduction of an independent body that reviews issues concerning the provision allowing law enforcement agencies regarding the access to data

besides legal procedures would, in turn, ensure that the demand for such information is backed up by reasonable grounds.

5. Special investigative actions and conditions for their application

Article 116 of the *Law on Criminal Procedure of Bosnia and Herzegovina* articulates the procedures and criteria for special investigative actions, and the conditions under which they can be applied. This provision is critical for regulating how law enforcement agencies access and use personal data during criminal investigations, ensuring that such actions are conducted legally and ethically, as its 2nd paragraph obliges them to obtain judicial approval to use special investigative measures that could permit wiretapping or other surveillance procedures.

Thus, according to *Law on Criminal Procedure*, the police and prosecutors are legally authorized to extract the identities and personal data of ECSPs subscribers with the approval of a court, in order to comply with the need for the data to be relevant and proportional in the context of criminal investigations. Namely, concerning:

1. Eavesdropping and technical recording of electronic communications. Under this rule, the police and the prosecution, upon court endorsement, can both monitor and record the communication between the suspects. This typically covers activities such as phone calls and text messages. The purpose is to collect proof of criminal activities from the intercepted communications.
2. Access to Computer Systems and Computer Matching. The police are provided with the access right to the computer systems of suspects. This access is used to find data and compare it to find out evidence of crimes. The process involves a detailed examination of digital footprints left by suspects.
3. Surveillance and Technical Recording of Premises. This is the case when the police may install cameras and other recording devices within the properties of suspects. The purpose is to collect both visual and audio evidence that may be the most significant in the finding of criminal activities executed in private properties.
4. Covert Monitoring and Technical Recording of Persons and Objects. This section gives the police the right to shadow suspects and video their activities secretly. Contact means not only monitoring behavior, but also collecting information by other methods, such as wiretapping, which generally is kept secret from the suspect. Under this scenario, covert operations can include tracking

movements, recording interactions, and observing behaviors without the suspects' knowledge.

5. Undercover Investigators and Informants. This can be achieved using undercover agents and informants, who are operatives of law enforcement agencies that often get inside criminal organizations to get information. These undercover agents can obtain information and evidence from crime scenes, which play an important role in dismantling criminal networks and prosecuting their members.

Then, paragraph 3 refers to the investigative measures from point 1. from Paragraph 2 - surveillance and technical recording of electronic communications. So, investigative measures can only be used against a person suspected of transmitting information to or from the executor of a criminal offense, or against a person suspected of using the suspect's electronic communications device

In short, Article 116 of the *Law on Criminal Procedure* bestows on the police and the prosecutor's office the provisions with which to carry out the collection of evidence that is necessary in the war against crime. Nevertheless, the exercise of these powers is subject to court approval and specific conditions. The judiciary's role involves scrutinizing these acts and ensuring the principles of relevance and proportionality, thereby safeguarding the rights of individuals and creating an environment that is conducive to the actions of law enforcement.

6. How close are the laws of Bosnia and Herzegovina to the standards of the EU Court of Justice after the judgments of *Digital Rights Ireland* and *Tele2 Sverige*?

In Bosnia and Herzegovina, as mentioned, RAK is the official regulator for the communications in Bosnia and Herzegovina. Their responsibilities are overseeing the electronic communications market, issuing licenses to ECSPs, including ISPs, protecting the rights of users of electronic communication services and ensuring fair competition within the sector. Additionally, RAK has the role of ensuring the compliance of ECSPs with the laws and regulations on data protection.

Therefore, one of the most significant legal provisions in this context is Article 41 of the *Law on Electronic Communications* ("Law on Electronic Communications of Bosnia and Herzegovina", Official Gazette of BiH, No. 31/03). This article outlines the regulations regarding the retention and processing of electronic communications data by ECSPs. The

article serves as a cornerstone for balancing the dual imperatives of data protection and crime prevention. As of, Article 41 (**Collection of data on electronic communications**) "Electronic Communications Services Providers cannot store data on attempted or completed electronic communications and content of these communications. Except for the period specified by law, or regulations adopted on the law".

In general terms, this provision hampers ECSPs from storing data related to attempted, established electronic communications, or the content of communications. Besides, data can only be retained for a period which is determined by law regulations. This exception allows legal frameworks to define circumstances and frames of time for metadata retention.

Even if this provision establishes a baseline for user privacy by prohibiting indiscriminate data retention by ECSPs, the exception clause allows for legal frameworks to define circumstances for metadata retention, potentially for law enforcement purposes. Moreover, such regulation will have to comply with the criteria and standards enunciated at the *Tele2 Sverige* Decision.

As stated, for the present, the exceptions are at Article 116 of the *Law on Criminal Procedure in Bosnia and Herzegovina*, stating the special investigative measures that law enforcement can use under some conditions. These measures include surveillance and technical recording of electronic communications and metadata access, including the capability to surveil and technically record electronic communications can potentially involve accessing metadata, such as phone numbers, time of communication, and location data.

Thus, law enforcement agencies can only have recourse to these measures if they can't obtain evidence through other means or if obtaining evidence through other means would be excessively difficult as stated in Clause (1). This implies there should be limitations on how often and for how long metadata can be accessed.

The most explicit statement is that, according to Article 41. law enforcement access provision doesn't disclose a clause exception like the one quoted above that can be considered rather specific. So, this clause does not cover the cases where a national measure (law or regulation) that would allow for metadata retention only for law enforcement purposes is present. On the other hand, such legislation or regulation must be clear and should fulfill the restrictions that, most likely, are prescribed within the legal setting.

Additionally, Article 116 also provides further details on metadata retention and access, related to the special measures available to law enforcement agencies in given cases. Specifically, cameras and technical tools that can record the conversations are the measures mentioned by this Act. Also, the possibility of electronic communication surveillance and technical recording can include the access of metadata pointing to the phone numbers, time of communication, and location data. The reason behind the decision to allow law enforcement to do so is the difficulty of using other methods or the infeasibility of their use as it stated in Clause (1). Thus, it gives the idea of the need for the legal restriction of these devices in terms of how much and how long they can be utilized.

For its part, Article 15 of the *ePrivacy Directive* (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)) specifies the discretion of the member states to limit the rights and obligations that are established elsewhere in Directive except when there are special circumstances. States may enact laws that impose certain restrictions on users relating to data protection and privacy as provided in other articles of the Directive.

Article 15
Application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on the European Union.

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply regarding national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

3. The Working Party on the Protection of Individuals about the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

Accordingly, these are only allowed if they are necessary, appropriate, and proportionate. They can also be used for national security defense, public security, and crime prevention, investigation, detection, and trial. Therefore, states can create laws permitting data retention for a brief period if they have the reasons given above, within the limits of EU Law

Although the term of storage of data is not directly addressed in article 15, it sets the legal frame for the regulation of this issue by member states. In *Tele2 Sverige* ruling, the court held that the practice of collecting and "indiscriminate and non-targeted" processing of traffic data by ECSPs is incompatible with EU Law. Consequently, Member states are not allowed to invoke Article 15 for justification of data retention for any period and in any manner; the period and the mode of retention must comply with the Article.

In the case of Bosnia and Herzegovina, namely, *BH Telecom* collects and stores personal data in order to ensure the provision of its services, including personal information such as name, e-mail address, telephone number, identity card data, date of birth, and any other relevant data required for functional reasons. *BH Telecom* declares that it strictly follows the regulations that protect information security and personal data of individuals in Bosnia and Herzegovina, especially the DP Law, having the GDPR as an interpretative benchmark.

In general, the personal data of a customer is stored and processed by *BH Telecom* if it is mandatory to provide services, within the regulatory period. But, if the regulations provide for longer or shorter periods for storage for one purpose or in other cases, the data will be deleted permanently, or it will become anonymous. Refusing to obey the request of anyone who is not from the state bodies or does not / has not written before the request of help from the state bodies is sufficient to verify that a prevention of access, hiding of data, or changing the configuration of the call detail record is impossible.

In conclusion, due to *BH Telecom*'s strict adherence to the regulations of data protection, people’s personal information is gathered and stored with the utmost care and responsibility. Through such observation, *BH Telecom* has extended not only the local legal framework but also very wide the slate of laws and other instruments the EU has charge of. The user's rights of privacy as consumers of the service and the remark of the necessity of legislation and other rights as the mainspring of data regulation were, in addition, changed.

7. Discussion

The compatibility of data collection and holding in Bosnia and Herzegovina is in conformity with EU standards, as per the EU Parliament's decision, which was sealed by the European Court of Justice in the landmark cases of *Digital Rights Ireland* and *Tele2 Sverige*, serves as an acceptance as well as a call for further development.

To begin with, *BH Telecom* ensures the shortening of the data storage period, thereby, the company is in line with the principle underlined by the CJEU that the storage period should be limited to what is necessary for the legitimate aim. However, the legislation which limits the duration of data storage must find the middle ground with the CJEU's stand of exceptions on legal basis.

Next, *BH Telecom* offers the subjection of data processing to some extent in that it allows users to opt-out of marketing messages, hence, providing a part of the rights of objection to data processing. Nonetheless, the control is partial. *BH Telecom* will have to build its policy further so that users are able to reach through and verify the data that is collected from their use and to be able to ask for its full deletion, thus having full control over the usage of their personal data, in order to comply with the DP Law and, in the future, with the GDPR.

Besides, *BH Telecom* must address data security and privacy issues in order comply with the European Union's expectations of improving the integrity of the system. Hence, the ground for the processing of data should be clarified. In addition, users' rights such as the right to access and raise a request for the correction of information, must also be restated, as well as the way of submitting a claim. Alongside specifying data storage periods, the criteria for determining the duration of storage for different categories of personal data would also enhance transparency.

However, in Bosnia and Herzegovina, the situation concerning the retention of electronic communications metadata and their access by law enforcement agencies is still complicated and uncertain. As we have seen, the main exception to the *Law on Electronic Communication*, at Article 41, gives room for further definition by subsequent laws or regulations, whether data retention is needed for law enforcement cases or otherwise. On the other hand, the *Law on Criminal Procedure* in Article 116 (2) - point a says that the Ministry of Internal Affairs cannot store their data in an external storage facility, but at (a) it does not explicitly mention data retention.

The lack of laws or regulations that specify the exception in Article 41 should be addressed, especially in order to define the extent of the metadata retention period and the

grounds of the access by law enforcement officers under Section 116. Hence, it is of the upmost relevance to clarify whether law enforcement agencies can access metadata retained according to Article 41 under the force of Article 116 and, if not, what is the overall status of that data. In short, the provision requires further clarifications to overcome these uncertainties.

8. Future trends and conclusions

Future directions, around a study on data processing and data protection in Bosnia and Herzegovina will most likely be related to aligning the domestic legislation with the EU guidelines. In the future, more efforts should be channeled into the draft of the proper legal setting through the making comprehensive data protection laws that adhere to CJEU requirements. The forthcoming period should also include steps ensuring the transparency of the data collection and processing purposes by Electronic Communications Services Providers and the access by law enforcement agencies.

Over the next years, educational programs should become the point of action, the development and running along with creating the protection training programs for more people in the electronic communications industry will be the most important achievement. In addition, future studies should also analyze the consumers' views and satisfaction *vis-a-vis* such data protection measures.

The area of research where the influence of new technologies on data protection and retention policies is most substantial has to do with the development of new policies. It is likely that scholars, also in Information and Communications Technologies, will be concerned with the legal and ethical aspects of data retention for law enforcement purposes. Based on the emerging trend we are likely to witness more and more of such high-quality comparative analysis exercises in BiH, yet the balance between the necessity of data retention and the privacy rights of individuals will remain a key issue of conflict.

Surely, best practices for the retention of data and access policies will be a point of concentration. Thus, exploratory research will have to be conducted on the possibility of multinational policy formation about data protection and retention. The same for the effectiveness of the education of users on rights and controls of data protection will be a significant sector of research. Further work will be needed for the purpose of understanding and evaluating the usability and integrability of Privacy-enhancing

technologies in accordance with privacy preservation in keeping and the use of data by the organizations.

To conclude, this brief research into the compliance of data processing and retention in BiH with EU standards shows that there is great development potential. Proper harmonization of national legislation with EU law, enhancement of transparency in the collection and processing of data, and creation of independent monitoring bodies in their regulation are very important steps toward higher levels of data protection. This must account for the user's full control over his/her data: access, reviewing, and even deleting of personal information. Besides, there is a continuing need for surveillance to balance national security interests with personal rights to privacy and constantly monitor policy adjustments to secure the protection of fundamental rights of citizens.

There are, however, evident shortcomings. The policies can be, and often are, obscure, sometimes even conflicting—thereby leaving a window open for data protection gaps. This is further compounded by the fact that there are no clear policies with respect to the retention periods and standards for accessing such data by the police. Furthermore, mechanisms for user control are weakly established, while transparency over the processing practices is not high. These weaknesses can only be overcome through concerted work of all stakeholders: policymakers, Electronic Communications Services Providers, and civil society organizations in Bosnia and Herzegovina to really deliver a strong legal framework for personal data protection, at least in the Electronic Communications Sector.

9. References

Agency for Personal Data Protection. (n.d.). Izbor jezika. Retrieved from: https://azlp.ba/

BH Telecom. (2021). Data Protection Policy. Retrieved from https://www.bhtelecom.ba/wp-content/uploads/2021/10/Politika-zastite-licnih-podataka-BHT.pdf

RAK - Communications Regulatory Agency. (n.d.). About. Retrieved from https://www.rak.ba/en/about

Federal Institute of Statistics, Bosnia & Herzegovina. (n.d.). Law on Personal Data Protection. Retrieved from: https://www.fzs.ba/

Granger, M-P. & Irion, K. (2014). The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection. *European Law Review*, 39(6), 834-850. Available at: https://hdl.handle.net/11245/1.432802

Kmezić, M. (2020). Recalibrating the EU's Approach to the Western Balkans. *European View*, 19(1), 54-61. Available at: https://journals.sagepub.com/doi/full/10.1177/1781685820913655

Lynksey, O. (2017). Tele2 Sverige AB and Watson et al: Continuity and Radical Change. *European Law Blog*. Available at: https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/

Masseno. M. D. (2011). Surveillance and Data Protection: why is data retention regulation so relevant? "Keynote Lecture" at the "Rovaniemi Summer School of Legal Informatics", University of Lapland. Available at: https://bit.ly/3y0HiCB

Mieńkowska-Norkiene, R. (2021). The Political Impact of the Case Law of the Court of Justice of the European Union. *European Constitutional Law Review*, 17(1), 1–25. doi:10.1017/S1574019621000080. Available at: https://www.cambridge.org/core/journals/european-constitutional-law-review/article/political-impact-of-the-case-law-of-the-court-of-justice-of-the-european-union/7087EF154AF71D6B36494E6B4FEB297B

Meškić, Z. & Samardžić, D. (2017). The Strict Necessity Test on Data Protection by the CJEU: A Proportionality Test to Face the Challenges at the Beginning of a New Digital Era in the Midst of Security Concerns. *Croatian Yearbook of European Law and Policy*, 13, 133–168. Available at: https://www.cyelp.com/index.php/cyelp/article/view/275

Murphy, M. H. (2014). Data Retention in the Aftermath of Digital Rights Ireland and Seitlinger. *Irish Criminal Law Journal*, 24(4), 105. Available at SSRN: https://ssrn.com/abstract=2614388

Pfisterer, V. M. (2019). The Right to Privacy — A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy. *German Law Journal*, 20(5), 722-733. Available at: https://www.cambridge.org/core/journals/german-law-journal/article/right-to-privacya-fundamental-right-in-search-of-its-identity-uncovering-the-cjeus-flawed-concept-of-the-right-to-privacy/412B4D05F6D91C60735234124BA5FA4B

Robinson, G. (2023). Targeted Retention of Communications Metadata: Future-proofing the Fight Against Serious Crime in Europe. *European Papers*, 8(2), 713-740. Available at: https://www.europeanpapers.eu/en/e-journal/targeted-retention-communications-metadata-future-proofing

Rojszczak, M. (2021). National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts. *European Constitutional Law Review*, *17*(4), 607–635. Available at: https://www.cambridge.org/core/journals/european-constitutional-law-review/article/national-security-and-retention-of-telecommunications-data-in-light-of-recent-case-law-of-the-european-courts/BCE3F7879744C2BFEC06DBD40F1F4A59

Tomić, A. (2024). *Bosnia & Herzegovina - Data Protection Overview | Guidance Note.* Atlanta: OneTrust. Available at: https://www.dataguidance.com/notes/bosnia-herzegovina-data-protection-overview

Vejnović, D. & Lalić, V. (2005). Community Policing in a Changing World: A Case Study of Bosnia and Herzegovina. *Police Practice and Research*, 6(4), 363-373. Available at: https://www.academia.edu/93387721/Community_Policing_in_a_Changing_World_A_Case_Study_of_Bosnia_and_Herzegovina

Zaımovıc, T. (2018). Telecommunication Sector Regulatory Challenges in Bosnia and Herzegovina. *İktisadi İdari Ve Siyasal Araştırmalar Dergisi / Journal of Economics Business and Political Researches*, 3(7), 165-185. Available at: https://dergipark.org.tr/en/pub/iktisad/issue/38174/422608