Chapter VI

Privacy and Data Protection in Serbian Law: Challenges in the Digital Environment

Dušan V. Popović

1. Introductory remarks

In the Republic of Serbia, as in other jurisdictions, there is no unanimously accepted definition of the privacy, either in legal doctrine or in legislative instruments. The national constitutions, including the Serbian one, usually protect the privacy of individuals by referring to: (1) the inviolability of home; (2) the confidentiality of letters and other means of communication; and (3) the protection of personal data. More extensively defined, the right to privacy may also encompass the freedom of thought, conscience, and religion, in the sense that the citizens do not have the obligation to declare their religious or other beliefs. The omnipresence of the Internet, and in particular social networks, search engines and cloud computing, has led to reducing the right to privacy to the right of personal data protection. Indeed, in the digital world, an individual is often reduced to data. Therefore, protecting one's privacy in the digital context means protecting data relating to an identifiable individual. The concept of personal data encompasses not just names, addresses and identification numbers, but also all data that can be traced back to an individual, such as photos, profiles on social networks or browsing history. Typically, social network websites contain user information such as age, relationship status, income, and information about close family members, as well as registered users' addresses. Many online service providers

Dušan V. Popović (2023) Privacy and Data Protection in Serbian Law: Challenges in the Digital Environment. In: Marcin Wielec (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice,* pp. 199–234. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2023.mwrtpida_6

store personal data about users so that users do not have to re-enter them each time they access the website, e.g., for online shopping, booking travel, etc. More recently, smart devices connected to the Internet, surveillance cameras, and automated decision-making based on online behavior history has raised privacy concerns across the globe. A recent survey revealed that only 7.5% of Internet users in Serbia believe that their personal data is protected online. Moreover, only 20% of Internet users in Serbia believe that it is even possible to protect privacy in the digital environment.[1]

Given the fact that the Republic of Serbia is a member of the Council of Europe and an EU candidate country, its legal system, including the rules on privacy protection, needs to be aligned to that of the Council of Europe and the European Union. However, with respect to the right to privacy, these two international organizations do not have a fully harmonized approach. Both the European Convention on Human Rights, a Council of Europe instrumen, signed in 1950 (ECHR), and the Charter of Fundamental Rights of the European Union, which was declared in 2000, and came into force in 2009 along with the Treaty of Lisbon (EU Charter), have a provision on privacy.[2] Art. 8 of the ECHR and similarly Art. 7 of the EU Charter provide that everyone has the right to respect for his or her private and family life, home, and communications. Moreover, Art. 8 of the EU Charter specifically addresses the fundamental right to the protection of personal data. Consequently, the EU Charter distinguishes data protection from privacy, and lays down some specific guarantees of personal data protection.[3] At the same time, the European Court of Human Rights (hereinafter, the ECtHR) has applied Art. 8 of the ECHR (covering the right to privacy) to give rise to a right of data protection as well. These legal developments raise the question of whether the right to data protection is only a subset of the right to privacy, or whether it provides additional protection.[4] A number of authors consider that, at least within EU law, data protection has gradually been disconnected from the right to privacy, by being regulated on an ever higher regulatory level and through ever more detailed legal regimes.[5] It seems that the approach of the Serbian legislature is similar to that of the EU, given the fact that the constitutional right to data protection is regulated separately from the right to privacy *stricto sensu*.[6]

The chapter begins with an analysis of the international obligations of the Republic of Serbia in privacy and personal data protection, stemming predominantly from the UN legal instruments, the European Convention on Human Rights and

1 Mitrović, 2020, p. 17.

2 Rights derived from international law are referred to as human rights, while rights derived from domestic constitutional law, as well as from European law, are referred to as fundamental rights.

3 Kokott and Sobotta, 2013, p. 222; Oostven and Irion, 2018, p. 9.

4 Ibid.

5 See for example van der Sloot, 2017, p. 8.

6 Constitution of the Republic of Serbia, Official Journal of the Republic of Serbia 98/2006, Arts. 40–42.

the Stabilization and Association Agreement concluded between the EU and Serbia (Section 2). A brief presentation of the existing legal framework for the protection of right to privacy in the Republic of Serbia follows (Section 3), then the right to privacy is analyzed as a value (Section 4). The right to privacy is undoubtedly a value protected by the Constitution, which leads us to explore the fundamental grounds for protecting the right to privacy (Section 5). The right to privacy, and more specifically the integrity of human person and family life, as well as other rights pertaining to a person, enjoy protection in civil law as well (Section 6). In criminal law, the right to privacy is protected by the Penal Code of the Republic of Serbia, which prescribes several types of criminal offences directly or indirectly related to the breach of privacy (Section 7). In Serbian administrative law, a specific mechanism for the protection of personal data has been established under the auspices of the Commissioner for Information of Public Importance and Personal Data Protection (Section 8). It is expected that further expansion of digital technologies shall require additional legislative efforts, particularly in mass surveillance and protection of children (Section 9). An overall assessment of the Serbian privacy and data protection system has been laid out in the final section of the paper (Section 10).

2. International obligations of the Republic of Serbia in privacy and personal data protection

The international obligations of the Republic of Serbia in privacy and personal data protection emanate from the country's membership in the United Nations and the Council of Europe, as well as from its EU candidate status. Under Art. 12 of the Universal Declaration of Human Rights, proclaimed by the United Nations General Assembly in Paris on December 10, 1948, no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to attacks upon their honor and reputation. The Federal People's Republic of Yugoslavia was not among the signatories of the Universal Declaration of Human Rights in 1948. Although the Universal Declaration is not a legally binding treaty, it is an expression of the fundamental values which are shared by all members of the international community. Moreover, it has had a profound influence on the development of international human rights law. Some argue that because countries have consistently invoked the Universal Declaration in the past decades, it has become binding as a part of customary international law.[7] In 1971, also under the auspices of the United Nations, the Socialist Federal Republic of Yugoslavia

7 Dimitrijević and Paunović, 1997, pp. 69–71.

ratified the International Covenant on Civil and Political Rights.[8] Under Art. 17 of the International Covenant, no one is to be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor and reputation. The International Covenant also prescribes that everyone has the right to the protection of the law against such interference or attacks.

For most European countries, and for Serbia as well, the membership in the Council of Europe represents the main international pillar for the protection of privacy and personal data. The Republic of Serbia became member of the Council of Europe on April 3, 2003, and ratified the European Convention on Human Rights (formally: Convention for the Protection of Human Rights and Fundamental Freedoms) on March 3, 2004.[9] Under Art. 8 of the ECHR, everyone has the right to respect for his private and family life, his home, and his correspondence. Public authorities should not interfere with the exercise of this right except when such interference is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. The Republic of Serbia also ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[10] and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows.[11] The Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data, and which seeks to regulate at the same time the transfrontier flow of personal data. On the other hand, the Additional Protocol provides for the setting up of national supervisory authorities responsible for ensuring compliance with laws or regulations adopted in pursuance of the convention, concerning personal data protection and transborder data flows. It also concerns transborder data flows to third countries. Data may only be transferred if the recipient state or international organization is able to afford an adequate level of protection. Finally, the Republic of Serbia ratified the Protocol amending the Convention for the Protection

8 Official Journal of the SFR Yugoslavia 7/71.

9 Law on the ratification of the Convention for the Protection of Human Rights and Fundamental Freedoms, Official Journal of Serbia and Montenegro 9/2003, 5/2005 and 7/2005; Official Journal of the Republic of Serbia 12/2010 and 10/2015.

10 ETS No. 108. Law on ratification of the Convention for the protection of individuals with regard to automatic processing of personal data, Official Journal of the FR Yugoslavia 1/1992; Official Journal of Serbia and Montenegro 11/2005. Law on amendments of the Law on ratification of the Convention for the protection of individuals with regard to automatic processing of personal data, Official Journal of the Republic of Serbia 12/2010.

11 ETS No. 181. Law on ratification of the Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, Official Journal of the Republic of Serbia 98/2008.

of Individuals regarding Automatic Processing of Personal Data[12], which has not yet entered into force.[13]

The Republic of Serbia is a country aspiring to join the European Union. In the process of European integration, Serbia signed the Stabilization and Association Agreement with the EU (hereinafter, the SAA)[14] in 2008.[15] Under Art. 81 of the SAA, dedicated entirely to the personal data protection, Serbia is required to harmonize its legislation concerning personal data protection with EU law and other European and international legislation on privacy upon the entry into force of the SAA. Serbia is also required to establish one or more independent supervisory bodies with sufficient financial and human resources to efficiently monitor and guarantee the enforcement of national personal data protection legislation. Further to this, within the statistical cooperation with the EU, Serbia is required to ensure the confidentiality of individual data.[16] The reason for harmonization of the national legal framework with EU rules on personal data protection is to be found in the preamble of the SAA, in which the parties to the agreement reaffirmed their commitment to respect human rights and the rule of law. One of the aims of the SAA is to support the efforts of Serbia to develop its economic and international cooperation, including through the approximation of its legislation to that of the EU.[17] The respect for democratic principles and human rights as proclaimed in the Universal Declaration of Human Rights and as defined, *inter alia*, in the ECHR form the basis of the domestic and external policies of the parties to the SAA and constitute essential elements of this Agreement.[18] To comply with the requirements of the SAA, Serbia adopted its first modern Law on Protection of Personal Data in 2008, adopted the Strategy for personal data protection in 2010[19] and established an independent supervisory body—the Commissioner for Information of Public Importance and Personal Data in 2009.[20]

12 CETS No. 223. Law on ratification of the Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data, Official Journal of the Republic of Serbia 4/2020.

13 As of February 2022.

14 Stabilization and Association Agreement between the European Communities and their Member States of the one part, and the Republic of Serbia, of the other part, Official Journal of the European Union L 278, 18.10.2013.

15 The SAA entered into force on September 1, 2013.

16 Art. 90 of SAA.

17 Art. 1, para. 2 d) of SAA.

18 Art. 2 of SAA.

19 Official Journal of the Republic of Serbia 58/2010.

20 On November 5, 2004, the National Assembly of the Republic of Serbia adopted the Law on Free Access to Information of Public Importance. The Law established an independent supervisory body—the Commissioner for Information of Public Importance. On 1 January 2009, following the entry into force of the 2008 Law on Personal Data Protection, the tasks related to protection of personal data were included in the Commissioner's scope of work. For a more detailed analysis of the national legal framework see Section 3 of this chapter.

3. National legal framework for the privacy and personal data protection

The right to privacy enjoys constitutional protection in Serbian legal system. The Constitution of the Republic of Serbia protects the right to privacy in at least two aspects. First, it protects the inviolability of home. Second, it protects the confidentiality of letters and other means of communication. Further to this, the Constitution enshrines the right to personal data protection.[21] The right to personal data protection and the right to privacy should not be considered identical. There are considerable overlaps in the scope of both rights, but also some areas where their personal and substantive scope diverge.[22]

In line with the trends in comparative law, the Serbian legislature predominantly intervened in personal data protection over the area of "traditional" privacy protection, by means of numerous laws and by-laws. The main piece of legislation currently regulating personal data protection in the Republic of Serbia is the Law on Protection of Personal Data (LPPD),[23] adopted in November 2018 and applicable since August 2019.[24] The 2018 LPPD replaced the previous law, adopted in 2008, which was the first modern legislative act regulating exclusively personal data protection.[25] The main reason for adopting the 2018 LPPD was the need to harmonize the Serbian legal framework with the European Union's General Data Protection Regulation (GDPR).[26] The LPPD applies to the processing of personal data wholly or partly by automated means, as well as to processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Also, the LPPD applies to the processing of personal data performed by a controller or a processor who has its business seat/place of residence in the territory of the Republic of Serbia, within the framework of activities performed in the territory of the Republic of Serbia, regardless of whether the processing takes place in the territory of the Republic of Serbia.

21 Constitution of the Republic of Serbia, Official Journal of the Republic of Serbia 98/2006, Arts. 40–42.

22 See Section 5 of this chapter.

23 Official Journal of the Republic of Serbia 87/2018.

24 The LPPD entered into force on November 21, 2018, but its application started nine months from the date of its entry into force, i.e., on August 21, 2019.

25 Official Journal of the Republic of Serbia 97/08, 104/09, 68/12 and 107/12. The first attempts to regulate personal data protection in Serbia were made in 1998, when the Law on Personal Data Protection was passed (Official Journal of the FR Yugoslavia 24/98 and 26/98). However, that law remained "dead letter," since only a few marginal cases of its enforcement were recorded. For that reason, the year 2008 is acknowledged as the beginning of a modern Serbian data protection law.

26 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L119, 4.5.2016.

Further to the LPPD, the Serbian data protection legislation includes the following by-laws:

(1) Rulebook on the manner of prior review of personal data processing,[27] which governs the procedure for notifying and approval by the relevant authority of intended personal data processing;
(2) Decree on the form for and manner of keeping records of personal data processing,[28] which regulates the form for keeping records of data, personal data processing, and the manner of keeping records of personal data processing;
(3) Rulebook on the form and manner of keeping record of the Data Protection Officer,[29] which defines the form and manner of keeping record of the Data Protection Officers;
(4) Rulebook on the form and manner of keeping internal record of violations of the LPPD and measures undertaken in the course of inspection supervision;[30]
(5) Rulebook on the form of notification on personal data breach and manner of notifying the Commissioner for Information of Public Importance and Protection of Personal Data;[31]
(6) Rulebook on the complaint form,[32] which defines the complaint form that a natural person can submit to the Commissioner if he or she considers that the processing of his or her personal data has been carried out contrary to the provisions of the LPPD;
(7) Decision on the list of types of personal data processing operations for which an assessment of the impact on the personal data protection must be performed and the opinion of the Commissioner for Information of Public Importance and Personal Data Protection must be sought;[33]
(8) Decision on the list of countries, parts of their territories or one or more sectors of certain activities in those countries and international organizations where it is considered that an adequate level of protection of personal data is ensured;[34]
(9) Decision on determining standard contractual clauses,[35] which determines the standard contractual clauses in the contractual relation between a controller and processor; and

27 Official Journal of the Republic of Serbia 35/2009.
28 Official Journal of the Republic of Serbia 50/2009.
29 Official Journal of the Republic of Serbia 40/2019.
30 Ibid.
31 Ibid.
32 Ibid.
33 Official Journal of the Republic of Serbia 45/2019, 112/2020.
34 Official Journal of the Republic of Serbia 55/2019.
35 Official Journal of the Republic of Serbia 5/2020.

(10) Rulebook on the form of identification card of the authorized person for performing inspection supervision in accordance with the LPPD.[36]

The LPPD is an "umbrella regulation" in the field of personal data protection in Serbia. Sectoral laws also apply to personal data processing in particular areas. The LPPD lays down general rules on personal data protection, while other laws may prescribe specific legal regimes applicable in certain areas or for certain type of activities. However, the principle *lex specialis derogate legi generali* does not apply, since the LPPD explicitly requires that the provisions of other laws regulating the processing of personal data must be in line with the LPPD.[37] There are numerous sectoral laws adopted in the last fifteen years in Serbia:

(1) Law on Electronic Communications[38] regulates interception of communications;
(2) Law on Electronic Commerce[39] regulates electronic marketing;
(3) Law on Consumer Protection[40] regulates electronic marketing;
(4) Law on Advertising[41] regulates electronic marketing;
(5) Law on Patients' Rights[42] regulates the duty of health professionals to keep the patients' personally identifiable information confidential;
(6) Labor Law[43] regulates the processing of personal data within the employment sector;
(7) Law on Labor Records[44] regulates the collecting of the personally identifiable data in the employment sector;
(8) Law on Healthcare Documentation and Healthcare Records[45] regulates the collecting of the personally identifiable information in the healthcare sector;
(9) Law on High Education[46] regulates the processing of the personally identifiable information within the sector of higher education;
(10) Law on the Education System[47] regulates the processing of the personally identifiable information within the education sector;

36 Official Journal of the Republic of Serbia 61/2019.
37 Art. 2, para. 2 of LPPD.
38 Official Journal of the Republic of Serbia 44/2010, 60/2013, 62/2014 and 95/2018.
39 Official Journal of the Republic of Serbia 41/2009, 95/2013 and 52/2019.
40 Official Journal of the Republic of Serbia 88/2021.
41 Official Journal of the Republic of Serbia 6/2016 and 52/2019.
42 Official Journal of the Republic of Serbia 45/2013 and 25/2019.
43 Official Journal of the Republic of Serbia 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017, 113/2017 and 95/2018.
44 Official Journal of the FR Yugoslavia 46/96; Official Journal of the Republic of Serbia 101/2005 and 36/2009.
45 Official Journal of the Republic of Serbia 123/2014, 106/2015, 105/2017 and 25/2019.
46 Official Journal of the Republic of Serbia 88/2017, 73/2018, 27/2018, 67/2019, 6/2020, 11/2021, 67/2021 and 67/2021.
47 Official Journal of the Republic of Serbia 88/2017, 27/2018, 10/2019, 27/2018, 6/2020 and 129/2021.

(11) Law on Pension and Disability Insurance[48] regulates the collecting of the personally identifiable information within the sector of pension and disability insurance; and
(12) Law on Health Insurance[49] regulates the collecting of the personally identifiable information within the health insurance sector.

The right to privacy enjoys protection in civil law. Under Art. 157 of the Law on Contracts and Torts (LCT),[50] everyone is entitled to demand that the court or other competent authority order the cessation of an action by which the integrity of an individual and integrity of family life, as well as other rights pertaining to a person, is violated. In case of a violation of privacy, the general principles of civil wrongs (torts) shall apply.[51] More specifically, with respect to the data protection right, the LPPD explicitly provides for an individual's right to receive compensation from the controller or processor for the material or nonmaterial damage suffered.[52]

The right to privacy enjoys protection in criminal law, as well. The Penal Code of the Republic of Serbia (PC)[53] prescribes several criminal offences that are directly or indirectly in relation to the breach of privacy:

(1) violation of privacy of letter and other mail (including emails);[54]
(2) violation of a home;[55]
(3) illegal search of an apartment, premises or person;[56]
(4) unauthorized disclosure of a secret;[57]
(5) unauthorized wiretapping and recording;[58]
(6) unauthorized photographing;[59]
(7) unauthorized publication and presentation of another's texts, portraits and recordings;[60]
(8) unauthorized collection of personal data;[61]

48 Official Journal of the Republic of Serbia 34/2003, 64/2004, 84/2004, 85/2005, 101/2005, 63/2006, 5/2009, 107/2009, 101/2010, 93/2012, 62/2013, 108/2013, 75/2014, 142/2014, 73/2018, 46/2019, 86/2019 and 62/2021.
49 Official Journal of the Republic of Serbia 25/2019.
50 Official Journal of the SFR Yugoslavia 29/78, 39/85, 45/89 and 57/89; Official Journal of the FR Yugoslavia 31/93; Official Journal of Serbia and Montenegro 1/2003; Official Journal of the Republic of Serbia 18/2020.
51 Arts. 154–155, 158–161, 164–169, 185–186, 198–205 of LCT.
52 Art. 84 of LPPD.
53 Official Journal of the Republic of Serbia 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019.
54 Art. 142 of PC.
55 Art. 139 of PC.
56 Art. 140 of PC.
57 Art. 141 of PC.
58 Art. 143 of PC.
59 Art. 144 of PC.
60 Art. 145 of PC.
61 Art. 146 of PC.

(9) dissemination of information on personal and family life;[62]
(10) showing, procuring, and possessing pornographic material of minors;[63]
(11) abuse of computer networks or other technical means of communication for committing criminal offences against sexual freedom of the minor;[64]
(12) unauthorized access to computer, computer network or electronic data processing;[65]
(13) unauthorized use of a computer or computer network;[66] and
(14) violation of confidentiality of proceedings.[67]

Further to criminal liability, several laws prescribe penalties for misdemeanors. For example, if the personally identifiable information has not been collected or processed lawfully, the LPPD empowers the Commissioner for Information of Public Importance and Personal Data to impose pecuniary fines for misdemeanors or to initiate misdemeanor proceedings before the competent court.[68] In such a case, the provisions of the Law on misdemeanors[69] must be observed.

The legal framework for the protection of privacy and personal data in the Republic of Serbia includes administrative remedies as well. Under the LPPD, the data subject (natural person whose personal data is processed) has the right to lodge a complaint before the Commissioner for Information of Public Importance and Personal Data, if they believe that the processing of their personal data was performed contrary to the law. Data subject, data processor or any other natural or legal person concerned by the Commissioner's decision may initiate an administrative dispute, within 30 days following the receipt of such decision.[70] Administrative disputes fall under jurisdiction of the Administrative Court and are conducted pursuant to the Law on administrative disputes.[71]

Although the Republic of Serbia is not an EU Member State, the European Union's General Data Protection Regulation may, under specific circumstances, be applicable in the Serbian context. Under Art. 3.2 of the GDPR, the regulation applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether

62 Art. 172 of PC.
63 Art. 185 of PC.
64 Art. 185b of PC.
65 Art. 302 of PC.
66 Art. 304 of PC.
67 Art. 337 of PC.
68 See for example Arts. 79, 95 of LPPD. The Commissioner may impose pecuniary fines for misdemeanors directly in case the latter are prescribed in fixed amounts. However, if the amount of a fine depends on the assessment of circumstances of the breach, i.e., there is a range prescribed by the law, the Commissioner must initiate misdemeanor proceedings before the competent court.
69 Official Journal of the Republic of Serbia 65/2013, 13/2016, 98/2016, 91/2019 and 91/2019.
70 Art. 83 of LPPD.
71 Official Journal of the Republic of Serbia 111/2009.

a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union.[72] This means that companies that have a connection with the European market must follow the same standard of data protection practiced by European companies.[73]

4. Privacy as a value

Privacy is a concept which is widely regarded as contested. As sociologist Alan Westin said, "Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists."[74] Privacy is a relatively modern concept, whose importance increased with the development of digital technologies. Since 1970s, the growing use of mainframe computers by states and large corporations, convened experts and policy-makers to explore the risks and develop protections for privacy. The use of computers and in particular the Internet have "commercialized" areas which were previously the individual domain. The omnipresence of both traditional and social media transformed the way we conduct our everyday activities. The information about our habits, our actions, and our beliefs are systematically being collected by various actors. Furthermore, such information may instantly be made accessible to a worldwide audience. Living in "a state of permanent visibility" highlights the importance of protection of privacy and personal data.[75]

There are different theoretical approaches to the concept of privacy. The "skeptical" approach sees privacy as a parasitic interest which derives its value from other more fundamental entitlements. Under this reductionist view, privacy claims should be more properly characterized as assertions of other interests; in particular, property rights, and rights in respect of the person.[76] The lighter "skeptical" theory does not see the privacy as a concept without value, but rather as an individual's interest in maintaining exclusivity over his or her body or property. Contrary to reductionist theories, intuitionism suggests the existence of a consensus that privacy has value, but it is unable to authoritatively determine what that value practically entails.[77] The intuitionist approach to this concept has led to different definitions of privacy, one of them being "the right to be let alone." This

72 For a more detailed analysis of extraterritorial application of the GDPR, see Greze, 2019, pp. 109–128.
73 Jaeger Junior and Copetti Cravo, 2021, p. 367.
74 Westin, 1967, p. 5.
75 Delany and Carolan, 2008, p. 1.
76 Ibid. p. 4.
77 Ibid. p. 6.

definition has been particularly influential in the constitutional sphere, where it has been frequently invoked in support of individual's claims to freedom from the state's intervention. However, a right to privacy which would apply only against the state does not offer the individual adequate protection. It is too narrow to capture the potential range of privacy infringement, since privacy interests may be undermined by non-public (non-state) actors.[78] Nevertheless, the definition of privacy as "the right to be let alone" need not necessarily be interpreted restrictively. It could be understood as a shield not only against the state actors, but against everyone. Another intuitionist approach to privacy defines it in terms of individual's inaccessibility. The simplistic interpretation of this definition would mean that when an individual is out of reach of all external actors, he or she is said to be enjoying "perfect privacy."[79] Finally, an intuitionist approach to privacy may lead us to understanding it as specific "natural" zones within which privacy interests arise and ought to be protected. These natural areas are usually identified as the home and the body.[80]

The analysis of privacy as a value leads us inevitably to exploring the possible religious roots to this concept. Since Serbia's population is predominantly of Orthodox Christian religion, we focus on the exploration of a possible Christian background of the concept of privacy. Today, the right to privacy is comprehended as a human right. The approach of Orthodox Christian churches[81] to human rights is cautious. This reflects the approach of the Orthodox Church to modernism. Contrary to the Catholic Church, the Orthodox Church entered the modern world from the period of Ottoman rule. The brief period of liberty was soon replaced by the repression of Communist regimes. Consequently, the Orthodox Church found itself astounded by modernism and did not have enough time to react to such social changes. This resulted in a variety of disharmonized approaches to human rights in mid-20th century and later.[82]

One of the notable examples of the Orthodox Church's approach to human rights is that of a social doctrine called "The Principles of Social Conception of the Russian Orthodox Church," adopted at the Bishops Council meeting in Moscow in August 2000. Under this doctrine, human rights cannot be superior to the values of the spiritual world. It is "inadmissible and dangerous," therefore, to interpret human rights as the ultimate and universal foundation of societal life to which religious views and practice should be subjected. From the point of view of the Orthodox Church, the political and legal institution of human rights can promote the good

78 Ibid. p. 7.
79 Ibid. p. 8.
80 Ibid. p. 9.
81 The Orthodox Church is made up of a number of self-governing churches which are either "autocephalous" (having their own head) or "autonomous" (self-governing). The Orthodox Churches are united in faith and by a common approach to theology, tradition, and worship. One of the autocephalous churches is the Serbian Orthodox Church.
82 Božović, 2020, p. 54.

goals of protecting human dignity and contribute to the spiritual and ethical development of the personality. One's human rights cannot be set against the values and interests of one's homeland, community, and family.[83] In June 2008, the Russian Orthodox Church adopted a document called "The Basic Principles of the Russian Church Teaching on Human Dignity, Freedom, and Rights" in which for the first time it takes a clear position on the right to privacy, particularly in the digital context:

> People's private life, worldview, and will should not become a subject of total control. Any manipulation over people's choice and their conscience by power structures, political forces and economic and media elites is dangerous for a society. Such things as compilation, concentration, and use of information about any aspect of people's life without their consent are also inadmissible. Information about a person can be collected without his or her consent only in cases where it is required for the defense of the homeland, preservation of morality, protection of people's health, rights and legitimate interests or the need to investigate a crime and to exercise justice. But in these cases, too, information may be collected and used in conformity with the stated aims and in accordance with law. The methods of collecting and processing information about people should not hurt the dignity of a person, restrict his freedom, or turn him from a subject of public relations into an object of machine operation. The adoption of technical devices accompanying a person permanently or inseparable from his body will be even more dangerous for human freedom if used to control his personality.[84]

More recently, at the Holy and Great Council of the Orthodox Church held in June 2016 in Crete (Greece), in the document entitled "The Mission of the Orthodox Church in Today's World," it has been emphasized that the Orthodox Church considered that every human being, regardless of skin color, religion, race, sex, ethnicity, and language, is created in the image and likeness of God, and enjoys equal rights in society. Consistent with this belief, the Orthodox Church rejects discrimination for any of the aforementioned reasons since these presuppose a difference in dignity between people. Although the quoted document does not refer to the right to privacy, it does show the alleviating of the Orthodox Church's general approach to human rights. This trend may be explained by the readiness of the Church to make use of the concept of human rights to protect its own institutional rights, as well as the individual rights of its believers.[85]

83 Novik, 2002, p. 12.

84 The Russian Orthodox Church's Basic Teaching on Human Dignity, Freedom and Rights, Section IV "Human dignity and freedom in the system of human rights", para. 7. [Online] Available at: https://old.mospat.ru/en/documents/dignity-freedom-rights/iv/ (Accessed: 23 February 2022).

85 Božović, 2020, p. 56.

5. Fundamental grounds for protecting the right to privacy

In Serbian law, the notion of privacy was initially employed to designate the protection of personal and family life, the protection of the home, and the protection of correspondence. In modern times, the concept of privacy is understood as the protection of personally identifiable data. The Serbian legal doctrine differentiates between general personal right and specific personal rights. The right to privacy is traditionally classified among specific personal rights, altogether with the right to identity, the right to a good name (derived from the right to human dignity), the right to respect of a deceased person.[86] The evolution of the concept of privacy is reflected in the constitutional history of Serbia. The earliest traces of the protection of privacy may be found in the Constitution of the Kingdom of Serbia, proclaimed on December 22, 1888. Under Art. 15 of the 1888 Constitution, the privacy of home may not be violated, except in cases prescribed by the law. A warrant to search the premises must be issued by a judge. The search must be conducted in presence of at least two witnesses who are Serbian citizens. The search may not be conducted during the night. Under Art. 23 of the 1888 Constitution, the secrecy of letters and telegraph messages may not be violated, except in cases of a criminal investigation or a war. The law is to prescribe which state organs are responsible for the breach of privacy of correspondence. The subsequent constitutions have also protected certain aspects of privacy. For example, the Constitution of the Socialist Federal Republic of Yugoslavia, proclaimed on February 21, 1974, guaranteed the inviolability of integrity of a person, personal and family life, and other rights of a person.[87] The 1974 Constitution proclaimed the inviolability of the home, which may be violated only in cases prescribed by the law.[88] The inviolability of letters and other means of communication was also guaranteed, except in case of a criminal investigation or if that is justified by the reasons of national security.[89] In contrast with the previous "particularized" approach, the Constitution of the Federal Republic of Yugoslavia, proclaimed on 27 April 1992, guaranteed the inviolability of all personal rights, without indicating any exception beforehand: "The inviolability of the physical and psychological integrity of the individual, his privacy and personal rights shall be guaranteed. The personal dignity and security of individuals shall be guaranteed."[90]

The current Constitution of the Republic of Serbia,[91] proclaimed on November 8, 2006, does not lay down a general right to privacy. Instead, it prescribes several

86 Vodinelić, 2014, pp. 258–271.
87 Art. 176 of the Constitution of the Socialist Federal Republic of Yugoslavia, Official Journal of the SFR Yugoslavia 9/1974.
88 Ibid. Art. 184.
89 Ibid. Art. 185.
90 Constitution of the Federal Republic of Yugoslavia, Official Journal of the FR Yugoslavia 1/1992, Art. 22.
91 Constitution of the Republic of Serbia, Official Journal of the Republic of Serbia 98/2006.

specific rights and liberties which, directly or indirectly, protect the private sphere of individuals. In that sense, the Constitution protects dignity and free development of individuals, and guarantees the inviolability of physical and mental integrity of individuals, the inviolability of the home, the confidentiality of letters, and other means of communication, as well as the freedom of thought, conscience, and religion. Additionally, the Constitution lays down a separate right to personal data protection. Currently, there are no plans for the constitutional amendments that would comprise any of these privacy-related provisions.[92]

Under Art. 23 of the Constitution, human dignity is inviolable, and everyone is obliged to respect and protect it. A violation of privacy would typically violate human dignity as well, i.e., the illegal posting of one's private explicit photos online or the publication in the media of one's medical records. A breach of privacy may also violate one's mental integrity, which is guaranteed, together with physical integrity, under Art. 25 of the Constitution. The highest national legal act guarantees the inviolability of the home. Under Art. 40 of the Constitution, no one may enter one's home or other premises against the will of its tenant, nor conduct a search in them. The tenant of the home or other premises has the right to be present during the search, in person or through his legal representative, together with two other witnesses who must not be minors. Entering one's home or other premises, and in special cases conducting a search without witnesses, is allowed without a court order if necessary for the purpose of the immediate arrest and detention of a perpetrator of a criminal offence, or to eliminate the direct and grave danger for citizens or property under conditions prescribed by the law. The Constitution also guarantees the confidentiality of letters and other means of communication. This provision may be interpreted as to include emails as "other means of communication." Under Art. 41 of the Constitution, derogation from this prohibition is allowed only for a specified period and based on decision of the court if this is necessary to conduct criminal proceedings or to protect the safety of the Republic of Serbia, in a manner stipulated by the law. The right to privacy is also protected through the constitutional guarantee of the freedom of thought, conscience, and religion laid down under Art. 43, in the sense that the citizens do not have the obligation to declare their religious or other beliefs. Finally, Art. 42 of the Constitution prescribes a separate right to personal data protection. Collecting, keeping, processing, and using of personal data is further regulated by the law. The use of personal data for purposes other than those for which they were collected is prohibited and punishable by law, unless this is necessary to conduct criminal proceedings or protect safety of the Republic of Serbia, in a manner stipulated by law. The Constitution also lays down the right to be informed about the personal data that is being collected, in accordance with the law, and the right to court protection in case of the abuse of such data. By prescribing a separate right to personal data protection,

92 On January 16, 2022, at a constitutional referendum, the Serbian citizens approved the constitutional amendments which would introduce the changes in the election of judges and prosecutors.

the Serbian constitution-makers were influenced by the Charter of Fundamental Rights of the European Union, which distinguishes data protection from privacy in the traditional sense, and lays down some specific guarantees of personal data protection.[93]

Human and minority rights that are guaranteed by the Constitution are implemented directly. The Constitution guarantees and directly implements human and minority rights guaranteed by the generally accepted rules of international law, ratified international treaties, and laws. The law may prescribe manner of exercising these rights only if explicitly stipulated in the Constitution or necessary to exercise a specific right owing to its nature, whereby the law may not under any circumstances influence the substance of the relevant guaranteed right. Provisions on human and minority rights are interpreted to the benefit of promoting values of a democratic society, pursuant to valid international standards in human and minority rights, as well as the practice of international institutions which supervise their implementation.[94] Human and minority rights guaranteed by the Constitution may be restricted by the law if the Constitution permits such restriction and for the purposes allowed by the Constitution, to the extent necessary to meet the constitutional purpose of restriction in a democratic society and without encroaching upon the substance of the relevant guaranteed right. The level of human and minority rights attained may not be lowered. When restricting human and minority rights, all state bodies, particularly the courts, are obliged to consider the substance of the restricted right, pertinence of restriction, nature and extent of restriction, relation of restriction and its purpose, and possibility to achieve the purpose of the restriction with less restrictive means.[95]

The Constitution lays down the right to judicial protection in case human or minority rights guaranteed by the Constitution have been violated or denied. The citizens also have the right to elimination of consequences arising from the violation. Under Art. 170 of the Constitution, a constitutional appeal may be lodged against individual acts or actions of state bodies or organizations entrusted with public powers, which have violated or withheld human and minority rights and freedoms guaranteed by the Constitution. A constitutional appeal may be lodged provided that other legal remedies for the protection of human and minority rights have been exhausted or have not been envisaged. In addition, constitutional appeal may be filed if legal remedies have not been exhausted, as when the submitter of a constitutional appeal has suffered a violation of the right to a trial within a reasonable time. A constitutional appeal may be filed by any (legal or natural) person who holds that their constitutionally guaranteed human or minority right or freedom have been violated by an individual act or action of a state body or organization entrusted with public powers. Hence, a legal or natural person may file a constitutional appeal

93 See Section 1 of this paper.
94 Ibid. Art. 18.
95 Ibid. Art. 20.

only if a violation of their own right is in question, i.e., they must have a personal and real interest that the disputed act is removed. A decision of the Constitutional Court upholding a constitutional appeal is the legal grounds for filing a claim for compensation of damage or removal of other detrimental consequences before a competent body, in accordance with law. According to the Constitutional Court's database, so far, no proceedings related to the breach of privacy in the digital context were initiated.[96]

Citizens also have the right to address international institutions to protect their freedoms and rights as guaranteed by the Constitution.[97] More specifically, with respect to the alleged violation of the right to privacy, Serbian citizens may address the European Court of Human Rights and the United Nations' Human Rights Committee. The ECtHR hears applications alleging that a contracting state has breached one or more of the human rights provisions concerning civil and political rights set out in the European Convention on Human Rights and its protocols. An application can be lodged by an individual, a group of individuals or one or more of the other contracting states. Presently,[98] there is only one case before the ECtHR against the Republic of Serbia with respect to the alleged violation of the right to privacy in the digital environment. The application *Aleksić v. Serbia* concerns the interception and reading of the applicant's emails by his public employer, the Serbian Statistics Office. These emails were sent from the applicant's official account and contained information regarding his personal and his professional circumstances, including comments as to the situation in the office. The emails were subsequently also used as evidence in a civil defamation suit brought against the applicant by one of his colleagues.[99] The ECtHR addressed several questions to the parties, related *inter alia* to the possible interference with the applicant's right to respect for his private and family life or his correspondence, within the meaning of Art. 8, para. 1 of the ECHR, and the compliance of such potential interference with the conditions laid down under Art. 8, para. 2 of the ECHR. The case is pending. The Serbian citizens have also the possibility to address the United Nations' Human Rights Committee, which may consider individual communications alleging violations of the rights set forth in the International Covenant on Civil and Political Rights by States parties to the First Optional Protocol to the International Covenant on Civil and Political Rights. Presently,[100] there are no cases brought against the Republic of Serbia before the United Nations' Human Rights Committee on the grounds of the breach of the right to privacy in the digital context.

96 Situation in February 2022.
97 Ibid. Art. 22.
98 Situation in February 2022.
99 ECtHR, *Aleksić v. Serbia,* application no. 40825/15, 31 July 2015.
100 Situation in February 2022.

6. Protection of the right to privacy in civil law

In civil law, the right to privacy enjoys protection under the general principles of civil wrongs (torts). A violation of personality rights would, in principle, generate the duty to compensate of nonmaterial, and more rarely, material damage.[101] Under the general principles of civil wrongs, whoever causes injury or loss to another is liable to redress it, unless proven that the damage was caused without his fault.[102] Injury or loss comprises a diminution of someone's property (simple loss) and preventing its increase (profit lost), as well as inflicting on another physical or psychological pain or causing fear (nonmaterial damage, or mental anguish). Fault exists after a tort-feasor has caused injury or loss intentionally or out of negligence.[103] With respect to the liability of minors, the LCT prescribes that a minor from seven to fourteen years of age is not liable for loss, unless it is proved that he was mentally competent while causing the damage, while a minor older than fourteen shall be liable according to general rules of tort liability.[104] Parents are liable for loss or injury caused by their child of over seven years of age, unless proving that the loss or injury took place without their fault.[105]

In case of violation of an individual right, the court may order that, at the expense of the tort-feasor, the sentence, namely the correction, be made public, or it may order that the tort-feasor takes back the statement causing the violation, or may order something else that would serve the purpose, otherwise it would apt to be achieved by indemnity.[106] For offended reputation, honor, freedom, or rights of personality, as well as for fear suffered, the court may—after finding that the circumstances of the case and particularly the intensity of pains and fear, and their duration, provide a corresponding ground thereof—award equitable damages, independently of redressing the property damage, even if the latter is not awarded.[107] In deciding on the request for redressing nonmaterial loss, as well as on the amount of such damages, the court shall consider the significance of the value violated, and the purpose to be achieved by such redress, but also that it does not favor ends otherwise incompatible with its nature and social purpose. Under the general principles of civil wrongs, at the request by a person sustaining loss the court may also award damages for future general loss if, according to regular course of events, it became certain that it will continue.[108]

These general rules serve to redress the damage suffered from the violation of personality rights, which presupposes that a violation have already occurred.

101 Pajtić, Radovanović, and Dudaš, 2018, p. 520.
102 Art. 154 of LCT.
103 Art. 158 of LCT.
104 Art. 160 of LCT.
105 Art. 165 of LCT.
106 Art. 199 of LCT.
107 Art. 200, para. 1 of LCT.
108 Art. 203 of LCT.

However, these rules do not provide for a mechanism which would protect an injured party from ongoing violations, from repetitive violations or from threats to violate personality rights.[109] This gap is filled by a specific demand to cease with the violation of individual rights. Under Art. 157 of the LCT, everyone is entitled to demand that the court or other competent authority order the cessation of an action by which the integrity of an individual, the integrity of family life, as well as other rights pertaining to a person, is violated. The court or other competent authority may order cessation of the action under the threat of a fine[110] set as a lump sum or a sum per instalments, to the benefit of the person suffering damage. The legislature did not indicate in relation to which personality rights (individual rights) this specific request may be invoked. The dominant view in legal doctrine is that Art. 157 of the LCT may be invoked to protect: (1) the right to human integrity, both physical and mental integrity; (2) the right to inviolability of personal and family life, including the right to privacy of correspondence, the right to protection of a business secret, the protection from illegal audio and video recording, and the inviolability of home; (3) other personality rights, such as the right to health, the right to a good name, the right to freedom, and the right to a personal name.[111] In the online environment, the first situation in which this specific demand to cease with the violation of individual rights may be invoked concerns the case of an ongoing violation consisting, for example, of the permanent availability of a website containing a personally identifiable data or a data that threatens a person's reputation. The second situation in which this demand may be invoked concerns the case where a violation has already taken place (e.g., by publishing untrue information in an online media outlet), and it is probable that a violation will be repeated (e.g., the perpetrator threatens that it will publish the same information in another online media outlet). The final and third scenario concerns the case where a violation have not yet taken place, but it is likely that it will (e.g., a person threatens that it will publish another's personal data online).[112]

More specifically, with respect to the personal data protection right, the LPPD explicitly provides for an individual's right to receive compensation from the controller or processor of personal data for the material or nonmaterial damage suffered.[113] The compensation cannot be obtained in the proceedings before the Commissioner for Information of Public Importance and Personal Data Protection, but in a separate civil law proceedings under the general principles of civil wrongs (torts). If a personal data has been controlled and/or processed by several controllers/

109 Pajtić, Radovanović and Dudaš, 2018, p. 520.

110 The use of the term "fine" requires further clarification. The above-described mechanism is modeled upon the French enforcement mechanism called "astreinte." "Astreinte" is a compensation payment for the delay in the execution of a court decision. Such payment, in contrast to court fines, is paid not to the state, but to the person in whose favor the decision was issued.

111 Perović, 1983, p. 556.

112 Pajtić, Radovanović and Dudaš, 2018, p. 521.

113 Art. 86, para. 1 of LPPD.

processors, they shall bear unlimited solidary/joint responsibility.[114] Also, an individual has the right to initiate civil law proceedings or other court proceedings in case of a violation of one of the rights guaranteed under the LPPD, such as the right to data portability, the right to erasure, the right to restrict personal data processing.[115] Such lawsuit does not preclude the right of an individual to initiate other administrative or court proceedings aiming at protecting his/her rights under the LPPD.[116] The lawsuit is to be lodged before the higher court that has jurisdiction over the territory of residence, domicile, or seat of a personal data controller or its representative, or before the higher court that has jurisdiction over the territory where a person to which data relate has residence or domicile, except if a personal data controller or processor is a state organ.[117]

Further to the general principles of civil wrongs (torts) laid down by the LCT, the Law on Media Services (LMS)[118] may be relied on to protect the personality rights which were injured by a registered media outlet. The Serbian Business Registers Agency runs the Media Register, which represents an integrated electronic database of dailies and periodicals, news agency services, radio programs, television programs, and independent online media editions (editor-formatted online portals).[119] The LMS prohibits the publication of the following information without consent of a concerned person: (1) information pertaining to private life or a personal records (e.g., letter, diary, digital recording); (2) visual recordings (e.g., photograph, drawing, video recording); and (3) audio recordings. Exceptionally, such information may be published without consent of a concerned person, if the audience cannot infer from the published information the identity of a concerned person.[120] A consent given for one specific type of media coverage cannot be interpreted as a consent for a subsequent publication of information within the same or other type of media coverage.[121] If a personal information pertains to a deceased person, a consent to publish may be given by a widow/widower, children who are sixteen years old, parents, brother or sister.[122] A person to which a published information pertains to enjoys the right of reply and the right of correction. If a media outlet rejects to publish a reply or correction, without such action being justified by one of the limitations to the right to privacy, prescribed by the LMS, a concerned person may request from the court to

114 Art. 86, para. 5 of LPPD.
115 Art. 84, para. 2 of LPPD.
116 Art. 84, para. 1 of LPPD.
117 Art. 84, para. 4 of LPPD.
118 Official Journal of the Republic of Serbia 83/2014, 58/2015 and 12/2016.
119 The LMS provides examples of what the media is not (e.g., book, movie, audio and audio-visual support, scientific and professional journals, web browsers, social networks, blogs). Exceptionally, online presentations may be treated as a media outlet within the meaning of the LMS if they are registered as such. See Art. 30.
120 Art. 80 of LMS.
121 Art. 80 of LMS.
122 Art. 84 of LMS. A consent of one of the indicated persons is sufficient even in case another relative objects to the publication of information.

order the reply or correction to be published.[123] A person whose right to privacy is violated by a media outlet may request from the court to: (1) determine that a right to privacy has been infringed; (2) order a media outlet to cease the infringing activity; (3) hand over or destroy the infringing content (e.g., delete an audio or video recordings, or hand over a negative).[124] A person whose right to privacy is allegedly violated may apply for interim measures, aiming at prohibiting the publication of information as long as the court proceedings are pending.[125]

The LMS allows for limitations to the right to privacy, which are justified by reasons of the public interest. The LMS enlists *exempli causa* circumstances under which a media outlet may publish an information pertaining to one's private life, without consent of a concerned party: (1) if information or record was intended to be made public by a concerned person, or if information or record was submitted to the media by a concerned party; (2) if information or record pertains to a person or event of public interest, in particular if it pertains to a public or political figure, and publishing such information is in interest of national security or economic well-being of a country, prevention of crime or disorder, protection of health or public morality, or protection of third party's rights and freedoms; (3) if a concerned party attracted public interest by way of his/her conduct in private, family, or professional life or by his/her public statements, thus creating incentive for media coverage; (4) if information is communicated during parliament session; (5) if publication of such information is in the interest of judiciary or national security; (6) if a concerned person did not object to obtaining the information or to making a recording, although he/she knew that such information/recording will be published; (7) if publication of such information is in the interest of science or education; (8) if publication of such information is necessary to alert the public of a danger (e.g., finding a missing person, or preventing a fraud); (9) if a recording pertains to a number of persons (e.g., concert audience or protesters at rallies); (10) if a recording is made at a public event; (11) if a person's face is made available to public as part of wider recording of an urban or natural site.[126]

The Serbian case law on privacy protection mainly comprises the disputes arising out of media coverage of certain events. Lawsuits often aim at protecting both the right to privacy and the right to reputation and honor. Nevertheless, the Serbian courts are undoubtedly of the view that the right to privacy may also enjoy protection separately and independently from the protection of the right to reputation and honor. This also stems from Art. 8 of the ECHR which directly protects the right to privacy.[127] Court competence in privacy disputes that concern the Internet is shared between the high and basic courts. Under Art. 4, para. 2 of the Law on

123 Arts. 83, 84 of LMS.
124 Art. 101 of LMS.
125 Art. 104 of LMS.
126 Art. 82 of LMS.
127 See for example: Appellate Court in Belgrade, decision no. Gž3 29/19, 1 March 2019; High Court in Belgrade, decision no. P3 br. 439/16, July 3, 2018.

Seats and Territories of the Courts and Public Prosecutors Offices,[128] a high court adjudicates in the first instance, in civil disputes about the printing of corrected information, and responses to information about violations of the prohibition of hate speech, protection of the right to privacy, and failure to publish information and compensation of damages in connection with the publication of the information.[129] However, a basic court shall adjudicate in the first instance if a violation of personality rights which generates the duty to compensate of nonmaterial damage occurred on social networks or other information exchange platforms that are not registered as a media outlet. The latter stems from Art. 22, para. 2 of the Law on Organization of Courts (LOC),[130] which prescribes that a basic court adjudicates in civil disputes in the first instance, unless the disputes are assigned to another court, and conducts enforcement and non-contentious proceedings that are not under the jurisdiction of another court. This interpretation of the rules on court jurisdiction, based on the distinction between registered media outlets and other information exchange platforms, is also reflected in Serbian case law.[131]

There is a significant number of disputes for the violation of privacy between individuals, on the one hand, and web portals and official webpages of Serbian newspapers, on the other, that follow the same pattern: a media outlet first publishes detailed information about the identity and private life of the claimant, which then wins the court case if it proves that he/she cannot be taken as a political or public figure whose private life enjoys lesser privacy protection. For example, a website of a Serbian daily newspaper published an Art. containing details from police records pertaining to a son of a famous chess player who committed a crime. The article contained information about his family ties with a famous chess player (whose name was also published), information about his current and previous employer, and details about the criminal act itself. The Supreme Court of Cassation confirmed the decision of a lower court finding a violation of privacy, showing that a relative of a celebrity is not a public figure within the meaning of the LMS. Consequently, he/she enjoys full privacy protection under Serbian law.[132] Similarly, a Serbian weekly magazine and its website were found to have violated privacy of a famous singer by publishing photographs of her cell phone screen, clearly showing the contents of SMS messages she was exchanging with a friend. Although the claimant was a public figure who enjoys limited privacy protection, the court found that publishing the contents of her SMS exchange without her consent did constitute a violation of

128 Official Journal of the Republic of Serbia 101/13.

129 Judicial power in the Republic of Serbia is vested in courts of general and special jurisdiction. The courts of general jurisdiction are basic courts, higher courts, appellate courts, and the Supreme Court of Cassation.

130 Official Journal of the Republic of Serbia 116/08, 104/09, 101/09, 31/11, 78/11, 101/11 and 101/13.

131 See for example: Appellate Court in Belgrade, decision no. R 210/17, 15 August 2017; Third Basic Court in Belgrade, decision no. 16P 1761/17, April 25, 2017; Supreme Court of Cassation, decision no. R1. 161/19, 20 March 2019; Supreme Court of Cassation, decision no. P1 263/2021, April 29, 2021.

132 Supreme Court of Cassation, decision no. Rev 405/2015, February 18, 2016.

the right to privacy. The court ordered that the magazine or its editor-in-chief compensate for the nonmaterial damage.[133] Conversely, if a website observes its duties under the LMS and the journalistic code of ethics, it shall not be responsible for a violation of privacy of a public or political figure. For example, a webpage of a Serbian daily newspaper published an article about a political figure in which it stated that she is under investigation for abuse of state funds. The article also stated that the claimant's domestic partner was allegedly involved in a similar criminal act. Prior to publishing the article, the journalist contacted the claimant, who confirmed the identity of her partner and the fact that there is an ongoing criminal investigation. The court found that the respondent merely published information that was either already in public domain or confirmed by the claimant, in full observance of the provisions of the LMS. Therefore, the court found no breach of privacy in the case.[134] Finally, if a web-portal simply reposts an article taken from another news outlet, while clearly indicating the source of information, it shall not be liable for privacy and/or reputation infringement, even if the information is inaccurate or offensive. This view has been taken by the Supreme Court of Cassation, which found no violation of provisions of the LMS in case of re-publishing of an online article containing both a false information that the claimant abused public funds and an offensive information that the claimant belongs to a political party with extremist views.[135]

The civil law proceedings for privacy breaches that do not involve online media outlets (as respondents) are less frequent. Citizens tend to initiate administrative proceedings before the Commissioner for Information of Public Importance and Personal Data Protection more often than civil law court proceedings, even though the compensation for material or nonmaterial damage suffered can only be obtained in the civil court. One of the rare examples to the contrary involves an employee whose personal data regarding an ongoing labor dispute with her employer, as well as data regarding her health status, were made available to her colleagues via the employer's web app. The injured party first notified the Commissioner for Information of Public Importance and Personal Data Protection of the privacy breach, which carried out an inspection and issued a warning to the employer–owner of the web app. The employee then initiated civil law proceedings before the First Basic Court in Belgrade for violation of personality rights and violation of reputation and honor, requesting nonmaterial damage compensation.[136] The first instance court found that the claimant did not prove it suffered any damage because of the defendant's conduct. However, the appellate court in Belgrade overturned the first instance court's decision, finding that non-pecuniary damage to personality rights (but not to honor and reputation) was proven by simply referring to the Commissioner's prior inspection and its findings.[137]

133 Supreme Court of Cassation, decision no. Rev 1903/2016, March 1, 2017.
134 Supreme Court of Cassation, decision no. Rev. 2347/2017, June 6, 2018.
135 Supreme Court of Cassation, decision no. Rev. 2163/2017, January 24, 2018.
136 First Basic Court in Belgrade, decision no. anonymized, March 17, 2021.
137 Appellate Court in Belgrade, decision no. anonymized, August 24, 2021.

7. Protection of the right to privacy in criminal law

The Penal Code of the Republic of Serbia (PC) prescribes criminal liability for breaches of privacy, which form subject-matter of several offences, belonging to different categories of criminal offences: (1) criminal offences against rights and freedoms of citizens; (2) criminal offences against honor and reputation; (3) sexual offences; (4) criminal offences against the security of computer data; and (5) criminal offences against the judiciary.

Within the category of criminal offences against rights and freedoms of citizens, the following criminal offences regard direct or indirect breaches of privacy: (1) violation of privacy of correspondence and other mail; (2) violation of the home; (3) illegal search of an apartment, premises, or person; (4) unauthorized disclosure of a secret; (5) unauthorized wiretapping and recording; (6) unauthorized photographing; (7) unauthorized publication and presentation of another's texts, image, or recordings; and (8) unauthorized collection of personal data. Under Art. 142 of the PC, anyone who violates the privacy of electronic mail may be punished with fine or imprisonment up to two years. The penalty may also be imposed to whoever communicates to another the content of another's mail, telegram or consignment acquired by violating the privacy thereof, or makes use of such contents. If the offence is committed by an official in discharge of duty, such a person may be punished with imprisonment from six months to three years. Under Art. 139 of the PC, an infringement of the inviolability of the home is sanctioned. However, such violation is unrelated to the Internet. Similarly, Art. 140 of the PC (illegal search of an apartment, premises, or person) protect one's privacy, but not in an online context. Under Art. 141 of the PC, a lawyer, physician, or other person who discloses without permission a secret that has come to his or her knowledge during the performance of his or her professional duty, shall be punished with fine or imprisonment up to one year. Such a disclosure of a secret may take place both offline and online. Under Art. 143 of the PC, anyone who wiretaps or records conversations, statements, or announcements that is not intended for him or her, using special equipment to do so, shall be punished with fine or imprisonment from three months to three years. Extensively interpreted, this would also allow sanctioning any person who records such statements made online, e.g., within an intercepted video call. The penalty may also be imposed on anyone who enables a third party to be informed about the conversation, statement, or announcement obtained through unauthorized wiretapping or audio recording. Under Art. 144 of the PC, whoever without authorization makes a photograph, film, video, or other recording of another, thereby significantly violating his/her personal life, or who delivers such a recording to a third party or otherwise enables him/her to familiarize himself/herself with the contents thereof, shall be punished with a fine or imprisonment of up to one year. If the offence is committed by an official in discharge of his/her duty, such person shall be punished with imprisonment up to three years. Under Art. 145 of the PC, whoever publishes or publicly presents another's text, portrait, photograph, film, or audio recording

of a personal character without the consent of a person who has drawn up the text or to whom it is related, or without consent of the person depicted in the portrait, photograph or film or whose voice is recorded on audio, or without consent of the person whose consent is mandatory by law, and thereby significantly violates the private life of that person, shall be punished with a fine or imprisonment up to two years. If the offence is committed by an official in discharge of duty, the offender shall be published by imprisonment up to three years. For example, the Basic Court in the municipality of Prokuplje sentenced the editor-in-chief of an online portal who published a photograph of a woman that was taken and published without her consent. The photograph was used to illustrate an article, the contents of which were completely unrelated to the photographed woman. The Basic Court found that the online portal breached the privacy of the photographed woman, and sentenced its editor-in-chief to three months' home detention, without imposing an electronic monitoring measure. The Supreme Court of Cassation upheld the decision.[138]

The introduction of data protection rules into the Serbian legal system led to the amendments of the PC that resulted in prescribing a specific criminal offence sanctioning the unauthorized collection of personal data. Under Art. 146 of the PC, anyone who, without proper authorization, obtains, communicates to another, or otherwise uses information that is collected, processed, and used in accordance with law, for purposes other than those for which they are intended, shall be punished with a fine or imprisonment up to one year. The penalty may also be imposed on anyone who, contrary to law, collects personal data on citizens and uses the data so collected. If the offence is committed by an official in discharge of duty, he/she will be punished with imprisonment up to three years. To interpret the precited provisions one primarily needs to refer to the LPPD, which lays down the definition of data processing, as well as the principles which must be upheld during data processing. Under Art. 4 of the LPPD, data processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The LPDP prescribes certain principles which must be upheld during data processing. The processing must be lawful, fair, and transparent; it must be limited in proportion to the goal and limited only to the data truly necessary; the data must be protected and kept not longer than is necessary to achieve the aim of the processing.[139] All forms of the criminal offence are adjudicated by a basic court in summary proceedings.[140] Committing some of the forms of this criminal offence can contain elements of another criminal offence, such as the unauthorized wiretapping or recording. In such a

138 Supreme Court of Cassation, decision no. Kzz 1383/2019, January 23, 2020.

139 Art. 5 of LPPD.

140 Art. 22 para 1 of LOC; Criminal Procedure Code, Official Journal of the Republic of Serbia 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 and 62/2021, Art. 495.

case, these criminal acts can converge with the unauthorized collection of personal data.[141] The available statistics from 2018 shows that only two persons were accused for the criminal offence of unauthorized collection of personal data, out of total of 1394 persons accused for all criminal offences against rights and freedoms of citizens, which represents 0.14% of all accused persons for that category of offences.[142]

Within the category of criminal offences against honor and reputation, one criminal offence regard direct or indirect breaches of privacy, i.e., dissemination of information on personal and family life. Under Art. 172 of the PC, whoever disseminates information about anyone's personal or family life that may harm his/her honor or reputation, shall be punished with a fine or imprisonment up to six months. If the offence is committed through press, radio, television, or other media or at a public gathering, the offender shall be punished with a fine or imprisonment up to one year. If such dissemination of personal information resulted or could have resulted in serious consequences for the injured party, the offender shall be punished with imprisonment for up to three years. The harm to one's honor or reputation must be proved, and the former must be explicitly stated in the court decision.[143] The offender shall not be punished for disseminating information on personal or family life in discharge of official duty, journalist profession, defending a right or defending justifiable public interest, if he/she proves the veracity of his/her allegations or if he/she proves reasonable grounds for belief that the allegations he/she disseminated were true. The criminal offence of dissemination of information on personal and family life may be conducted against a deceased person as well. In such a case, the incrimination protects the honor and reputation of deceased person's relatives.[144]

Within the category of sexual offences, the following criminal offences regard direct or indirect breaches of privacy: (1) showing, procuring, and possessing pornographic material and underage pornography; and (2) abuse of computer networks or other technical means of communication for committing criminal offences against sexual freedom of the minor. Under Art. 185 of the PC, whoever uses a minor to produce photographs, audio-visual or other items of pornographic content or for a pornographic show, shall be punished with imprisonment of six months to five years. If the act is committed against a child, the offender shall be punished with imprisonment of one to eight years. Also, whoever procures for himself or another and possesses, sells, shows, publicly exhibits, or electronically or otherwise makes available pictures, audio-visual or other items of pornographic content resulting from abuse of minor person, shall be punished with imprisonment of three months to three years. Whoever uses the means of information technologies to deliberately access the photographs, audio-visual or other items of pornographic content resulting from the abuse of a minor shall be punished with a fine or imprisonment of up to six months. Under

141 Sekulić and Grujić, 2020, p. 372.
142 Ibid. p. 374.
143 Supreme Court of Cassation, decision no. Kzz 1030/20, 7 October 2020.
144 Delić, 2022, p. 91.

Art. 185b of the PC, whoever with intent to commit sexual offence, by using computer network or communication with other technical devices makes appointment with a minor and appears on the place of the appointment, shall be punished with imprisonment of six months to five years (eight years in case of a child) and with fine.

Within the category of criminal offences against security of computer data, the following criminal offences regard direct or indirect breaches of privacy: (1) unauthorized access to computer, computer network or electronic data processing; (2) unauthorized use of a computer or computer network. Under Art. 302 of the PC, whoever, by circumventing protection measures, accesses a computer or computer network without authorization, or accesses electronic data processing without authorization, shall be punished by fine or imprisonment up to six months. Whoever records or uses data obtained in such a way, shall be punished by fine or imprisonment up to two years. Under Art. 304 of the PC, whoever uses computer services or computer network with intent to acquire unlawful material gain for himself or another, shall be punished by fine or imprisonment up to three months.

Finally, within the category of criminal offences against the judiciary, one of them regards breaches of privacy: a violation of confidentiality of proceedings. Under Art. 337 of the PC, whoever without authorization discloses what he has learned in court, misdemeanor, administrative, or other procedure established under law, when the law stipulates that such information may not be publicized or if declared secret by a decision of the court or other competent body, shall be punished by fine or imprisonment up to one year. Whoever without permission of the court publishes the course of proceedings against a juvenile or the disposition reached in such proceedings or who publishes the name of the juvenile against whom proceedings were conducted or information that may reveal the identity of the juvenile shall be punished with imprisonment up to two years. Whoever without authorization discloses information on the identity or personal data of a person protected in criminal proceedings or data regarding special protection program, shall be punished by imprisonment of six months to five years.

8. Personal data protection in administrative law

The main piece of legislation currently regulating personal data protection in the Republic of Serbia is the Law on Protection of Personal Data (hereinafter, the LPPD),[145] adopted in November 2018 and applicable since August 2019. The LPPD defines a personal data as any information relating to a natural person whose identity is determined or identifiable, directly or indirectly, in particular by reference to an identifier such as a name and identification number, location data, an online

145 For complete references, see Section 3 of this chapter.

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[146] The LPPD applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Furthermore, the LPPD applies to the processing of personal data performed by a controller or a processor that has its business seat/place of residence in the territory of the Republic of Serbia, within the framework of activities performed in the territory of the Republic of Serbia, regardless of whether the processing takes place in the territory of the Republic of Serbia or not. The LPPD also applies to the processing of personal data of data subjects residing in the territory of the Republic of Serbia by a controller or processor who does not have its business seat/place of residence in the territory of the Republic of Serbia, where the processing activities are related to: (1) the offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the territory of the Republic of Serbia; and (2) the monitoring of data subject's behavior as far as their behavior takes place within the territory of the Republic of Serbia. The LPPD does not apply to the processing of personal data by a natural person during a purely personal or household activity.[147] By reason of the matter, the LPPD covers all forms of use or other processing of personal data. The LPPD defines personal data processing as any action taken in connection with the information, including collection, recording, transcription, multiplication, copying, transmission, search, classification, storage, separation, adaptation, modification, making available, use, dissemination, recording, storage, disclosure through transmission or otherwise, dislocation, or other actions carried out in connection with the personal data, regardless of whether such actions are automated, semi-automated, or otherwise carried out.

Following the EU's GDPR model, the LPPD prescribes several specific rights of a data subject. First, the data subject has the right to be informed. The controller is obliged to respond appropriately to provide to the data subjects and prescribed information, i.e., information concerning the exercise of rights, in concise, transparent, intelligible, and easily accessible from, using clear and plain language if the information is intended for a minor. Second, the data subject has the right to request from the controller access to personal data. Third, the data subject has the right to have their inaccurate personal data rectified without undue delay. Fourth, the data subject has the right to have their personal data deleted by the controller when: (1) the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed; (2) the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing; (3) the data subject objects to the processing and there are no overriding legitimate grounds for the processing; (4) the personal data have been unlawfully processed; (5)

146 Art. 4 of LPPD.
147 Ibid. Arts. 1–3.

the personal data has to be erased for compliance with a legal obligation; or (6) the personal data has been collected in relation to the offer of information society services.[148] Fifth, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling. Sixth, the data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, if: (1) the processing is based on consent or a contract; and (2) the processing is carried out by automated means. Seventh, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, if such decision produces legal effects concerning to the data subject or in a similar manner significantly affects the data subject. However, the data subject may consent to such automated processing, or the latter may be explicitly allowed by the law in specific cases. Eight, the data subject has the right to lodge a complaint before the Commissioner, if they believe that the processing of their personal data was performed contrary to the LPPD. Lodging a complaint before the Commissioner does not affect the data subject's right to initiate other administrative or judicial proceedings.[149]

The LPPD prescribes additional rules with respect to the processing of specific categories of personal data: the LPPD prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[150] Exceptionally, the said prohibition does not apply in certain cases prescribed by the LPPD, such as when: (1) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except when it is prescribed that the consent is not a legal basis for such processing; (2) processing is necessary to protect the vital interests of the data subject or of another natural person if the data subject is physically or legally incapable of giving consent; (3) processing relates to personal data that are manifestly made public by the data subject; (4) processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts are acting in their judicial capacity; (5) processing is necessary for reasons of substantial public interest envisaged by law, if such processing is proportionate to the aim pursued, respecting the essence of the right to data protection and provided that the implementation of suitable and specific measures to safeguard the fundamental rights and the interests of the data subject is ensured.

148 See Midorović, 2019, pp. 293–296.

149 However, a possibility that a number of state authorities at the same time discuss one and the same legal matter may lead to opposite decisions being passed by these authorities.

150 Art. 17 of LPPD.

The national data protection authority responsible for overseeing the implementation of the LPPD is the Commissioner. The latter has the right to access and examine personal data, all documents relating to collection of personal data, personal data controllers' general enactments, and premises and equipment that the controllers use. The Commissioner supervises personal data controllers by conducting inspections. The inspectors act upon information acquired *ex officio* or received from complainants. According to the most recent report, the Commissioner completed 303 inspections in 2021,[151] and received total of 211 complaints for alleged breaches of data protection rules in the same period.[152] If in the process of supervision, the Commissioner establishes a breach of the LPPD, it may issue of warnings or orders. The Commissioner may: (1) order the rectification of the irregularity within a specified period; (2) temporarily ban the processing carried out in breach of the provisions of the LPPD; or (3) order deletion of the personal data collected without a proper legal basis. Certain breaches of law are set out as misdemeanors for which the LPPD prescribes fines. The Commissioner is authorized to initiate misdemeanor proceedings before the competent court.[153] The fine imposed may not, in any case, exceed the maximum amounts that can be imposed on the controller or processor for a misdemeanor under the LPPD, i.e., up to RSD 2,000,000 (approx. €17,000).[154]

In its latest review of case law, the Commissioner highlighted several inspections initiated at the request of a data subject, which are related to the processing of personal data in the digital environment.[155] For example, in one recent case the Commissioner found that an email address containing one's forename must treated as a personal data, given that it allows for identification of a physical person.[156] In another case, the Commissioner rejected the complaint of an individual who requested that Google removes a hyperlink referring to a press article that portrays him in a negative light. The Commissioner found that the request to remove the link from the search results was not founded, since in the case at hand the interests of freedom of information outweigh the interest of personal data protection. The Commissioner emphasized the fact that the disputed article contained information on the complainant's professional life, which was of public interest.[157]

151 Report on the activities of the Commissioner for Information of Public Importance and Personal Data Protection for 2021, p. 96. [Online] Available at: https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2021/Izve%C5%A1ta2021CIR.pdf (Accessed: 15 April 2022).

152 Ibid. p. 60.

153 When the legislature prescribed pecuniary fines for misdemeanors in fixed amounts, the Commissioner is empowered to impose them directly. However, this is not typically the case.

154 Art. 95 of LPPD.

155 The Review of Case Law [Online] Available at: https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/7PublikacijaZZPL/ZZPLPublikacija_7.pdf (Accessed: 6 April 2022).

156 The Commissioner, case no. 072-16-110/2021-6, 19 February 2021.

157 The Commissioner, case no. 072-16-05/2021-6, February 19, 2021.

9. The digital future as a challenge for privacy

As our analysis has shown, privacy has been directly or indirectly protected in Serbian civil and criminal law for decades. However, it is the widespread use of the Internet that has truly brought attention to privacy and personal data protection issues, and led to the development of specific protection mechanisms in administrative law. Further expansion of digital technologies shall require additional legislative efforts, particularly in mass surveillance and protection of children.

Mass surveillance, which is employed to monitor a specific area, activity or person through an electronic device or system for visual monitoring, is established as a central tool of public security policy. It is expected that the use of sophisticated video surveillance platforms will continue to increase in the years to come. Further to public entities, many private sector operators are using video surveillance in their daily performance.[158] Video surveillance represents a starting point for implementing advanced technologies such as automatic number plate recognition (ANPR) and automatic facial recognition (AFR). Mass surveillance may raise concerns as to the right of privacy but also freedom of expression, which is why it needs to be properly regulated. The analysis of the LPPD reveals that in Serbia mass surveillance is not regulated by specific norms; it rather remains within the framework of general data protection provisions. For instance, the LPPD does not require that a special written decision on deployment of a video surveillance system is enacted by the controller if legal basis is not provided by the law. Also, the LPPD does not impose the publishing of a mandatory notification that video surveillance is being carried out, in a manner that enables the individual to become familiar with the implementation of video surveillance. The notification should include: (1) the identity of the controller; and (2) information on how to get informed of duration and location of storage. Finally, the LPPD does not impose any storage limitation, while the prevailing approach in comparative law is to limit the storage of data collected through mass surveillance mechanisms up to six months.[159]

One of the notable cases of abuse of video surveillance mechanisms in Serbia regards a police traffic camera which was used to zoom in on a couple having sexual intercourse in the vicinity of the Belgrade Arena, a major sports and concert hall. The video was then uploaded to pornographic websites. Another case concerned the installation of cameras in toilets of the Belgrade Bus Station, under the excuse of fear of a possible terrorist attack.[160] The cases of abuse should alert the legislature to regulate mass surveillance in a general sense, regardless of the purpose and type of controllers performing it. Clearly, in the absence of general video surveillance rules, the specific legal frameworks developed per type of controllers could be over

158 Goold, 2010, p. 39.
159 Krivokapić et al., 2021, p. 15.
160 Ibid. p. 18.

intrusive. The 2021 Initial Draft Law on Internal Affairs[161] is a drastic example of such regulatory approach. Under the 2021 Initial Draft Law, the police were authorized to undertake mass biometric surveillance in public spaces in Serbia, by means of advanced technologies equipped with facial recognition software that enable capturing and processing of large amounts of sensitive personal data in real time. Even before the start of public consultations on the 2021 Initial Draft Law, the Commissioner for Information of Public Importance and Personal Data Protection emphasized that using this type of video surveillance systems for the purpose of biometric data processing is not legal now, since there is no legal basis for such processing in the national legal framework.[162] Following the reaction of the civil sector, the Ministry of Internal Affairs withdrew the Initial Draft Law.

Another area that necessitates additional legislative and advocacy effort is that of protection of children in digital environment. Given the recent COVID-19 pandemic experience, it has become questionable whether children, as the most vulnerable group, would be adequately safeguarded in times when they are required to spend much of their time online not just for fun but for education purposes as well.[163] The national legal framework on protection of children's privacy online is yet to be completed. The LPPD prescribes that a minor, who is at least 15 years old, may independently give consent for processing their personal data in relation to information society services. If the minor is below 15 years of age, consent must be given by the parent holding the parental responsibility, i.e., a legal guardian of the minor. The controller must take reasonable measures to verify whether the consent was given by the parent (or other legal guardian), taking into consideration available technology.[164] To properly enforce these rules, several issues must be resolved. For example, all providers of information society services must establish an age verification system. Also, it should be clarified whether an education institution could give consent on behalf of its pupils for personal data processing so that the latter may access an online education tool. Furthermore, the relationship between the right to personal data processing, on the one hand, and the right to freedom of expression (including freedom to seek, receive and impart information and ideas), the right to education and the right to participate in decision-making, on the other hand, needs to be further clarified.

It seems that the authorities are aware of the need to reinforce children's privacy protection mechanisms in the digital environment, given the significant number of strategies, regulations and initiatives that are being implemented or envisaged. In 2016 the government of the Republic of Serbia adopted the Regulation

161 The Draft Law [Online] Available at: http://www.mup.gov.rs/wps/wcm/connect/c8c5d780-fcb1-46b2-96be-650dbb3ef94e/NACRT+ZAKONA+O+UNUTRASNJIM+POSLOVIMA-cir.pdf?MOD=AJPERES&CVID=nKmncZs (Accessed: April 15 2022).

162 The Commissioner, Data Protection Impact Assessment of the Use of Video Surveillance System by the Ministry of Internal Affairs, opinion no. 073-15-1741/2019-02, November 12 2019.

163 Cendić, 2020, p. 83.

164 Art. 16 of LPPD.

on Children Safety and Protection in the Use of Information and Communication Technologies,[165] which was replaced by the new Regulation[166] adopted in 2020. The regulation provides for preventive measures for protection and safety in online environment, which are supposed to be implemented through informing and educating children, parents, and teachers, as well as through establishing a place for offering advice and receiving applications related to harmful, inappropriate, illegal content and behavior online. In 2017, the Ministry of Trade, Tourism and Telecommunications established the National Contact Centre for Child Safety on the Internet (hereinafter, the NCCCSI), as the central system for applications, education, and counselling related to child safety when using digital technologies.[167] In 2020, the government adopted the Strategy for the Prevention and Protection of Children against Violence for the period 2020–2023.[168] Finally, the government published a Draft Law on the Rights of the Child and the Protector of the Rights of the Child,[169] which lays down child's right to protection of his/her personal, private and family life, including the protection of his/her home and means of communication.[170]

10. Concluding remarks

Digital transformation has created a situation of severe tension between the right to privacy and the extensive (personal) data pooling on which the digital economy is based. To preserve at least some aspects of citizens' privacy online, the national legislatures need to react promptly and amend the rules when needed. As our analysis has shown, within the Serbian legal framework privacy enjoyed civil and criminal law protection for decades. However, the privacy-related case law remained rather scarce up until the appearance of the Internet, which drastically increased the number of privacy breaches. Most privacy breaches in the digital environment are dealt with under administrative law framework, in proceedings before the Commissioner for Information of Public Importance and Personal Data Protection. Very few of them are resolved in civil or criminal court proceedings. The analysis of the Serbian legal framework revealed two areas in which additional legislative efforts are required, those of mass surveillance and protection of children

165 Official Journal of the Republic of Serbia 61/16.
166 Ibid. 13/20.
167 NCCCSI web-portal [Online] Available at: https://pametnoibezbedno.gov.rs/kontakt-centar/ (Accessed: 17 April 2022).
168 Official Journal of the Republic of Serbia 80/20.
169 Draft Law [Online] Available at: https://www.paragraf.rs/dnevne-vesti/070619/070619-vest15.html (Accessed: 17 April 2022).
170 Art. 20 of Draft Law.

in the digital environment. However, one should not expect that online privacy breaches can be dealt with only by way of proper and timing legislative action. The best approach would be to combine the enforcement of appropriate legal framework with upgrading of the citizens' digital literacy. Such digital literacy should at least include knowledge about economic interests in data collection and sharing practices of all digital stakeholders, the ability to identify the specific privacy risks in online environment, and knowledge about how to implement preventive data protection strategies.

Bibliography

Božović, N. (2020) 'Biblija i ljudska prava' [Bible and Human Rights] in Božović, N., Tatalović, V. (eds.) *Evropa i hrišćanske vrednosti: Putevi Biblijske recepcije* [Europe and Christian Values: Biblical Reception]. 1st edn. Belgrade: Pravoslavni bogoslovski fakultet Univerziteta u Beogradu and Konrad Adenauer Stiftung, pp. 51–71.

Cendić, K. (2020) 'Children's Rights to Privacy in Times of Emergency: The Case of Serbia in Relation to Internet Education Technologies', *Global Campus Human Rights Journal,* 4(1), pp. 68–90.

Delany, H., Carolan, E. (2008) *The Right to Privacy – A Doctrinal and Comparative Analysis*. Dublin: Thomson Round Hall.

Delić N. (2022) *Krivično pravo – posebni deo* [Criminal Law – Special Part]. Belgrade: Faculty of Law of the University of Belgrade.

Dimitrijević, V., Paunović, M., Đerić, V. (1997) *Ljudska prava* [Human Rights]. Belgrade: Beogradski centar za ljudska prava.

Goold, B. (2010) 'How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy' in Schartum, D.W. (ed.) *Overvåking i en rettsstat – Surveillance in a Constitutional Government*. 1st edn. Bergen: Fagbokforlaget, pp. 38–48.

Greze, B. (2019) 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives', *International Data Privacy Law,* 9(2), pp. 109–128 [Online]. Available at: https://doi.org/10.1093/idpl/ipz003 (Accessed: 12 October 2022).

Jaeger Junior, A., Cravo, D.C. (2021) 'The extraterritoriality of the right to data portability: Cross-border flow between the European Union and Brazil' in Cunha Rodrigues, N. (ed.) *Extraterritoriality of EU Economic Law.* 1st edn. Cham: Springer, pp. 359–370; https://doi.org/10.1007/978-3-030-82291-0_17.

Kokott, J., Sobotta, C. (2013) 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law,* 3(4), pp. 222–228 [Online]. Available at: https://doi.org/10.1093/idpl/ipt017 (Accessed: 12 October 2022).

Krivokapić, Đ., Krivokapić D., Adamović J., Stefanović, A. (2021) 'Comparative Analysis of Video Surveillance Regulation in Data Protection Laws in the Former Yugoslav States', *Journal of Regional Security,* 16(1), pp. 5–26 [Online]. Available at: https://doi.org/10.5937/jrs16-27170 (Accessed: 12 October 2022).

Masur, P.K. (2020) 'How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information', *Media and Communication,* 8(2), pp. 258–269 [Online]. Available at: https://doi.org/10.17645/mac.v8i2.2855 (Accessed: 12 October 2022).

Midorović, S.D. (2019) 'Pravo na brisanje podataka o ličnosti dostupnih na internetu' [The Right to Erasure of Personal Data available on the Internet], *Zbornik radova Pravnog fakulteta u Nišu,* 58(84), pp. 281–306 [Online]. Available at: https://doi.org/10.5937/zrpfn0-22953 (Accessed: 12 October 2022).

Mitrović, M. (2020) 'Sloboda izražavanja i zaštita podataka o ličnosti na internetu: perspektiva internet korisnika u Srbiji' [Freedom of expression and personal data protection on the Internet: Serbian Internet users' perspective], *Communication and Media,* 15(47), pp. 5–34 [Online]. Available at: https://doi.org/10.5937/cm15-28316 (Accessed: 12 October 2022).

NOVIK, B. (2002) 'Analysis of The Fundamentals of Social Conception of the Russian Orthodox Church', *Occasional Papers on Religion in Eastern Europe,* 22(5), [Online]. Available at: https://digitalcommons.georgefox.edu/ree/vol22/iss5/2 (Accessed: 12 February 2022).

OOSTVEN, M., IRION, K. (2018) 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?' in BAKHOUM, M., CONDE GALLEGO, B., MACKENRODT, M.-O., SURBLUTÉ-NAMAVIČIENÉ, G. (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?.* 1st edn. Berlin: Springer, pp. 7–26; https://doi.org/10.1007/978-3-662-57646-5_2.

PAJTIĆ, B., RADOVANOVIĆ, S., DUDAŠ, A. (2018) *Obligaciono pravo* [Law of Obligations]. Novi Sad: Pravni fakultet u Novom Sadu.

PEROVIĆ, S. (ed.) (1983) *Komentar Zakona o obligacionim odnosima* [Commentary of the Law on Contracts and Torts]. 2nd edn. Belgrade: Savremena administracija.

SEKULIĆ, M.B., GRUJIĆ, G. (2020) 'Krivičnopravna zaštita ličnih podataka' [Personal Data Protection from the Criminal Law Perspective], *Glasnik Advokatske komore Vojvodine*, 92(3), pp. 347–378 [Online]. Available at: https://doi.org/10.5937/gakv92-26404 (Accessed: 12 October 2022).

VAN DER SLOOT, B. (2017) 'Legal fundamentalism: Is data protection really a fundamental right?' in LEENES, R., VAN BRAKEL, R., GUTWIRTH, S., DE HERT, P. (eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures.* 1st edn. Cham: Springer, pp. 3–30; https://doi.org/10.1007/978-3-319-50796-5_1.

VODINELIĆ, V. (2014) *Građansko pravo: Uvod u građansko pravo i opšti deo građanskog prava* [Civil Law: Introduction to Civil Law and General Principles of Civil Law]. Belgrade: Pravni fakultet Univerziteta Union and Službeni glasnik.

WESTIN, A.F. (1967) *Privacy and Freedom.* New York: Atheneum.