Dragana B. Petrović*

Review scientific paper
UDK: 343.211.3:342.721
doi: https://doi.org/10.56461/SPZ_22407KJ

PRIVACY AND PROTECTION OF PERSONAL DATA – CRIMINAL LAW ASPECT**

Abstract

Currently, across the globe and on different levels, serious debates are held on the possibilities of modern information communication technologies (ICT), including the internet, as well as their undesirable consequences. To an ordinary person, the "new" way of communicating via the internet and mobile phone is at the same time easy, simple, quick, and essential – it has become a fact of their daily lives. Moreover, the modern age purports the internet as one of the critical means of communication. If used "properly", it represents an abundance of information on nearly every topic and entails many opportunities. With a vast and varied amount of collected data, it easily negotiates the acquirement of new learning and the shaping of lifestyle. However, the use of modern technologies which constantly transform, at times even completely changing and automatising nearly all areas of human activity, has its dark, destructive, and devastating side. Within that perspective, life in a network becomes increasingly more susceptible to manipulation and abuse. And the list of abuses is long... from having these technologies abused as a database, to an assault on someone's privacy, stalking, cyber-mobbing, peer violence, sexual harassment and violence, human trafficking, organ trafficking, etc. Thus, a stance is formed – the emergence of new technologies has significantly endangered the right to privacy. In recent years, the right to privacy has been mostly associated with personal data, so, in that regard – when speaking about privacy, it is nearly always done in the context of personal data processing. The right to privacy and personal data protection falls within basic human rights, so, being that it is a fundamental right of man and citizen, the baseline of its protection in our legislation is comprised within, above all, the Constitution, The Law of data protection and The Criminal Code (Art. 146. Unauthorized collection of personal data). As the title suggests, the criminal law aspect of privacy and protection of personal data provided for in Art. 143 of the CC is the focus of this paper. In this context, the author,

* PhD, Research Fellow, Institute of Comparative Law, Belgrade, Serbia
E-mail: *d.petrovic@iup.rs*

* This paper is a result of the research conducted by the Institute of Comparative Law financed by the Ministry of Education, Science and Technological Development of the Republic of Serbia under the Contract on realisation and financing of scientific research of SRO in 2022 registered under no. 451-03-68/2022-14/200049.

first of all, embarked on an analysis of the current state of threats to the right to privacy as a prerequisite for action in the direction of its protection. Abandoning the general consideration of this type, the examination is then focused on concretely explaining the meaning and essence of the criminal act – unauthorized collection of personal data, the forms in which it manifests itself, the criminal responsibility and punishment of the person who committed this act. With the statement that this is a dynamically changing reality, some of the key problems and challenges in the application of appropriate mechanisms for the protection of the right to privacy in the Republic of Serbia (with a special emphasis on the year behind us) were highlighted.

Keywords: *information technologies, internet, privacy, personal data protection, Criminal Code.*

1. Introductory Contemplations

Today it is useless to memorize data from history, mathematics, art, and literature... we are but two clicks away from the information. By becoming increasingly dependent on the internet and, to the delight of numerous users all across the globe, modern technology is becoming more available and easier to use by each day. Most of us have smartphones, computers, tablets... social media, SMS, videos, and photos... As one can observe, new technologies are becoming our external memory. They have, for the most part, subdued our lives and spontaneous communication. With its omnipresence, they have comprehended the "microstructures of everyday lives all the way to human privacy and intimacy, even to their dream".

On the fourth of March 2022, the internet social media Facebook celebrated its 18th birthday. Two billion and eight hundred million of its monthly active users across the globe confirmed that it was one of the most attractive media phenomena at the beginning of this millennium (2010-2019), globally (Diligenski & Prlja, 2018, p. 9).[1] Yes, it's a global phenomenon – spatial, regional, ethnic, and all other restrictions are cancelled – and thus, the world becomes a global community, and the internet – a super-road network of information (Cybercrime law around the world | Links and updates). It is noteworthy that it has become a technological, social, media, political, and at the same time a legal phenomenon. That

[1] Facebook was conceived by Mark Zuckerberg, a former Harvard student (together with his friends). Initially, it was intended only for the students of the university to communicate and exchange information via this network. Later, it was joined by many other universities, high schools, large global corporations, etc. When the famous Microsoft company bought 1.6 shares of Facebook for 240 million dollars, and the value of the site was estimated to 15 billion dollars, it became clear that a new global phenomenon was born, and its creator – the youngest person on Forbes Billionaire list. In 2021, Facebook changed its name to META.

"multitude" suddenly seems like an incomprehensible chaos. Undoubtedly, it is not possible to achieve complete protection of the information system at today's level of development. Therefore, it is necessary to provide absolute and effective protection if it comes to its abuse (identity theft, fraud, terrorism, piracy, hate-speech, internet vandalism, abuse of photographs, pathological internet addiction, etc.) (Summers, 2015, pp. 48-60).

As the powerful dynamics in this field has swept us, the technicalization of human communication has adopted new methods, and it is done in such a way that there is only one thing left – a complete substitution of reality with the "reality" of the network. The mobile phone has become a crucial accessory. Manufacturers are very quickly adapting to the new trend of mass and obsessive usage of this device, drawing customers into their networks of pathological addiction (the "big brother" tool) (Stallman, 2011) with no resistance. It is an irreversible process – modern internet technology has nested itself everywhere and has not spared a single level of human activity and personality. It has made everything bare and public, leading to the annulment of every part that comprises the human most intimate "private property".

From the point of view of the world we live in, with the sudden development of digital technologies, the right to privacy, and so personal data protection has seriously been challenged. It is as if the affliction of privacy and illegal personal data processing has become inevitable elements of the modern internet landscape (Prlja & Reljanović, 2009, pp. 163-164). It is the reality in which we currently find ourselves. However, alongside this ominous reality, the efforts to develop a legal regulation on both a national and international level have been growing – all intending to efficiently solve the matter of protection and to strengthen and expand that protection (What is IT law, ICT law or Cyber law).

Because, understandably, the changes in the modern IT usage stage and the negative effects they produce also require changes in terms of reacting to the endangerment of this right – one of the most cardinal human rights.

2. What Is Privacy?

As early as the first written article on the notion and content of privacy, in 1890 Samuel D. Warren and Louis Bradeis defined this right as "the right to be alone" (Popović & Jovanović, 2017, pp. 123-125).[2] In such an interpretation, a more

[2] "The right to privacy" as a term that is so widely discussed today, existed in ancient cultures as well – in Chinese, Hebrew, Greek, and Roman. It is first mentioned by Aristotle in his *Politics*, when making a distinction between private and public spheres. However, even though Ancient

extensive meaning of the notion is being defined – one which comprehends the right of a person to autonomously select "isolation from the presence of others if they desire and the right to be protected from being followed in a private environment such as their own home" (Ilić, 2016. p. 20). In regular communication, the term privacy is used to signify something which is personal, confidential, unofficial, hidden, shut from the public (Hadson, 2010, p. 13). From this perspective, we can consider private what is opposite of public. Within the private sphere, an individual has the right to be unavailable to others in things that do not concern them (that they should not even engage in), it is a protected space from which every other person is physically or mentally excluded (Vodinelić, 2012, p. 259). Within the private space, the individual is free from the involvement and interference of others, left to themselves, their feelings, needs, or whims. In such a manner, privacy implies the establishment of physical boundaries against the entrance of a third party into the personal space of the individual. From the marked conceptualizations of the term privacy (Bornes, 2006), its basic meaning and essence emerge, which involve the protection of moral and physical integrity, the right to choose a corresponding style and manner of living, interaction between people, etc. (Ilić, 2016, p. 20).

On an international level, normative regulation of this area began with the adoption of Universal Declaration of Human Rights – the United Nations, (Art. 12), in 1948, The Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights (Art. 8) in 1950, and International Covenant on Civil and Political Rights (Art. 17) in 1966. European Convention on Human Rights which by Art. 8, includes the right to privacy among basic human rights "with a fanfare", "everyone has a right of respect towards their private and family lives, homes, or correspondences". The European Court of Human Rights in Strasbourg stipulated that the relative article provides protection in communication via the internet, e-mail communication, online tracking of an internet communication. By precisely establishing the aforementioned forms of protection, the Court puts an emphasis on the protection of personal data which is, in fact, included in the article. In short, the protection refers to data on the entire mental and physical integrity of a human (from name, origin, health condition, sexual orientation... to potentially sensitive data, *e.g.* IP address of an internet user) (Popović & Jovanović, 2017, p. 127).

Within the European Union, there is the exceptionally significant Charter of Fundamental Rights of *the European Union*,[3] which regulates the right to

Greece and Rome knew about privacy, they did not practice it in the way we know it today. It was only in Early Christianity and propagating prayers in silence, and the right and need for peace and unobstructed intimacy, that privacy in its genuine sense gained importance.

[3] The Charter of Fundamental Rights of the European Union (CFR) enshrines certain political,

protection of personal data via Art. 8, Protection of personal data[4] while Art. 7 is specifically focused on the protection of private and family life, and The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Today, the legislation of the EU rests on two most important prescripts: General Data Protection Regulation (EU) GDPR 2016/679, which substituted Directive 95/46/EC, and Directive 2002/58/EC. In a sense, the standing ePrivacy Directive is the precursor of today's general act, as well as the new ePrivacy Regulation, which should, in fact, be a *lex specialis* concerning GDPR. We turn our attention to Directive 95/46/EC, which largely determined – "paved the path" – for further development of legal prescripts in the EU considering data protection and the right to privacy – to General Data Protection Regulation. In that sense, we are concerned with the most substantial directive not only because a longstanding jurisprudence is based on it, but also because other directives represent an annex so as to enable their application in electronic communications area (Tomić & Petrović, 2009, pp. 95-97). We want to emphasize the importance of Directive 95/46/EC with the fact that it has provided basis for the new GDPR. So, to reiterate, we are dealing with the most important documents on an international level, whose orders were later incorporated into all national criminal laws of signatory countries and countries that ratified the relative documents.

This right is mentioned in over 150 national constitutions in the world (Right to privacy). The Constitution of Serbia[5] does not define the right to privacy in an explicite manner, but it does it in a way that guarantees the rights and freedoms through which that right is realized, meaning – it protects dignity and free personal development (Art. 23 of the Constitution), inviolability of psychological integrity (Art. 25 of the Constitution), inviolability of the home (Art. 40 of the Constitution), as well as the secrecy of letters and other means of conversation (Art. 41 of the

social, and economic rights for European Union (EU) citizens and residents into EU law. It was drafted by the European Convention and solemnly proclaimed on 7 December 2000 by the European Parliament, the Council of Ministers and the European Commission.

[4] Art. 8, Protection of personal data:

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

[5] See: *Sl. glasnik RS*, nos. 98/2006, 16/2022 Decision on the proclamation of the Constitutional law for the execution of Act on changing of the Constitution RS – Amendments I - XXIX: *Sl. glasnik RS*, no. 115/2021.The attention is drawn to the fact that, via the Act on Changing the Constitution from the year 1888, inviolability of the home and secrecy of letters and telegraphic despatches have been guaranteed.

Constitution). However, the extent of response differs when it comes to the protection of personal data because the Constitution in Art. 42 explicitly provides special guarantees, "The protection of personal data is guaranteed (para. 1). Law regulates gathering, keeping, processing, and use of personal data (para. 2). The use of personal data beyond the purpose for which they were gathered is forbidden and punishable by the law, except to conduct a criminal proceeding or for protection of the security of the Republic of Serbia, in the manner provided by law (para. 3). Everyone has the right to be informed on their gathered personal data, in accordance with the law, and the right to legal protection in case of their abuse (para. 4)."

In this segment of the protection of human rights and freedoms, our Constitution thoughtfully tended to resolutions of the Law of Personal Data Protection, 2018, (further LPDP), which had served as the basis during its construction (Prlja, 2018, pp. 92-96). Under the influence of GDPR, in November 2018, Serbia adopted LPDP, by which it recognized the principles and values of GDPR with slight variations, thus undoubtedly introduced immeasurably higher standards of personal data protection. Practical adoption of GDPR resolutions with the effects of actual "raising" of personal data protection to a higher level represents a significant step towards improving our legislature.

3. Unauthorized Gathering of Personal Data (Art. 146 CC)

Even those with superficial and incomplete knowledge of information communications technology understand that the criminal-legal problem of use and protection from abuse of data on an individual is of exceptional importance. From the previous observation, the right to privacy includes the right to personal information with regard to gathering, keeping, revealing, insight, or security from third parties and displaying via the internet, etc. On the other hand, the growing use of the internet and social media, as well as the use of computer technology in everyday life increase the possibility of their abuse in various, highly sophisticated ways... and the data that is gathered without authorization by abusing the information system can be manipulated in various ways. The massiveness of these abuses has evolved to greater lengths, and direct damages are unfathomable (Grazia, 2012). It should be particularly emphasized that significant efforts are being made to suppres these phenomena, both in the Republic of Serbia and worldwide.

In that context, the regulation of criminal-legal personal data protection in our legislation was executed by formulating and sanctioning the criminal act of "unauthorized gathering of personal data". This act represents a novelty in the 2005 CC RS, systemized in section XIV under the title "Criminal acts against

freedom and rights of man and citizen". Therefore, it is a new incrimination that was justifiably included in the legal text due to the perspective of changed situations, new demands, and the conflict of interests.

As our intention is to problematically develop the essence of this criminal notion, it is only natural that in the observation that follows, we will rely on the legal conceptualization:

(1) "Whoever collects personal data that is being gathered, processed, and used based on the law without authorization, communicates them to others, or uses them for a non-intended purpose, will be punished with a fine or imprisonment up to one year.
(2) Whoever unlawfully gathers the personal data of citizens and thus uses the collected data will be punished with sanction from para. 1 of this Article.
(3) If an official commits the act from para. 1, he/she will be punished by imprisonment for up to three years."

It should be kept in mind that this is a criminal offence of blank nature, which means that it requires provisions of another appropriate prescript, more precisely, the Law of Personal Data Protection (LPDP), whose implementation began in August 2019, to be thoroughly understood and applied.

1. a) From the legal provision of Art. 146, two basic forms of this criminal act (paras. 1 and 2) and a qualified one clearly arise (para. 3). The action of execution when it comes to the basic form is alternatively determined and consists of gathering, communication, use... Thus conceptualised, the criminal act of unauthorized gathering of personal data from Art. 146. CC can be committed only via one of the abovementioned actions, for only they constitute the substance of this criminal act. More precisely, this criminal act consists of multiple actions of execution, of which each one separately is enough for the execution of the act and the establishment of criminal responsibility, because the central element of the act is alternatively determined in Art. 146.

It is precisely on that "scale" of different modalities of actions of execution that we first come across "gathering" of personal data. "Arriving" to those data, realizing their content is also taken into account. It is of no significance how these data are obtained unless it represents a realization of another criminal act. Moreover, communicating the data to another person means introducing him/her to the content of the data, while the use of personal data for non-intended purposes means the use of personal data to achieve an aim for whose achievement they were not intended (Lazarević, 2011, p. 552).

b) The listed actions ought to be done without authorization, meaning that there was no legal basis for their gathering or communicating with another. Regarding their use for purposes that are forbidden, it is always unauthorized, since there cannot be legal authority for such an action (Lazarević, Vučković, B. & Vučković, V., 2004, p. 463). Along these lines, professor Z. Stojanović regards the execution of such actions without a legal basis as an abuse of personal data which can themselves be, under conditions determined by law, a matter of gathering, processing, and using for purposes specified by law (Stojanović, 2018, p. 538). In the case of such conduct in the processing of personal data, it is obvious that the CC refers to provisions of LPDP. Thus, the processing of personal data entails any automated or unautomated action which is undertaken regarding personal data. It includes gathering, recording, keeping, sorting, insight, deleting, storing, as well as all other actions which refer to personal data.[6]

During the process of alignment with the Law, but also later during the application of handling data, six principles of data processing must be constantly attended to. These are, in fact, the so-called "Holy Commandments" which entail that every procedure or rule in the processing of data must be in accordance with them. The mere failure to respect principles, without violating any other provision of the Law, can generate a misdemeanor responsibility and a fine. In that sense, the LPDP first prescribes that data processing must be legal (Arts. 12, 13, 14 ZZPL), fair an unconcealed (Art. 21 ZZPL), then limited to the purpose intended and the necessary data which must be protected and kept only for the amount of time necessary to achieve the purpose of processing (Stojanović, 2018, p. 538). Likewise, they must be timely updated and aligned with the possibly occurring of changes concerning the person whose data it is. From this perspective, the problem of defining the term "unauthorized gathering of personal data" is seen not only when it is done in disagreement with the principle of legality, but also when it is done in disagreement with other principles provided by law (unfair, concealed, etc.).

c) The object of the criminal act is personal data gathered, processed, and used based on law. From the point of view of general specification of personal data, as we have much emphasized, we again enter the "domain" of LPDP, which very precisely and fully defines personal data (Art. 4, para. 1, point 1 LPDP; Art. 4, para 1. points 14-16 of LPDP).

d) The act is committed by undertaking some of the listed actions, so no harmful consequences to the person whose data it is are necessary to follow for the act to exist.

What is necessary for the existence of this act, according to Art. 146 CC, is intent.

[6] *E.g.* merely keeping personal data on a server, with no insight, is enough to be considered as processed data and to apply the new law (Art. 3 LPD).

2. In the beginning we have said, and now repeat, that the action of this criminal act consists of three forms, two basic and one severe – qualified. We have seen that the first basic action shows certain distinctions, *i.e.* characteristic features. However, from a wider perspective, but also, above all, from a closer, a more detailed one, one can observe that the second basic form does not differ from the first, although the difference is insisted upon in the legal description of the criminal act. Precisely, the act from para. 2 appears in the same form as the act from para. 1. There are no crucial details to define it as different from the first basic form. Therefore, the essence of the second act and its relation to the previously analyzed act (from para. 1) remain unclear. This stance arises from the fact that the object of the act from para. 2 is personal data, and gathering and using should be executed "contrary to law", while para. 1 criminal act mentions the term "unauthorized", which is, again, contrary to the law. However, it might be that the core of the issue is that a certain singularity of this form is seen in the fact that it concerns the personal data of "citizens". Thus, the act from para. 2 could only be performed in relation to a single person, while the term "citizen" implicates multiple persons (Lazarević, 2011, p. 554; Lazarević, Vučković, B. & Vučković, V., 2004, p. 464).

With regard to other features, they are identical, displaying no distinction between them.

3. Para. 3 provides a qualified form of the act from para. 1. The qualifying circumstance is in the capacity of the executor, an authorized official. According to the provision of Act. 1, para. 3 of CC, an authorized official is one of the following: a person who performs official duties within the state body, an elected, appointed, or assigned person in the state body, a body of a local government, or a person who performs official duties in those bodies (constantly or occasionally), then a notary public, public enforcement agent and arbiter including persons in an institution, enterprise, or other establishments, who has been entrusted with the execution of public authority, who decides on rights, obligations, or interests of natural and legal persons or public interests, as well as a person who has been entrusted with the performance of certain official duties or tasks, and military personnel.

The specified circumstances must involve the intent of the offender (Lazarević, Vučković, B. & Vučković, V., 2004, p. 464).

By the execution of this criminal act, a substance of another criminal act, such as unauthorized tapping or audio recording from Art. 143 CC or the criminal act of disclosure of another's writings from Art. 145 CC can be realized. Then, the principle incorporates offence-inclusion with this criminal act, unless the act

represents a necessary way to commit another criminal act (Lazarević, Vučković, B. & Vučković, V., 2004, p. 464).

Para 3. of this Article of the CC provides heavier penalties for those who commit the act as an authorized official. In such cases, the competent public prosecutor's office takes over the criminal proceeding, *i.e.* persecution, while that is done after a private lawsuit, as is determined by Art. 153 of the CC. The competence for conducting a court proceeding for Art. 146 is entrusted to Basic Courts in the Republic of Serbia.

In light of all that has been said on the criminal act of unauthorized personal data gathering and their contents, it is necessary to make a few remarks in terms of certain incoherences or, let us say, inconsistencies on a unique level Constitution–CC –LDPD.

Firstly, our attention is drawn to a particular terminological incoherence between constitutional guarantees and the term of this criminal act. To illustrate: the Constitution guarantees the protection of personal data, while the criminal act is termed – the unauthorized gathering of data about a person, although this term is not defined by any provision (Krivičnopravna zaštita podataka o ličnosti u Republici Srbiji).

Along these lines, pointing to the internal content of this criminal act is crucial, for, in the name of the criminal act, only data about a person appears, and not personal data. Thus, another inconsistency of a terminological and essential nature is formed.

Likewise, when dealing with certain terminological and essential inconsistencies, what draws attention is that the action itself is comprehended within the name of the criminal act – unauthorized gathering of personal data – and the criminal act incriminated: unauthorized acquiring, communicating to others, or using personal data gathered and used based on the law for non-intended purposes, as well as gathering personal data contrary to law or using thus gathered data. Therefore, the gathering of data represents only one form of personal data processing, while other unauthorized processing actions mentioned above are included within this criminal act.

In the first paragraph of this act, incriminated actions of processing exclusively include personal data which are gathered, processed, and used based on law, while the second paragraph includes unlawful gathering and using of thus gathered personal data, regardless of which data it is about.

* * *

Even though we will not cover a detailed explanation of public prosecutor's office proceedings from the area of personal data protection in the Republic of Serbia, our particular approach to the consideration of the relative problem will partly be based on this analysis. Of course, only to the extent to which it will lead us to a more in-depth understanding of key problems and challenges in the application of criminal-legal protection of this right – a right for which we claim rests in the very centre of human freedom!?

So, are mechanisms of criminal law protection from the violation of this right effective in the Republic of Serbia, and what are the effects of adopting and adjusting to the new LPDP, in terms of judicial protection and sanctioning of right violation guaranteed by this law (after the first year of its application) (Mileusnić *et al.,* 2021, p. 12)?

In short, before the courts of Serbia (14 Basic Courts), from 2015 to July 2020, 28 cases for the criminal act from Art. 146 CC were formed, 26 cases were initiated by private lawsuits, while the remaining 2 were initiated by the act of indictment of the competent public prosecutor's office.

In 6 cases a decision was made to dismiss the petition, in 13 cases it was rejected, in 2 cases the decision of suspension was made, 2 cases were finalized by a guilty verdict, 4 cases reached acquittal, while one court altered the verdict and denied the charge against the accused. Furthermore, amongst the cases which were closed by an acquittal, one case was initiated by the act of indictment of the competent public prosecutor's office, and three by a private lawsuit. What also attracts attention is the fact that among cases that ended with a guilty verdict, two probations were ruled.

Only a superficial glance at these statistics plainly shows that a dramatically small number of cases of authorized personal data gathering were opened in the courts of Serbia. Namely, the number of 28 cases in this area since 2015 is evidently inconsistent with the frequency of violating the right to data protection in the same period relying on the results of a previous analysis – on only two guilty verdicts for Art. 146 CC and, what is more, probation. It is not even possible to declare whether the penalty policy of courts for this criminal act is mild or harsh. As the basic reason for such poor (devastating) statistics or, otherwise, why the mechanisms of personal data protection "failed", we can provide the fact that the criminal departments of courts in Serbia "have not received a case with a substantial violation of privacy, either in the sense of the severity of consequences for the injured party or in the number of injured parties" (Mileusnić *et al.,* 2021, pp. 11-20).

This certainly doesn't serve to transfer responsibility to the courts. On the contrary, the lack of this approach should be searched for outside the courts – having in mind the authorities for particular proceedings (Mileusnić *et al.,* 2021, pp. 11-20).

Relating to what was mentioned above, one of the reasons could be found in the small number of proceedings initiated by the public prosecutor's office, that is, the small number of indictments that the public prosecutor's offices direct to the courts. To illustrate: in the observed period which encompasses 5 years, only two cases had the public persecutor's office as the prosecutor (Mileusnić *et al.,* 2021, pp. 20-28).

In conclusion, adequate legal protection for the injured parties (the victims of personal data abuse) in terms of the protection of individuals and their privacy is absent. Unfortunately, it appears that in these, in many ways reckless, times the criminal law protection to the injured parties for violations from Art. 146 is neither efficient, nor effective (Mileusnić *et al.,* 2021, pp. 30-31). Arriving at the accurate explanation for this, ultimately negative, practice, the emphasis is on the following: not a single criminal charge filed to the Commissioner for information of public interest and personal data protection in the last five years has reached its epilogue. Likewise, the highest number of filed criminal charges for the relative criminal act ends in the public prosecutor's office due to it being statute-barred or with no outcome whatsoever, which practically undermines the criminal law protection for personal data abuse, as the constitution guarantees (Krivičnopravna zaštita podataka o ličnosti u Republici Srbiji).

4. Data Protection: Normative Basis for Action in the Countries of the Former Yugoslavia

We will round off the previous presentation on the criminal law protection of personal data with a presentation of the current situation in this area in the ex-Yugoslavia countries.

For our consideration, which we did on the occasion of the comparative presentation of the provisions on the protection of this, one of the fundamental, human rights, it must first of all be stated that the adopted solutions are conceptually very similar to each other, some even identical. But there are those who advocate different approaches in this regard. Let us go in order.

1. Criminal Code of the Republic of Slovenia, Chapter 14 – Criminal offenses against human rights and freedoms: Art. 143. Misuse of personal data: from the

wording of the criminal offense of misuse of personal data, it can be seen that this criminal offense fully belongs to computer crime because it is carried out over the internet. A criminal offense is committed by anyone who enters or accesses a computer database about a person without authorization with the aim of obtaining certain personal data for himself or someone else; who makes other people's personal data publicly available via the internet, and especially about victims of criminal acts, victims of violations of the rights and freedoms of protected witnesses, persons who are in the court files of court proceedings, as well as protected personal files about them in connection with court proceedings (*Uradni list*, no. 59/2012).

2. The Croatian Criminal Code, Chapter 14, Criminal offenses against privacy provides: (1) Whoever collects, processes or uses personal data of natural persons contrary to the conditions specified in the law, will be punished by imprisonment for up to one year. (2) Whoever, contrary to the conditions specified in the law, brings personal data from the Republic of Croatia for the purpose of further processing or publishes them or otherwise makes them available to others, or who by the action referred to in para. 1. of this article obtains a significant material benefit for himself or another or causes significant damage, shall be punished by imprisonment for up to three years. (3) With the penalty from para. 2. of this article will be punished who commits an act from para. 1. of this article, commits a crime against a child or who collects, processes or uses personal data of natural persons related to racial or ethnic origin, political views, religious or other beliefs, trade union membership, health or sex life and personal data of natural persons regarding criminal or misdemeanor proceedings. (4) If the criminal offense referred to in paras. 1. to 3. of this article committed by an official in the exercise of his powers, he shall be punished by imprisonment from six months to five years (*Narodne novine*, nos. 125/11, 144/12 … 84/21, consolidated text of the law made official on 31 July 2021).

3. Criminal Code of Bosnia and Herzegovina, Chapter XVII, Criminal offenses against the freedom and rights of man and citizen, Unauthorized use of personal data, Article 193: An official or responsible person in the Federation who, without the consent of an individual, collects, processes or uses his personal data or uses the data contrary to the legally permitted purpose of their collection, will be punished by a fine or a prison sentence of up to six months (*Sl. novine FBiH*, nos. 36/2003, ... 75/2017).

Other legislations have almost identical solutions to the Serbian legislative solution.

4. Criminal Code of Montenegro, Chapter XV, Criminal offenses against freedoms and rights of man and citizen. As we can see, this is also one of the criminal offenses that protect an individual's freedom of personality and his right to know all the information that concerns him. Unauthorized collection and use of personal data, Article 176: (1) Whoever unauthorizedly obtains personal data that is collected, processed and used on the basis of the law, communicates it to another or uses it for a purpose for which it was not intended, shall be punished by a fine or imprisonment of up to one year. (2) The punishment referred to in paragraph 1 of this article shall also be imposed on those who, contrary to the law, collect personal data of citizens or use such collected data. (3) Whoever takes over the identity of another person without authorization and under the name of that person uses one of his rights or gains a benefit for himself or another, or by using his identity interferes with the personal life of that person or orders his personal dignity or causes him any damage, shall be punished by imprisonment for up to one year. (4) If the act from paras. 1 and 3 of this article is committed by an official in the performance of his duties, he shall be punished by imprisonment from three months to three years (*Službeni list Republike Crne Gore*, nos. 070/03, ... 003/20).

5. Criminal Code of the Republic of Srpska, Chapter XIII – Criminal offenses against the freedoms and rights of citizens, Article 157: (1) Whoever, contrary to the conditions set forth in the law, without the consent of citizens, obtains, processes, communicates to others or uses their personal data, shall be punished by a fine or imprisonment up to one year. (2) Whoever enters another's protected computer database without authorization with the intention of using it to obtain a benefit for himself or another or to cause harm to another shall be punished with the penalty referred to in paragraph 1 of this article. (3) If the act from paras. 1 and 2 of this Article, is committed by an official by abuse of position or authority, he shall be punished by a prison sentence of six months to three years. (4) Attempted criminal offense from paras. 1, 2 and 3 of this article is punishable (*Službeni glasnik Republike Srpske*, nos. 64/2017, 104/2018 – decision of the Constitutional Court, 15/2021 and 89/2021).

6. The Criminal Code of the Republic of North Macedonia, Misuse of personal data, Article 149: (1) Whoever collects, processes or uses his personal data contrary to the conditions established by law without the consent of the citizen, will be punished with a fine or imprisonment for up to one year. (2) The penalty from paragraph 1 shall be imposed on the person who enters the computer information system of personal data with the intention of using it for himself or for another to achieve some benefit or to cause some damage to another. (3) If the

crime from paragraphs 1 and 2 is committed by an official in the performance of his duties, he will be punished with imprisonment from three months to three years. (4) The attempt is punishable. (5) If the offense of this article is committed by a legal entity, it will be punished with a monetary penalty (*Služben vesnik na RM*, nos. 80/1999 … 132/2014).

5. Conclusion

A grandiose development of information-communications technologies marked the age after the turn of the century. The internet and social media have, with no exaggeration, become a part of our daily lives, "permeating" every part of human being, every human gene. The process is active and drastically rising. A central position in the process is taken by the chip, *i.e.* microchip or bit. It is a way to biochips, artificial intelligence, robotization, digital communication, etc. We live in a world in which an immeasurable amount of data, movies, photos, and other materials is exchanged, posted on profiles, and made publicly available – in other words, they are turned into data that make new capital. Because digital network technologies have transformed this type of criminality, the society of the future will be forced to adopt a different concept of thinking which will increase both the complexity of investigations and crime prevention, while simultaneously expanding regulation challenges. Along these lines, not so long ago, laws that comprehensively treat this complex and very dynamic problem have been incorporated into our legal system. Thus, responses have been offered to the wide range of questions regarding data protection, the right to privacy, the right to freedom of opinion and expression, the freedom of the internet as a medium, and others. From our perspective, LPDP (which is practically a translated version of GDPR) came as the center of focus. Judicial protection guaranteed by this law comprehends the right of the individual of the relative personal data to initiate: an administrative dispute, a civil dispute (a suit for the protection of rights, a suit for damages compensation), as well as an offense proceeding. LPDP, however, does not treat the criminal law judicial protection in the case of "personal data abuse", like several laws which provide criminal acts from the areas they manage. Instead, this protection is regulated by the Criminal Code, which provides the criminal act of unauthorised gathering of personal data in Art. 146. Considering that this is an act of blank nature, it was necessary to "cross" from this general position to a special theoretical interpretation that arises from LPDP in order to contemplate its conceptual definition, that is, the complete understanding of its meaning and essence.

Lastly, we must emphasize that the right to privacy and protection of personal data is one of the rights of the foundation of human freedoms. It is inseparable from the character of a political system of a society. We are talking about a reciprocal influence because societies based on ideas such as the rule of law and human freedoms take the highest positions on the scale of respect for the privacy of citizens. On the contrary, in authoritarily "colored" societies, the concept of rule is directed towards the devastation of the private lives of citizens.

Our CC implemented norms of international law. On the one hand, it has achieved the fulfilment of all assumed obligations, and on the other, it has followed the regular standards of criminal law, and also applied solutions that correspond to the needs of our society and the legal system. However, relying on the results of the analysis of existing practice (which served as the basis for this conclusion), the right to privacy and personal data protection at the extent of their application shows its objectivity and effectiveness, which is yet to be improved both in the public and the private sector.

References

Bornes, S., 2006. A Privacy Paradox: Social Networking in the United States. *First Monday*, 11(9). Available at: http://firstmonday.org/article/viev/1394/1312, https://doi.org/10.5210/fm.v11i9.1394.

Diligenski, A. & Prlja, D. 2018. *Fejsbuk, zaštita podataka i sudska praksa*. Beograd: Institut za uporedno pravo.

Hadson, L.D. 2010. *The Right to Privacy.* New York: Infobase Publishing.

Ilić, m.B. 2016. *Povreda prava na privatnost zloupotrebom društvenih mreža kao oblik kompjuterskog kriminaliteta.* Doktorska disertacija. Niš: Pravni fakultet Univerziteta u Nišu.

Lazarević, Lj. 2011. *Komentar Krivičnog zakonika*. Beograd: Pravni fakultet Univerziteta Union u Beogradu i JP Službeni glasnik.

Lazarević, Lj., Vučković, B. & Vučković, V. 2004. *Komentar KZ Crne Gore*. Cetinje: Obod.

Mileusnić, D., Ćurčić D., Tasić D. *et al*. 2021. *Privatnost i zaštita podataka o ličnosti u Srbiji, Analiza odabranih sektorskih propisa i njihove primene*. Beograd: Partneri za demokratske promene Srbija (Partneri Srbija).

Popović, D. & Jovanović, M. 2017. *Pravo interneta – odabrane teme*. Beograd: Pravni fakultet Univerziteta u Beogradu.

Prlja, D. & Reljanović, M. 2009. Sybercrime - Comparative experiences. *Strani pravni* život, 65(3), pp. 161-184.

Prlja, S. 2018. Pravo na zaštitu ličnih podataka u EU. *Strani pravni život*, 62(1), pp. 89-99, https://doi.org/10.5937/spz1801089P.

Stojanović, Z. 2018. *Komentar Krivičnog zakonika*. Beograd: Službeni glasnik.

Summers, S. 2015. EU Criminal Law and the Regulation of Information and Communication Technology. *Bergen Journal of Criminal Law and Criminal Justice*, 1, https://doi.org/10.15845/bjclcj.v3i1.827.

Tomić, N. & Petrović, D. 2009. *Društveno umrežavanje i zaštita privatnosti korisnika interneta*, Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju, Beograd: Saobraćajni fakultet Univerziteta u Beogradu.

Vodinelić, V.V. 2012. *Građansko pravo, Uvod u građansko pravo i opšti deo građanskog prava,* Beograd: Pravni fakultet Univerziteta Union i JP Službeni glasnik.

Legal Sources

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L 281, 23.11.1995, p. 31.

European Convention on Human Rights, of the Council of Europe (1949) on the protection of freedoms and rights, adopted in Rome, Italy, on November 4, 1950.

International Covenant on Civil and Political Rights, United Nations General Assembly. Resolution 2200A (XXI) of December 16, 1966.

Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications, otherwise known as ePrivacy Directive (ePD), is an EU directive on data protection and privacy in the digital age, L201, 2002-07-31, pp. 37–47.

Službeni glasnik RS, no,. 98/2006, 16/2022 Decision on the proclamation of the Constitutional law for the execution of Act on changing of the Constitution RS – Amendments I - XXIX: *Sl. glasnik RS*, no. 115/2021. The attention is drawn to the fact that, via the Act on Changing the Constitution from the year 1888, inviolability of the home and secrecy of letters and telegraphic despatches.

The Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights, was opened for signature in Rome on 4 November 1950 and came into force on 3 September 1953.

The Charter of Fundamental Rights of the European Union (CFR) enshrines certain political, social, and economic rights for European Union (EU) citizens and residents into EU law. It was drafted by the European Convention and solemnly proclaimed on 7 December 2000 by the European Parliament, the Council of Ministers and the European Commission.

The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data is a 1981 Council of Europe treaty that protects the right to privacy of individuals, taking account of the increasing flow across frontiers of personal data undergoing automatic processing.

The ePrivacy Regulation (ePR) is a proposal for the regulation of various privacy-related topics, mostly in relation to electronic communications within the European Union. Its full name is "Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

Universal Declaration of Human Rights - the United Nations, 1948.

Kazneni zakonik Republike Slovenije (*Uradni list*, no. 59/2012).

Kazneni zakon Hrvatske (*Narodne novine*, nos. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, consolidated text of the law made official on July 2021).

Krivični zakon Bosne i Hercegovine (*Sl. novine FBiH*, nos. 36/2003, 21/2004 – correction notice, 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 and 75/2017).

Krivični zakonik Crne Gore (*Službeni list Republike Crne Gore*, nos. 070/2003, 013/2004, 047/2006, *Službeni list Crne Gore*, br. 040/2008, 025/2010, 073/2010, 032/2011, 064/2011, 040/2013, 056/2013, 014/2015, 042/2015, 058/2015, 044/2017, 049/2018, 003/ 2020).

Krivični zakonik Republike Srpske (*Službeni glasnik Republike Srpske*, nos. 64/2017, 104/2018 - decision of the Constitutional Court, 15/2021 and 89/2021).

Kривičen zakonik na Republika Makedonija (*Služben vesnik na RM*, nos.80/1999…132/2014).

Website References

Stallman, R. 2011. Mobilni telefoni su Staljinov san. Sajt *B92*. Available at:. http://www.b92.net/tehnopolis/vesti.php?yyyy=2011&=038nav_id=499267, (19. 7. 2012).

Right to Privacy. Available at: https://cic.gov.in/sites/default/files/Right%20 to%20Privacy%20 and%20RTI %20by% 20Aditya%20Verma%20%20 %281%29%20%281%29.pdf, (30. 3. 2018).

Grazia, M. 2012. Data Protection and the Prevention of Cybercrime: The EU as an area of security?. Available at: https://cadmus.eui.eu/handle/1814/23296, (27. 3. 2022).

Petrović, Z., Krivičnopravna zaštita podataka o ličnosti u Republici Srbiji, *LAW-Life* portal za pravo i privredu. Available at: https://lawlife.rs/index.php/pravo/144-krivicnopravna-zastita-podataka-o-licnosti-u-republici-srbiji, (15. 9. 2022).

What is IT law, ICT law or Cyber law?. Available at: https://www.michalsons.com/blog/what-is-it-law-ict-law-or-cyber-law/286, (17. 12. 2021).

Cybercrime law around the world | Links and updates. Available at: https://www.michalsons.com/focus-areas/cybercrime-law, (14. 10. 2021).

Dragana B. Petrović
Naučni saradnik, Institut za uporedno pravo, Beograd, Srbija
E-mail: *d.petrovic@iup.rs*

PRIVATNOST I ZAŠTITA PODATAKA O LIČNOSTI – KRIVIČNO-PRAVNI ASPEKT

Sažetak

Danas se u svetu na različitim nivoima vode ozbiljne rasprave o mogućnostima modernih informaciono-komunikacionih tehnologija (ICT) uključujući i internet, ali i o njihovim neželjenim posledicama. Za običnog čoveka „nov" način komunikacije preko interneta i mobilne telefonije je istovremeno lak, jednostavan, brz, nužan – postaje činjenica njegovog svakodnevnog života. Štaviše, savremeno doba podrazumeva internet kao jedno od glavnih sredstava komunikacije. Ukoliko se koristi „kako treba", predstavlja izobilje informacija na gotovo svaku temu i donosi mnoge benefite. Uz ogromnu i raznovrsnu količinu prikupljenih podataka, s lakoćom posreduje u sticanju novih znanja i oblikovanju životnog stila. Ali, korišćenje modernih tehnologija koje se neprekidno transformišu, do mere da potpuno promene i automatizuju gotovo sve aspekte ljudske delatnosti, ima i svoju tamnu, rušilačku stranu. U toj perspektivi život u internet mreži postaje sve više prostor podložan manipulacijama i zloupotrebama. A spisak zloupotreba je dug... od toga da se ove tehnologije mogu zloupotrebiti kao baza podataka do napada na tuđu privatnost, proganjanja, sajber mobinga, vršnjačkog nasilja, seksualnog uznemiravanja i nasilja, trgovine ljudima i ljudskim organima i dr. Na taj način, precizira se stav: pojava novih tehnologija značajno ugrožava pravo na privatnost. Poslednjih godina se pravo na privatnost u najvećoj meri dovodi u vezu sa podacima o ličnosti, pa u tom pravcu, kada se govori o privatnosti, to se gotovo uvek čini u kontekstu obrade podataka o ličnosti. Pravo na privatnost i zaštita ličnih podataka spadaju u red osnovnih ljudskih prava, pa budući da se radi o temeljnom pravu čoveka i građanina, osnov njegove zaštite u našem zakonodavstvu sadržan je, pre svega, u Ustavu, Zakonu o zaštiti podataka (ZZLP) i Krivičnom zakoniku (čl. 146. Neovlašćeno prikupljanje ličnih podataka). Kao što iz naslova proizilazi, krivičnopravni aspekt privatnosti i zaštite podataka o ličnosti predviđen odredbom člana 143 KZ nalazi se u fokusu ovog rada. U tom kontekstu, autorka se, najpre upustila u analizu postojećeg stanja ugroženosti prava na privatnost kao pretpostavke za delovanje u pravcu njegove zaštite. Napuštajući opšte razmatranje te vrste, ispitivanje je zatim usmereno na

konkretno objašnjavanje smisla i suštine krivičnog dela Neovlašćeno prikupljanje ličnih podataka, formi u kojima se ono ispoljava, krivične odgovornosti i kažnjivosti onoga ko je učinio ovo delo. Uz konstataciju da je ovde reč o realnosti koja se dinamično menja, posebno su istaknuti i neki od ključnih problema i izazova u primeni odgovarajućih mehanizama zaštite prava na privatnost u Republici Srbiji (sa posebnim akcentom u godini iza nas). Na ovaj način obeležen je i osnovni problem u pogledu zaštite ovog prava, jednog od onih prava koja se nalaze u temelju ljudskih sloboda.

Ključne reči: informacione tehnologije, internet, privatnost, zaštita podataka o ličnosti, Krivični zakonik.

Primljeno: 10. 11. 2022.
Izmenjeno: 12. 12. 2022.
Prihvaćeno: 30. 12. 2022.