FACTA UNIVERSITATIS
Series: **Law and Politics** Vol. 14, N° 1, 2016, pp. 15 - 30

Review Paper

NORMATIVE FRAMEWORK ON ONLINE PRIVACY IN THE EUROPEAN UNION AND IN SERBIA

UDC 343.45:004.738.4](4-672EU:497.11)
341.231.14:004.738.4](4-672EU:497.11)

Vidoje Spasić

Faculty of Law, University of Niš, Republic of Serbia

Abstract. *The development of modern technology has brought many benefits to its users but it has also seriously endangered individual privacy and raised numerous issues concerning the the protection of personal data. The common assumption that Internet users are largely anonymous in cyberspace is wrong because they leave a trail of all their online activities. Actively or passively, consciously or unconsciously, individuals leave certain personal data which can be either abused or used without the owner's authorization. Thus, personal privacy can be seriously endangered. In this paper, the author provides an overview of the normative framework on online privacy in the European Union and in Serbia. The EU regulation concerning the protection of privacy in cyberspace is fairly satisfactory, and it is constantly updated in order to keep up with the latest technological developments. The Republic of Serbia has enacted a number of legislative acts regulating some segments of online privacy but the Serbian legislation in this area is generally more suitable for the analogue than for the digital environment, for which reason it has to be further amended and upgraded.*

Key words: *the Internet, personal data, online privacy, violation.*

1. THE CONCEPT AND KINDS OF PRIVACY

The right to privacy is one of the fundamental human rights that are guaranteed by international and national legislation. The term "privacy" implies a set of data which are inseparable from an individual who owns these personal data. These data define a person's individuality and, in effect, they are protected from unauthorized access. The data are primarily associated with some personality rights but they also pertain to family life, sexual orientation, habits, hobbies or other personal interests. Thus, privacy may imply many different things to different people in diverse contexts. One of the earliest definitions of the right to privacy

Received February 24th, 2016/ Accepted April 12th, 2016
Corresponding author: Vidoje Spasić, LL.D., Associate Professor, University of Niš, Faculty of Law, Trg kralja Aleksandra 11, 18000 Niš, Republic of Serbia, E-mail: vidza@prafak.ni.ac.rs

was provided by the American jurisprudence at the end of the 19th century, when it was defined as "the right to be left alone".

First and foremost, the right to privacy protects immaterial assets which represent one's personality and are embodied in one's personal data. Essentially, the violation of privacy does not entail a physical violation of personal data in a classical sense but rather a violation of a person or personality rights. Nevertheless, for the purpose of reviewing the protection of personal data (as the major asset of every individual), the term "privacy" is traditionally used because it links the assets from one's personal data to the immaterial essence of every individual.

A modern concept of the "right to privacy" developed alongside the development of the first information technology devices, such as the telephone, telegraph, etc. (Simons, 1982: 14)

In contemporary legal theory, the "right to privacy" is observed from the so-called active point of view (Prlja, Reljanović, Ivanović, 2012: 95). The interest that accompanies the "right to privacy" is the interest of self-determination of one`s own communication with other people, which reflects a desire of an individual or a group to impart personal information as they wish and to whom they wish (Schafer, 1980: 9). The contemporary concept of "right to privacy" in personal and family life includes a set of multifaceted human rights that can be viewed from different aspects: as the privacy of home, transcripts, communication, intimate and family life.

The right to privacy is an absolute right which has an "erga omnes" effect, but there are cases where it may be limited for the sake of general public interest; the limitations are explicitly prescribed by the law. In general, individual privacy is divided into: spatial privacy, privacy of information and privacy of communication.

Spatial privacy

This kind of privacy refers to one's home and/or other space where a person lives separately from others. The Constitution guarantees the right of every citizen to the inviolability of one's home. Spatial privacy ensures the observance of every individual`s right to personal space or dwelling domain, either at home or at workplace.

Privacy of Information

In a modern society, information is one of the most important resources in almost every area of human life. It is essential in corporate management and decision-making processes; it is the cornerstone of economic and cultural progress of human civilization. Technically speaking, information is the message carrier in communication processes. The transfer of information and the preservation of its integrity is a growing challenge in the modern technological society. The term "privacy of information" denotes the aspect of privacy related to gathering, handling and using information about an individual. Briefly, it refers to personal data which cannot be used by third persons without obtaining permission from the owner of the personal data. The act of violating one's personal data constitutes an intrusion into a domain of privacy; considering the personal nature of the inflicted damage or harm, privacy is the asset which has to be safeguarded.

Privacy of communication

Communication rights are fundamental human rights. The Constitution guarantees the right to seek, receive and impart information, the right to disseminate information through mass media, and the right to privacy. Communication is an act of transferring a message to one or more persons through a system of symbols. Communication is a necessary presumption in every society, a "condicio sine qua non" of human life and social order [Watzlawick, Beavin, Jakson, 1974: 13]. In that context, the privacy of communication is an aspect of privacy pertaining to personal notes and correspondence, and any other type of interpersonal communication, which is legally protected as an aspect of the individual privacy rights. The protection of privacy of one's communications is envisaged in the Constitution, which guarantees the inviolability of the freedom and confidentiality of correspondence and all other forms of communication, which may be limited or restricted only in exceptional cases.

The development of modern technology has given rise to a new form of personal data protection and engendered a new concept of data protection, designated as "e-privacy" and pertaining to communication via electronic networks. In this case, personal data are gathered through technological proceedings which are called profiling.

Profiling problems are directly linked to a user's private and/or business domain. However, when a user's business domain is concerned, it is highly disputable to what extent an employer is allowed to use diverse methods and techniques to control the communication of his/her employees without violating their privacy.

2. Related Terminology and Definitions

The complexity of the right to privacy imposes the need to define certain concepts, contents and categories underlying this multifaceted human right.

2.1. Information, data, message

Keeping in mind that data and information are often used as synonyms, it is important to make a clear distinction between the two terms. Thus, *information* is defined as a set of data put into a meaningful context, while a *datum* may exist outside a specific context.

Information is a key concept in all the sciences dealing with any kind of symbolic communication (mathematics, linguistics, social sciences and humanities). In a modern community, information is a multidisciplinary phenomenon, which is important in different contexts; it is the basis of public information, communication, decision-making processes, and a crucial factor in political and democratic processes. The most important aspect of information is the message, as the carrier of information, which conceptually binds individual data into information. Information is a result of processing, analyzing and organizing data in a way that adds to the recipient's awareness or knowledge.

A datum (a piece of data) is a record on a specific event, phenomenon, fact or observation in the environment, recorded in any form, which has certain relevance and value for its holder/owner. Data may appear in different forms: as text, numbers, symbols, signs, illustrations, images, sounds, etc.

A piece of information is a piece of meaningful and applicable data; on the other hand, a piece of data that cannot be used and/or understood by the recipient is not information. Therefore, information is a set of meaningful, useful symbols which reveal something new to the recipient; information is a message that is received and understood. The carriers of information may be living creatures, printed or electronic media, genes, light, sound, smell, water, soil, etc.

Message is a piece of information in its material form. The main characteristic of a message is that it is informative, i.e. it gives some new information to the recipient. By its content, the information is always about something, which means that it can be either true or false. In order to be useful and functional, all participants in the communication chain should have some prior knowledge about the matter.[1] Information technology includes the development, research, design, implementation and management of information systems, and particularly the software administration and hardware support. Information technology contributes to the dissemination of knowledge and culture.

2.2. Distinction between personal data and the right to privacy

Despite the similarities, personal data cannot be equated with the concept of privacy. By its content, privacy is a wider term than personal data. In addition to personal data, the concept of privacy includes some facts and/or circumstances facts or circumstances which are not recorded and quantified. Thus, privacy also includes one's sexual life, family relations, emotions, social circles, and other categories which exceed the scope of personal data.

Personal data include any piece of information pertaining to a natural person, irrespective of the information carrier and the form it is provided in (paper, tape, film, electronic medium, etc.), irrespective of the person who ordered or on whose behalf the personal data have been obtained, irrespective of the place and manner of obtaining information (by direct observation, listening, recording, or indirectly by examining document), or any other information properties.

The English word "privacy" comes from the Latin word "*privatus*", meaning withdrawn from public, confidentiality and private/personal relations; the word "personality" comes from a German word "*Personklicheit*", and the word "intimacy" comes from a French phrase "*le droit au respect da la vie intime"*. The term "personality" denotes individuality, distinctive identity, specific personal traits, etc. Therefore, the concept of *personality* pertains to the distinctive identity, the exclusive personal domain of an individual and his/her personal life. On the other hand, the concept of *"privacy"* includes a wider circle of features which need not have a specific significance when taken in isolation but, when connected in a stable structure, they provide a personal profile which is most frequently familiar to that person only.

In a broader sense, the term "*digital personality*" is generally defined in terms of digital safety, which means that an individual is the exclusive holder of personal information that he may or may not share with others, and decide how, when and to whom he/she will disclose personal data (if at all), by taking into account his personal rights, needs and interests as well as the rights, needs and interests of the community.

[1] Yet, information and a message should not be necessarily viewed in a strictly linguistic context because even noise that disrupts a course of communication may carry certain information.

3. PRIVACY IN THE DIGITALWORLD

Due to the emergence and development of digital technology (especially the Internet), privacy has become one of the key problems in the cyber world. The electronic collection of personal data and the likelihood of their abuse have become a reality, particularly in the field of e-business/commerce, medical procedures, and using diverse Internet services. Individuals may disclose personal data on the Internet either actively (voluntarily) or passively (involuntarily). Personal data are actively revealed through online shopping, by making profiles on social networks, etc. They are passively revealed through the use of"cookies", files which may generate information about the "clickstream" or click path data, and reveal information about the user, the visited websites, the time/length and frequency of using a specific website, including information about the content of the hard drive of the user's computer. Technically speaking, every message may be "traced", "read"and "decoded". There are numerous ways of violating online privacy (Spasić, 2010: 11).

The Internet is a community of unremitting communication (Tatomirovic, 2009: 1). It blurs the traditional boundaries between interpersonal relations and mass-communication phenomena; it generates new possibilities and new risks in human interactions.

In the document "*Communication 1996"*, the European Commission noted: "The unique characteristic of the Internet is that it simultaneously functions as a medium for publishing information and for communication. Unlike traditional media, the Internet supports a variety of communication modes: one-to-one, one-to-many, and many-to-many. Therefore, the Internet is radically different from traditional broadcasting. It is also significantly different from traditional telecommunications services." [2]

Electronic communication means electronic exchange of information between two users, or between a user and a server. This exchange can be visible or invisible. Visible exchange implies a voluntary consent of the user who is actively engaged in chat-room discussions, news groups, e-mailing, subscriber directories, e-banking/commerce, etc. (even though, in some cases, these activities may take a form of invisible exchange/communication as well). Invisible exchange occurs without the user's knowledge and it is performed via log files (linking data), traffic data and "cookies".

The Internet leaves a detailed trace of data about every single step taken by the user. A huge amount of information about consumers is collected during online shopping, especially via "click stream monitoring". Transactional data, "click stream" data, or "mouse-droppings" data can provide a personal profile of one`s online life. Technologies like "cookies", written directly on the user`s hardware, make it possible for websites to secretly gather information about the user's online activities and preserve them for a later wider use.

For example, when individuals share some information with a doctor, a salesperson or a bank, they expect their personal information to be treated professionally and used for specific purposes with due diligence. However, companies often use their clients' confidential personal data for purposes which exceed the clients' needs and intentions.

Similarly, when sending an e-mail, one relies on the privacy and confidentiality of this service. Unfortunately, it is not always the case. While traveling through the World Wide Web, an e-mail is manipulated by many independent entities. Thus, while the message path is unobstructed, the protection of privacy ends as soon as the message is sent. As

[2] http://www2.echo.lu/legal/en/Internet/content/communic.html. Accessed on 12.12.2002

there are no checkpoints on the Internet for centralized supervision and control, the ultimate result of the progressive exchange of personal information on the Internet is the poor and inadequate protection of personal information on the web.

The privacy of personal documents and files is also poorly protected. In the past, people used to keep their personal diaries and photo albums stored under the bed or locked in a secret drawer. Upon the emergence of computers, personal diaries were moved onto PC hard drives, and photo albums were transferred onto CD-ROMs. Today, the new digital technology known as "cloud computing" allows individuals to rent virtual space outside their home computers and keep their personal data there (Spasić, Stevanović, 2015: 121-141). But, keeping personal data on a distant server eliminates many privacy protection options which were available to users when they kept their personal data at home in the traditional way.

4. PRIVACY IN THE EU LAW

Article 12 of the Universal Declaration of Human Rights provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Article 8 of the *European Convention on Human Rights and Fundamental Freedoms* (ECHR)[3] guarantees the "right to private life," and stipulates that the intervention of public authorities must be imposed by law, necessary in a democratic society and pursue one of the following legitimate goals: national security, public safety or economic well-being of the country, prevention of disorder or crime, protection of health or morals, or protection of the rights and freedoms of others.[4]

The European Court of Human Rights has adopted a very broad interpretation of the right to privacy. In resolving cases involving a conflict between media rights and the right to privacy, the ECtHR uses the "principle of proportionality" by weighing the public and the private interest.

Considering the manner of regulating privacy issues, there are two basic systems used in the contemporary world: the Anglo-Saxon (common law) and the European-continental (civil law) system. Thus, relying on the standpoints of "private law" protection of an individual, the common law countries will resort to passing the "privacy law"(e.g. in the USA, a vast majority of Canadian provinces, etc.), where individual privacy is protected in courts by means of "personal initiative".[5] On the other hand, the civil law countries

[3] The ECHR was adopted on 4 November 1950 and took effect on 3 September 1953. The latest amendment, Protocol 14, was open for signing on 13 May 2004, but it is still not in effect; CoE ETS No. 005

[4] For example, the right to privacy is also protected in Art. 16 of the Convention on the Rights of the Child, or in some other documents envisaging the right to a fair trial (see Art. 6 ECHR or Art. 14 ICCPR), which contain specific provisions on the exclusion of the public and media from trial.

[5] In Great Britain, the Data Protection Act envisages *inter alia* the establishment of a special "registrar for keeping records on data protection", who is appointed by the Crown and is practically independent from the UK Government. This Act is more in line with the European-Continental than with the Anglo-Saxon model.

where privacy is protected by providing a "public law" protection of an individual resort to passing special legislation on "data protection" (e.g. France, Germany, Sweden, etc.).[6,7]

The French Act No 78-17 on information technology, data files and civil liberties (1978) established a special body, the "*Commission Nationale de l'Informatique et des Libertés"* (CNIL), which is only subjected to judicial control [Maisl, 1987: 581].

Many national criminal laws sanction different forms of violation of the right to private life.[7] The punishable criminal acts include: unauthorized photographing, publishing another person`s documents/records, portraits, photographs, films or personal phonographs, unauthorized phone-tapping and sound recording.

Within the EU normative framework, there are several important documents that regulate the subject matter of private data protection and privacy in digital environment.

4.1. The International Covenant on Civil and Political Rights

In Article 17, the ICCPR[8] provides that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". It further states that "everyone has the right to the protection of the law against such interference or attacks."

Other rights also may be affected by mass surveillance, interception of digital communications and collection of personal data. However, the establishment of digital mass surveillance has raised questions concerning the extent to which such measures are consistent with international legal standards and whether more substantial surveillance safeguards should be put in place in order to protect individuals against violations of their human rights. Specifically, surveillance measures must not arbitrarily or unlawfully interfere with an individual's privacy, family, home or correspondence. Governments must take specific measures to ensure legal protection against such interferences.

As the EU Court of Justice recently observed, communications metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained."[9] It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy. Even the mere possibility of communications information being captured creates an interference with privacy,[10] with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy.

---

[6] The first separate law which directly regulates the issue of data protection was passed in Hessen, a federal state in the Federal Republic of Germany, in 1970. The model was later followed by other countries. In some countries, the matter of personal data protection is directly regulated in their constitutional documents.

[7] In France, Article 9 of the French Civil Code states that everybody has the right to privacy; this article ws introduced by adopting the Act No 70-643 of July 17th, 1970. In Germany, Federal Law on Multimedia, which has been in force since August 1st 1997, regulates data protection in Article 2, under which the providers of services are obliged to offer to their consumers a possibility of anonymous (or pseudonymous) access and payment whenever it is reasonable and technically possible.

[8] The ICCPR was adopted in 1966, and entered into force in 1976.

[9] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Judgment of 8 April 2014, paras. 26-27 and 37. See also: Executive Office of the President, "Big Data and Privacy: A Technological Perspective" (available from www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_may_2014.pdf), p. 19.

[10] See: European Court of Human Rights, Weber and Saravia, para. 78; *Malone v. UK*, para. 64.

Interference with an individual's right to privacy is only permissible if it is neither arbitrary nor unlawful. In its general comment No. 16, the Human Rights Committee explained that the term "unlawful" implied that no interference could take place "except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant".[11]

Interference that is permissible under national law may nonetheless be "unlawful" if that national law is in conflict with the provisions of the International Covenant on Civil and Political Rights. The expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of this concept, the Committee explained, "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.[12]The Committee interpreted the concept of reasonableness to indicate that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case".[13]

Unlike certain other provisions of the Covenant, Article 17 does not include an explicit limitations clause. Guidance on the meaning of the qualifying words "arbitrary or unlawful" nonetheless can be drawn from the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights;[14] the practice of the Human Rights Committee as reflected in its general comments, including Nos. 16, 27, 29, 34, and 31, findings on individual communications[15] and concluding observations;[16] regional and national case law;[17] and the views of independent experts.[18]

Any limitation to privacy rights reflected in Article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances.[19]

4.2. European Council Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

The aim of this Convention[20] is to widen the protection of the primary human rights and freedoms, especially the right to privacy, during the automatic processing of personal data. The signatory states are obliged to enact relevant national legislation on this matter. The Convention is based on the principles of legality and impartiality in protecting personal data.

---

[11] Official Records of the General Assembly (see footnote 3), para. 3
[12] Ibid., para. 4.
[13] Communication No. 488/1992, Toonan v Australia, para. 8.3; see also communications Nos. 903/1999, para 7.3, and 1482/2006, paras. 10.1 and 10.2.
[14] See E/CN.4/1985/4, annex.
[15] For example, communication No. 903/1999, 2004, Van Hulst v. The Netherlands
[16] CCPR /C/USA/CO/4.
[17] For example, European Court of Human Rights, Uzun v. Germany, 2 September 2010, and Weber and Soravia v. Germany, para. 4; and Inter-American Court of Human Rights, Escher v. Brazil, Judgment, 20 Nov. 2009
[18] See A/HRC/13/37 and A/HRC/23/40. See also International Principles on the Application of Human Rights to Communications Surveillance, available at https://en.necessaryandproportionate.org/text
[19] The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation must be shown to have some chance of achieving that goal. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination.
[20] Adopted in Strasbourg, in January 1981.

Personal data shall be collected, processed and used in a way that does not insult human personal dignity. The principle of access to information implies the right of a person whose data are gathered and processed to be informed about all the relevant facts considering the data collection and processing, and to take all protection measures if the data are used in contravention with the law. The Convention also envisages that the rights of a person whose data are gathered and processed may be limited or restricted to an extent necessary for the protection of common or public interests, as well as the protection of rights and freedoms of others.

Special categories of highly sensitive data shall be gathered, processed and used in compliance with special strict rules and upon obtaining a written consent of the specific person. It refers to sensitive personal data on racial origin, national and religions orientation, political and syndical beliefs, health and sexual life, and criminal convictions.

In accordance with the principle of security, the law should regulate measures and actions that a person responsible for keeping records and collections of personal data should take for the protection of these collections from natural disasters and human interference and abuse.

Relying on the principle of free trans-border flow, exchange and transfer of personal data across national borders, national law should establish conditions for a cross-border exchange of information and privacy protection measures.

4.3. Directive on the Protection of Individuals with regard to the processing of personal data and free movement of such data

This Directive[21] obliges the member states to harmonize their legislations with the aim of providing an adequate level of protection of the fundamental rights and freedoms, especially the right to privacy in electronic communication within the EU. In that sense, providers of public electronic communication services must take all the necessary technical and organizational measures to provide safety of their services.

The EU member states are obliged to provide relevant national legislation which would oblige the providers of public communication services to ensure the confidentiality of communications in terms of "traffic data" (traffic on the web). Such data must remain secret and inaccessible to third persons, except to public authorities for the purpose of taking some action.

The date related to a subscriber or some other network user must be destroyed or kept anonymous, and they may be used only for strictly specified purposes. In cases where a user must reveal his identity to be allowed to use the network, a service provider is obliged to prevent it from being reveled to third persons. The Directive also regulates the issues concerning directories or registers of subscribers. Thus, before one's personal data are entered into a directory/register, a subscriber should be duly informed (at no costs) about the purpose of keeping a printed or electronic directory where his/her personal data will be entered.

4.4. The Declaration on Freedom of Communication on the Internet (2003)

This Declaration[22] *stipulates* that the freedom of communication does not prejudice the right to dignity or any other fundamental human rights. Under the Declaration, it is

[21] Directive 95/46/EC from October 24th, 1995, Official Journal L 281, 23/11/1995. p. 0031-0050
[22] Adopted by the Council of Europe in 2003.

essential *inter alia* to strike a balance between the right to anonymity on the Internet and the need to catch the perpetrators of crimes. The Declaration clearly sets out the basic postulates of the (non) regulation of the Internet content, using the following principles: a) things permitted "off-line" should also be allowed "on-line", and b) it is unacceptable to apply restrictions on the Internet contents to any extent greater than that otherwise allowed for other transmitters of contents.

The set of regional European standards in the area of online privacy shall also include the following documents: the Council of Europe *Cyber-crime Convention* (2001); the EU directives protecting personal data (Directive 95/46/EC, *Data Protection Directive),* e-privacy (Directive 2002/58/EC, *E-Privacy Directive)*[23] and other legitimate goals, such as the protection of national security and prevention of terrorism (Directive 2006/24/EC, *Data Retention Directive); the* Personal Data Directive 97/66 on proceedings for the protection of personal data in communication sector (of December 15th 1997)[24] Finally, the Personal Data Directive in electronic communication was adopted on July 12th 2002.[25]

5. PRIVACY LEGISLATION IN THE REPUBLIC OF SERBIA

In Article 42, the Constitution of the Republic of Serbia[26] guarantees the protection of personal data. The Constitution proclaims that using personal data beyond the purposes for which they are collected is forbidden and punishable by the law, except in cases involving criminal proceedings and protection of state security, as prescribed by the law. The Constitution states that specific issues concerning the collection, storing, processing and using personal data will be regulated by enacting special legislation.

In Serbia, privacy issues are regulated in several legislative acts.

5.1. The Personal Data Protection Act

This Act [27] regulates the collection, processing and protection of personal data. It envisages personal data protection of every natural person, regardless of nationality, gender, religious belief, race, or any other characteristic or affiliation. The authority to institute action for the protection of personal data protection is vested in the Commissioner for information of public importance and personal data protection.

Personal data include any information pertaining to a natural person, irrespective of the information carrier and the form it is provided in (paper, tape, film, electronic medium, etc.), irrespective of the person who ordered or on whose behalf the personal data have been obtained, irrespective of the place and manner of obtaining information

[23] The E-privacy Directive sets out standards on how personal data can be used and collected, particularly in case of e-mail spam or other forms of e-mail communication which an individual user has not requested (unsolicited communications). For example, the Directive forbids direct e-mail advertising without the recipient's consent if the recipient is a private person ("opt-in" regime).

[24] Official Journal NºL 024, 30/01 1998, p. 0001-0008.

[25] Directive on private life and electronic communication, No 2002/58, 12. 07. 2002; Official Journal No 201, 0731/07/2002; p. 0037-047

[26] Article 42, the Constitution of the Republic of Serbia, "Official Gazette of RS"No 83/06

[27] The Personal Data Protection Act, Official Gazette RS"No 97/2008, 104/2009 – State law 68/2012 – Decision of CC and 107/2012; Articles 8, 12, 13, 16, 17, 31

(by direct observation, listening, recording, or indirectly by examining document), or any other information properties.

Data processing is any automatic, semi-automatic or some other activity related to handling data. Article 8 of this Act provides a set of rules concerning a possible violation of personal data in the course of data processing. Thus, *data processing is prohibited* if: 1) it is performed without the natural person's consent, i.e. illegally; 2) it is performed for purposes other than those previously specified, except for humanitarian causes; 3) the purpose of collecting personal data is not explicitly specified, is unauthorized, has been modified, or has been accomplished; 4) the person whose data is being processed is not designated or cannot be designated even after accomplishing the aim of data processing; 5) the mode of data processing is prohibited by the law; 6) the piece of data being processed is unnecessary or inadequate for accomplishing the legitimate aim of data processing; 7) the amount or the kind of data being processed is disproportionate to the legitimate aim of data processing; 8) the piece of data is incorrect or incomplete, it is not based on reliable sources, or it is outdated (Article 8 PDPA).

Given the fact that right to privacy is not unlimited, this Act also regulates the issue of *data processing without informed consent* (Article 12), which is allowed as follows: 1) to accomplish or protect a vital interest of the person whose data are being processed or another person; 2) to ensure the performance of some obligation prescribed by the law, a by-law or a contractual obligation (towards the operator), as well as for the purpose of signing a contract; 2a) for the purpose of gathering humanitarian aid; 3) for other purposes determined by this Act, aimed at fulfilling some justified interests of the person, operator or user. (Article 12 PDPA).

The Act also allows non-consensual data processing by competent state authorities if it is necessary for the protection of general public interests and rights and freedom of others; in other cases, a written consent of an individual is necessary (Article 13 PDPA).

In particular, the Act regulates the special category of sensitive data (Articles 16, 17), pertaining to national affiliation, race, gender, language, religious belief, political and syndical orientation, health condition, social welfare benefits, sexual life, victims of violence and criminal law convictions. These data can be processed only on the basis of a person's written consent, except in cases where data processing is strictly prohibited by the law even if there is a written consent. Exceptionally, the data concerning one's affiliation to a political party, health condition and social welfare benefits may be processed without obtaining the person's consent, but only if it is explicitly prescribed by the law.

Chapter III of this Act regulates special rights of persons whose data are being processed: the right to be informed about data processing; the right to access and inspect the data being processed; the right to get a copy of the processed data, as well as some personal rights related to access and inspection of the processed data.

Finally, the protection of an individual's personality is provided is Article 31 PDPA. In case the publication of personal data in a public newspapers or some other media violates the right or legally protected interest of an individual, the person may ask the responsible editor and/or publisher to provide information about his/her personal data that are being processed, may seek access to inspect these data and obtain copies of these data, except in cases which are explicitly prescribed by the law.

The power of supervision and control over the implementation of this Act is vested in the Commissioner for information of public importance and personal data protection, who

is obliged to keep the obtained data confidential both in the course of exercising his constitutional powers and after the expiry of his term of office.

5.2. The Patients' Protection Act

This Act [28] regulates the protection of patient's personal data and privacy. Thus, the Act envisages two rights pertaining to patients' privacy protection. Article 14 establishes the patients' right to privacy and confidentiality of information. Thus, a patient has the right to privacy and confidentiality of all personal data that have been given to the authorized medical staff, including data related to one's health condition, diagnostic and therapeutic procedures throughout the course of medical treatment.

Article 21 regulates the right to the confidentiality of data related to a patient's medical condition. According to the law, the data from medical files on a patient's health condition fall into the category of very sensitive personal data. Therefore, medical professionals and other personnel that may have access to such data are obliged keep and respect the confidentiality of these data and the patients' right to privacy. In particular, the category of sensitive data may include personal data on one's genetic code or substances that may be used for establishing the ancestor's identity.

5.3. Other relevant legislative acts

The Public Information and Media Act[29] protects personal dignity and the right to authenticity (Article 79), as well as the right to private life and personal profile record (Articles 80-82). This Act also regulates the issues related to obtaining a response to requested information as well as the correction of information which constitutes a violation of some right or interest of an individual (Article 83 and further). In case of such a violation, the Act envisages the right to legal protection (Article 101 and further).

Article 14 of the *Act on Free Access to Information* of Public Importance[30] bans the access to information which may infringe on the right to privacy, reputation or any other right, except in special cases where the disclosure of such information is a matter of public interest.

The Republic of Serbia has enacted a number of legislative acts directly pertining to the the protection of personal data, such as: the Identity Card Act[31] and the Passport Acts,[32] which envisage the use of biometrical personal data in new documents. Yet, without an adequate control system for using and processing these personal data, there is a real danger that the constitutional right to personal data protection may be violated.

[28] The Patients' Protection Act, "Official Gazette RS"No 45/2013
[29] The Public Information and Media Act,"Official Gazette RS"No 83/2014 and 58/2015
[30]"Official Gazette RS" No 120/2004, 54/2007, 104/2009 and 36/2010
[31] The Identity Card Act, "Official Gazette RS" No 62/2006 and 36/2011
[32] The Passport Act, "Official Gazette RS" No 90/2007,116/2008, 104/2009 and 76/2010

5.4. The Criminal Code of the Republic of Serbia

The Serbian Criminal Code[33] has a key role in the protection of personal data in Serbia. In Chapter 14, the Code envisages a set of criminal offences against human rights and freedoms.

Unauthorized disclosure of confidential information (Article 141) in the course of providing professional services (by doctors, lawyers, etc.) is punishable by imprisonment not exceeding one year, or a fine.

A violation of confidentiality of letters, parcels and communications (Article 142) is punishable by a fine or imprisonment for a period not exceeding 2 years. If the confidentiality right has been violated by an employee in the course of performing his/her official duty, he/she shall be imposed a sentence of imprisonment ranging from 6 months up to 3 years.

Unauthorized wire-tapping and recording (Article 143) will be punished by a fine or a term of imprisonment ranging from 3 months to 3 years. If the act is committed by an employee in the course of performing his/her official duty, he/she shall be imposed a sentence of imprisonment ranging from 6 months to 5 years.

Unauthorized photographing (Article 144) is punishable by a fine or a term of imprisonment not exceeding year. If the act is committed by an employee while performing his/her official job, he/she shall be sentenced to a term of imprisonment not exceeding 3 years.

Unauthorized publication and disclosure of another person's documents, images and recordings (Article 145) is punishable by a fine or a term of imprisonment not exceeding 2 years. If the act is committed by an employee in the course of performing his/her official duty, he/she shall be sentenced to a term of imprisonment not exceeding 3 years.

Unauthorized gathering of personal data (Article 146) will be punished by a fine or a term of imprisonment not exceeding 1 year. If the criminal act is committed by an official employee while performing his/her official duty, he/she shall be sentenced to a term of imprisonment not exceeding 3 years.

6. CONCLUSION

Modern information technologies pose great challenges to privacy and personal data protection. Different means of communication and diverse online activities lead to a great exchange of information, including personal data which may be used for various autorized or unauthorized purposes. There is no dispute that the privacy of an individual is very fragile in the contemporary digital world. The privacy of information is a rare commodity in cyberspace. Thus, the key issue is whether privacy actually exists at all.

Digital technology has brought us into a situation of being surrounded by machines that constantly monitor every step we take and collect data which can be used for unauthorized purposes. Our personal data and privacy are further endangered by continuous emergence of new or improved devices. For example, "Smart TV" sets are connected to the Internet like computers: they are not just receivers; they enable two-way communication. Thus, they can observe us and send certain data to service providers.[34] The imminent reality of such

[33] The Criminal Code of the Republic of Serbia,Official Gazette RS" No 85/2004, 88/2005-corr. 107/2005-corr. 72/2009, 111/09 and 121/2012

[34] In mid-November 2013, a British IT consultant Jason Huntley established and proved that the LG television-set in his living room endangered the privacy of his family. Being connected to the Internet, this "Smart TV"

technological developments poses a serious threat to privacy of an individual and personal data protection.

In the EU and in Serbia, the normative framework concerning the right to privacy is quite adequate. The difference is that Serbian legislation is more suitable for an analogous than for a digital environment. In practice, privacy is violated in many different ways. First of all, video-supervision is widely and illegally used in many public places. Violation or unauthorized use of citizens' personal data in the area of commerce, telecommunication, banking, health and insurance sectors is also quite common.[35] There are numerous cases of stolen identity or false representation on social networks, unauthorized publication of another person's photographs or video documents, password abuses of e-mails and Internet profiles.

In essence, the Internet promotes rights and freedoms but it also endangers them. Instead of being the key subject in the modern society, a man is increasingly turning into an object of social developments. In spite of all proclamations and efforts exerted to preserve human rights and freedoms, we seem to be running out of options in terms of protecting our privacy.

The contemporary trends in the development of new information technologies and global economy have contributed to a new sovereign position of technology in the society. It has given rise to a new media culture, which is widely supported by electronic media and in collision with ethical norms underlying our human society. In the era of globalization, the right to privacy (as one of the fundamental human rights) is gradually vanishing. The ultimate result is personal identity crisis.

In the near future, "a left earring may communicate with a right earring via low-orbiting satellite; and a digital planet will look and feel like the head of a pin" (Negroponte, 1998: 12).

Once set in motion, digitalization will progressively gain momentum. It may not be far-fetched to presume that the day will come in not-so-distant future when man will be "chipped"; namely, a human being will become a biometric product comprising a set of digital data.[36]

Scientists predict that, in a near future, the Internet will be accessible via contact lenses which will enable us to see not only the faces of persons we communicate with but also their biographies. We are most likely to use computers or drive a car merely by using our thoughts. Ultimately, the Internet may be replaced by "the Brain-Net" (brain-to-brain communication) or the ANN-networks (artificial neural networks simulating the operations of the human brain).

Information will be a highly valuable asset in the future. The growing value of information will eventually generate manifold violations of personal data and privacy rights. It is often said that the world will be managed by those powers who own the largest amount of information rather than those who have the largest amount of ammunition.

Finally, in order to provide for some kind of online privacy protection, it is necessary to take serious and comprehensive measures including a combination of legislative, political,

---

set sent data about all programmes watched by the family to the producer in Korea, who made a great profit from the announcers. The data included contents from Huntley's private video collection and recordings from family celebrations.

[35] It may be illustrated by a number of recent forfeiture cases involving the enforcement of judicial decisions by "collecting debt" from debtors' bank accounts, on the basis of unauthorized publication of data about bank clients.

[36] A case has been recorded in Sweden recently where a person who had a chip implant in his elbow managed to going through all customs formalities without any documents.

technological (cryptographic) methods and self-regulation (deontological or ethical codices, etc.). Apart from providing for the development of new technologies, the major task will be to protect man's right to privacy and freedom of expression (Smolović-Green, 2010: 13).

Acknowledgement: *This paper is the result of scientific research conducted within the project "Harmonizing the Serbian Legislation with the EU Law", which has been financially supported by the Faculty of Law, University of Niš, in the period 2013 – 2018.*

REFERENCES

1. Lea, M. & Spears, R. (1995). Love at first byte? Building personal relationships over computer networks. In J. T. Wood & S. Duck (Eds). Under-Studied Relationships: Off the Beaten Track. Thousand Oaks: Sage. 197–233.
2. Loon, A.v. (2010). Regulatorni okvir Saveta Evrope za sadržaje na Internetu [Council of Europe Regulatory framework on Internet contents]. Зборник: Слобода изражавања на Интернету. Београд. 58 – 63.
3. Maisl, H. (1987). Etat de la Legislation Française et Tendences de la Jurisprudence Relatives à la Protection des donnees Personnalles. *Revue Internationale de Droit Comparé*. No. 3. 581.
4. Negroponte, N. (1998). Biti digitalan [Being Digital]. Beograd: Clio.
5. Прља, Д., Рељановић, М., Ивановић, З. (2012). *Интернет право [Internet Law*]. Београд.
6. Schafer, A. (1980). Privacy - A Philosophical Overview. *Aspects of Privacy Law*. Ed. by Dale Gibson. Toronto.
7. Simons, G.L. (1982). *Privacy on the Computer Age*. Manchester.
8. Смоловић - Греен, С. (2010). Приватност и Медији [Privacy and the Media]. *Зборник: Слобода изражавања на Интернету*. Београд. 66 – 75.
9. Спасић. В. (2010). Онлајн безбедност [Online Safety]. Зборник радова Правног факултета у Нишу. No. 6. 77 – 102.
10. Спасић, В. Стевановић, Б. (2015). Услуге рачунарства у "облаку" - предности и ризици [Cloud Computing Services: benefits and risks]. *Услуге и заштита корисника*. Крагујевац: Правни факултет. 121 – 141.
11. Strangelove, M. (1994). The Internet, electric gaia and the rise of the uncensored self. *Computer-Mediated Communication Magazine*. 1 (5). http://sunsite.unc.edu/cmc/mag/1994/sep/self.html
12. Татомировић, Т. (2009). Виртуелна комуникација у будућности – употреба и злоупотреба [Virtual communication in the future: use and abuse]. Scribd, http://www.scribd.com/doc/9981281/Buducnost-virtuelnog-komuniciranja
13. Watzlawick, P., Beavin, J. H., Jackson, D.D. (1974). Menschliche kommunikation. *Formen, störungen, paradoxien*. Bern: Vierte, unveränderte auflage.

EU Law

1. *European Convention on Human Rights and Fundamental Freedoms* (1950), Article 8
2. *International Covenant on Civil and Political Rights* (1966), Article 17
3. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (1981)
4. *Directive 95/46/EC on the Protection of Individuals with regard to the processing of personal data and free movement of such data* (1995)
5. *Declaration on Freedom of Communication on the Internet* (2003)

Serbian legislation

1. Ustav Republike Srbije [The Constitution of the Republic of Serbia]. *Službeni glasnik RS [Official Gazette RS]*. No. 98 (2006).
2. Закон о заштити података о личности [The Personal Data Protection Act, Articles 8, 12, 13, 16, 17, 31] *Službeni glasnik RS [Official Gazette RS]*. No. 97 (2008), 104 (2009 - др. закон), 68 (2012), Одлука УС, 107 (2012).

3. Закон о правима пацијената [The Patients' Protection Act, Articles 14, 21], *Službeni glasnik RS [Official Gazette RS]*. No. 45 (2013).
4. Закон о јавном информисању и медијима [The Public Information and Media Act, Articles, 79, 80'82, 83 onwards, 101 onwards]. *Službeni glasnik RS [Official Gazette RS]*. No. 83 (2014), 58 (2015).
5. Закон о приступу информацијама од јавног значаја [*Act on Free Access to Information* of Public Importance], *Službeni glasnik RS [Official Gazette RS]*. No. 120 (2004), 54 (2007), 104 (2009), 36 (2010).
6. Закон о личној карти [The Identity Card Act]. *Službeni glasnik RS [Official Gazette RS]*. No. 62 (2006), 36 (2011).
7. Закон о путним исправама [The Passport and Travel Documents Act]. *Službeni glasnik RS [Official Gazette RS]*. No. 90 (2007), 116 (2008), 104 (2009), 76 (2010).
8. Krivični zakonik Republike Srbije [The Criminal Code of the Republic of Serbia]. *Službeni glasnik RS. [Official Gazette RS]*. No. 85 (2005), 88 (2005 - ispr.), 107 (2005 - ispr.), 72 (2009), 111 (2009), 121 (2012), 104 (2013), 108 (2014).

NORMATIVNI OKVIR ONLINE PRIVATNOSTI U EVROPSKOJ UNIJI I SRBIJI

Informatička tehnologija omogućila je mnoge pogodnosti korisnicima, ali je ozbiljno dovela u pitanje privatnost pojedinca. Pogrešno je mišljenje da se bilo koja radnja može obavljati na Internetu (dakle onlajn), a da to ne bude primećeno i/ili zabeleženo. Koristeći različite Internet servise, korisnici svesno ili nesvesno, aktivno ili pasivno ostavljaju određene lične podatke o sebi. Neko može te podatke kasnije neovlašćeno upotrebiti ili zloupotrebiti i tako povrediti privatnost pojedinca.

U Evropskoj Uniji postoji sasvim zadovoljavajuća regulativa u oblasti zaštite privatnosti u digitalnom okruženju. Uz to, u težnji da se ide u korak sa tehnologijom stalno se donose novi propisi. Sa druge strane, uprkos činjenici da postoje određeni zakoni koji regulišu pojedine segmente privatnosti, zakonodavstvo u Srbiji je još uvek primerenije analognoj tehnologiji, odnosno okruženju, a manje digitalnom. Sa tog razloga bilo bi potrebno izvršiti odgovarajuća upodobljavanja.

Bez obzira na kvalitet i konzistantnost zakonodavstva, privatnost pojedinca u mrežnom okruženju je veoma krhka i permanentno, na različite načine izložena kršenju. To je prosto neminovno i veoma je teško boriti se sa tim. Krucijalni razlog za ovakvo stanje predstavlja sama struktura Interneta i sistem njegovog funkcionisanja. Ovo pre svega, zato što Internet nema centralizovana mesta kontrole. Takođe, dokazivanje digitalnih povreda je znatno teže nego utvrđivanje nezakonitih radnji učinjenih na klasičan način. Na kraju, visoko stručni sajber prestupnici mogu ukloniti i sve dokaze, što je u fizičkom svetu nemoguće.

Na kraju, čini se da nije realno očekivati visok stepen onlajn privatnosti. Ovo sa razloga što internet, s jedne strane promoviše slobode (pa i privatnost), ali ih istovremeno i ograničava.

Ključne reči: *Internet, lični podaci, privatnost, povreda*.