MEST Journal
DOI 10.12709/mest.06.06.01.13

INTERNATIONAL AND SERBIAN LEGAL FRAMEWORK OF THE RIGHT TO PRIVACY IN CYBERSPACE

Vida Vilic
Clinic of Dentistry Nis, Nis, Serbia

JEL Category: **K14, K24, K33**

Abstract

With the usage of the Internet, transmission of digital data and information has become even easier. As soon as certain personal information is published on the Internet, it becomes public and available to anyone to read and use. The right to privacy in its origin indicates a person's desire not to be disturbed. Privacy on the Internet consists of the right to personal information, and informational privacy includes informational security, meaning that informational society exists when everyone can decide how to dispose of his personal data, regarding his needs and community requirements, and it is often referred to as 'e-privacy'. The right to be informed must not affect the right to privacy, within the legal framework on both international and national levels. Being that computer crime has become a transnational problem, it is clear that the mechanisms to counter fight this type of criminality should not merely focus on the changes in national criminal law legislation, but should also involve undertaking appropriate technical, structural and educational measures, followed by ratification and implementation of relevant technical and legal instruments in order to minimize the risk of computer misuse activities.

Keywords: *Privacy, e-privacy, information privacy, right to be informed, legal framework*

1 INTRODUCTION

The right to personal privacy in the virtual space has been endangered by the development of modern technology. The fact that it is possible to collect, store, distribute, reproduce, publish and make personal data available to a wide range of people in cyberspace, developed a feeling of insecurity and lack of safety and protection. A few decades back, while computer systems were just in a phase of development, all these data were transferred from the virtual space in a variety of digital media, making the 'digital dossiers' of each internet user. The development of information technologies enabled the connection between different databases, which further increased the risk of endangering the privacy of individuals.

The usage of the Internet made transmission of digital data and information even easier. Initially, the 'primitive' internet has allowed the anonymity of users - the information is forwarded via IP address, so both the sender and the recipient can keep their anonymity. Today's 'progressive' model of internet communication is entirely different and even more dangerous for the privacy of its users

Address of the author:
Vida Vilic
vila979@gmail.com

2 THE PRIVACY OF SOCIAL NETWORK USERS

The use of information and communication technologies has infiltrated into all spheres of human life (Vilic, V., & Radenkovic, I., 2016), and social networks have created detailed and comprehensive database of personal details from the lives of its users (Viegas, F. B., 2005) and this database is daily, complemented with increasing number of information that is public and accessible to all stakeholders of virtual interaction in cyberspace. As soon as certain personal information is published on the Internet, it becomes public and available for anyone to read and further use and the owner of the information loses control over the fact who has the access to his intimacy and the information that is published. The users of social networks and internet in general usually overestimate their power of having control over the information they have published via social networks because they are unaware of their technical ignorance and the possibilities of privacy settings of user profiles.

There are four main reasons why there is a possibility of violating the right to privacy on social networks (Shah, M., 2013):

1 The imperfection of social network users, related mainly to the imperfections of a man as a human being and his need to share his own privacy with other people and the lack of awareness that the privacy does not exist in cyber;
2 Flaws in the programs (software) that social networks use, resulting in lack of privacy protection mechanisms on social networks, making users' privacy unprotected from all direct malicious attacks;
3 Inadvertent disclosure of personal data;
4 Conflict of interest between social networks, advertising companies, and the users.

Internet users can protect their privacy in cyberspace through controlled disclosure of personal information. By the definition given by Joseph Cannataci, data protection means the protection of an individual from abuse or improper use of personal data by any other person, organization or the state (Cannataci, J. A., 1987).

Privacy on the Internet consists of the right to personal information concerning their preservation, use, safety and displaying this personal information in the cyberspace, as well as identification of information relating to particular website visitors. This is why the privacy in virtual space can be defined also as 'limited access to personal data / limited control of personal data' (Tavani & Moor, 2001. in Spinello, R., 2011:44). Privacy can be defined as 'a state of carefully limited access to personal data' (Spinello, R., 2011:44). Any behavior different from those described above can result in privacy rights abuse and the collection of sensitive personal information about someone without their consent and knowledge that the personal information could be manipulated.

In electronic communications, privacy can be understood as 'freedom from systematic observation, recording of activities and personal data, or the right of individuals to self-determine when, how and to what extent information about their communications can and should be available to others' (Nikolic, M., 2009).

Besides the fact that other social networks and Internet users could violate the privacy of another user by manipulating its personal sphere, the state also can often misuse the personal data stored in the virtual space. In this case, the question is to which extent is the collection of personal data necessary and justified for the functioning of a modern society, as well as the scope of the other social network users' right to use and to access other people's personal information. Edward Snowden, a former computer analyst, in June 2013 revealed that he collected certain information about how the official state governments violate the right to privacy of internet users in the virtual world, by unlawfully monitoring them and publicly disclosing their personal information.

3 THE CONCEPT OF PRIVACY AND INFORMATIONAL PRIVACY

In its origin, privacy indicates a person's desire not to be disturbed (Nikolic, M., 2009). Discussing the theoretical concept of privacy and the very content of that concept, Anglo-Saxon literature referred to Judge Louis Brandeis and attorney Samuel Warren and their article 'The Right to Privacy', published in 1890, in which they defined the most accurate and the most specific concept of privacy,

as the 'right to be left alone' (Surlan, T., 2014). This concept of privacy is protecting the privacy of personal autonomy, moral and physical integrity, the right to choose a lifestyle and the way of life, the interaction between people etc.

The right to privacy is one of the fundamental human rights, it is recognized both on the international and constitutional level, it is incorporated both in public law and civil law provisions, obligatory for everyone (lat. *Erga omnes*). The right to privacy allows the individual to selectively show to other people as much as that individual wants (Jovanovic, S., 2014: 94). Privacy in electronic communications includes the collecting, processing, and dissemination of information about users to third parties, whereby the individuals who record and publish their activities and personal data, determine when, how and to what extent should and can make available to others (Jovanovic, S., 2014: 94). The central point of this multidimensional structure of the right to privacy consists of the urge to retain personal data private and to prevent other people to interfere. Confidentiality of information that users share with others in virtual space should not be compromised: the user needs to be sure of the identity of the information sender and that received information is identical to the originally sent message. Any deviation from this rule reduces the trust of users.

Privacy, as such, has many critics. According to one, the right to privacy does not exist, because any interest protected as the private right may be equally well protected by some other human right, first of all under property ownership or property rights, or the right to physical integrity and security (Thomson, J. J., 1975). Other critics refer to the argument that the right to privacy that wishes to be protected, is not economically profitable (Posner, R., 1981), i.e. the protection of this right is not based on any known legal doctrine (Bork, R., 1990). The third critics are the feminist critique of the right to privacy, which refers to postulate that the special emphasis on the need to protect the right to privacy is actually harmful to women, because this right could be manipulated in order to control women and to make women under the constant domination of men, under the guise of their own wish to be protected (MacKinnon, C., 1989).

Privacy can be reviewed and defined from several different aspects: as a political right, as a civil right and as a right that exists to protect the interests of citizens (Barnes, S., 2006). As a political right, the right to privacy can be defined as 'security of the citizens that the state will not interfere with their personal civil rights' (Schement, J. R., & Curtis, T., 1995: 136). Privacy as a civil right does not mean to hide something from someone, but to control something that belongs to an individual, its autonomy, and integrity, or as 'the right to control what details of its' own life will be familiar to others' (Garfinkel, S., 2000:4). Concerning the limitations of the privacy right, it is essential to what extent one can reveal the privacy of an individual without violating the privacy.

The right to privacy, as an individual right, can be understood as controlling, editing, managing and deleting personal published information when the owner of the information decides so (Westin, A., 1970). In the context of social networks, privacy and personal information include all information that one individual can publish on its public profile, including photos, comments, information about the daily actions and friendly gatherings, etc. (King, J., Lampinen, A., & Smolen, A., 2011). From this point of view, the possibility for abuse the right to privacy on social networks can be viewed through two conceptual categories: social threats or organizational threats (Krasnova, H., Gunther, O., Spiekermann, S., & Koroleva, K., 2009).

Privacy can be divided into spatial, communications and informational privacy (Boban, M., 2012: 595). *Spatial privacy* refers to maintaining a privacy in someone's home and other space in which people lead their own lives separately from the others. This type of privacy includes the respect of the right to have its' own space, both within home and family and in the workplace. *Communications privacy* refers to privacy of correspondence and other forms of communication with other people. *Informational privacy* is closely related to the development of information technology and refers to collecting personal data about internet users, to managing these data and to their further use. It refers to a need of an individual, a group or an institution to independently decide when, how and what information about themselves they wish to cede to others, but also include information security, when

each individual can decide how to dispose of his personal data, regarding his needs and community requirements. Informational privacy consolidates legal values of protecting the rights of an individual in a society that have developed information technology and the concept of personal data, referred to as 'e-privacy'.

The right to informational privacy includes the right to be informed, the right to an adequate use of personal data, the right to control these data, the right of correction published data and the right to use legal remedies and appeals (Drakulic, M., 1996: 65). From this point of view, the possibility of abuse of the right to privacy on social networks can be viewed through two conceptual categories: social abuse or organizational abuse (Krasnova, H., Gunther, O., Spiekermann, S., & Koroleva, K., 2009: 97). *Social (interpersonal) abuse* may relate to individuals who use social networking and without authorization 'transfer' and 'spread' other people's personal confidential information to unauthorized third parties (e.g. When someone, using the status of friends on social networks, transfer someones' personal data to a third party or prospective employer). *Organizational (institutional) abuse* is imposed by accepting the rules of the social network itself, because of the existing threats to the privacy of users by the companies funding the social networks through its services and platforms (e.g. selling personal information about social networks' users to advertising companies).

Despite the daily development of information technologies and new forms of potential abuse, Internet users expect that each information system has the capacity to reject attacks that can endanger system data. Also, the problem is the fact that users voluntarily and on their own initiative publish a large number of their personal information in cyberspace, without thinking about whether this information will be misused or not. The most common methods of disrespecting the right to privacy on the Internet is unauthorized access, collection, and processing of personal data of users, misuse of collecting data, the interception of sending information etc. However, according to a European Commission report on EU citizens' experience and perceptions of cybersecurity issues in 2012 (European Commission - Special Euro-barometer 404: Cyber Security Report, 2013: 89), the majority of respondents expressed that they have changed their behavior when using the Internet by not giving their personal data or not opening e-mails that comes from the unknown people and whose in the content seems suspicious. One-half of respondents said that they have changed their password in the past year, several times for security reasons, especially due to the increase of security of personal data and financial transactions carried out via the Internet. One-third of respondents said that at least once have received an email that it could be considered as an internet fraud, that they were victims of a potential attempt of identity theft, hacking attempts or potential cyber violence or sexual harassment.

4 THE RIGHT TO PRIVACY AND THE RIGHT TO BE INFORMED

Internet, since the 1970's, transformed the society into three specific areas: privacy, freedom of expression and the free flow of information. Technological progress allows processing, storage, accessibility and transfer of information in any form, regardless of distance, time and quantity. Despite the fact that there is no generally accepted definition of the term 'information society', in the related literature there are three constitutional elements of the information society: information and knowledge; the proliferation of information and communication technologies; access and use of information and communication technologies (Alen, R., 2009, p. 174). Information or information flow is important both from a social as well as the psychological and legal aspects, and on the other hand, the right to public information and the right to privacy are basic human rights guaranteed by both international and national legislation, primarily as constitutional rights.

When we talk about the right to privacy, we need to emphasize that the right to be informed must not affect the right to privacy. Legal regulation of these two rights should lead to their balance and adjustment. In some cases, there is a legitimate interest of the public to have access to certain information and the legitimate interests of the individual to be 'left alone'. In such cases, it is necessary to estimate what principle should be given priority, but in such a way that the second principle affirms to the maximum possible extent.

The past few years, there is considerable debate in the feminist literature about freedom of expression, information published via the Internet and social networks, Internet censorship, as well as on how the Information communication technology (ICT) affects the awareness of women's rights. Information communication is not gender neutral since women are often excluded from the process of technology development and its application because of the cultural prejudices that exist. Better access to information and networking that ICT provides could contribute significantly to the process of economic empowerment of women, on counter fighting patriarchal stereotypes and cyber violence, in order to create a more equitable society.

Therefore, at the 59th session of the United Nations Commission on the Status of Women in the report by APC (Association for Progressive Communication) as the main objectives of the WRC (Women's Rights Program) was highlighted the struggle for women's freedom of speech, the prevention of 'technological violence' against women, counterfeit negative consequences of technological development and media reporting in a way that does not threaten the privacy of women. It was also mentioned that privacy is an important segment in the struggle for women's rights and that censorship of information about sexual health, reproductive rights and violence against women prevents women from exercising the rights guaranteed by international documents.

In the digital world, female privacy is compromised and significantly associated with new and fearsome forms of cyber violence. Female journalists and bloggers are most of all exposed to severe forms of online harassment, which often have sexual and violent character and it is often justified by freedom of speech (Vujnovic, A., 2015). Studies show that in the digital environment female journalist is three times more likely to be targets of very aggressive and insulting comments than their male colleagues (Zikic, B., 2014). As a participant in a public speech and information, in the process of giving their own opinion and attitude, female journalists are often victims of threats, sexual harassment, sexism and cyberstalking, which shows that online communication is a visible trend of gender inequality. Female journalists vividly describe what will happen to them: rape, murder, assault on children and other family members. Emma Watson has received threats that her nude photos would be published immediately after she appeared at the United Nations in the campaign 'His For Her'. British journalist and feminist Caroline Criado-Perez launched a public action for women to appear on British banknotes, after which she was exposed to such online campaign that she had to cancel her Twitter account because she could not bear the vulgar threats that she will be killed, massacred and first of all raped. Azerbaijani female journalist, characterized in cyber media as a 'national traitor', has received similar threats which included a description of the act of rape and the location where she will be buried after she got murdered. (See: Zikic, B., 2014). Threats, offensive comments, aggressive behavior and degradation occur in brutal forms in cyberspace, resulting in their removal from digital space. Therefore, it is very important that social networks take certain measures to prevent these phenomena, but also to build the feminist movement (both offline and online), which will strive to protect the privacy of information and fair media reporting.

5 PROTECTING THE RIGHT TO PRIVACY IN INTERNATIONAL AND NATIONAL DOCUMENTS IN REPUBLIC OF SERBIA

The right to privacy as a fundamental human right has a special significance in the corpus of human rights. The international normative framework of the right to privacy consists of more international instruments: The Universal Declaration of Human Rights (1948), International Covenant on Civil and Political Rights (1966), European Convention on Human Rights - Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 1950), Convention on the Rights of the Child (1989), Resolution of the Parliamentary Assembly of the Council of Europe (1970), Charter of fundamental rights of the European Union (2000), EU Directive 95/46/EC (1995), Directive of the European Parliament and Council Directive 97/66/EC(1997), Directive on privacy and electronic communications 2002/58/EC (2002).

These documents make a general regulatory framework for the establishment and understanding of the right to privacy, but they differ in the way of application, interpretation and sanctioning. Protecting privacy rights at the international and national level refers to the private sphere of life, family life, home and correspondence, honor and reputation of individuals.

1. *The Universal Declaration of Human Rights* is the first comprehensive document about human rights, with undoubtedly an influence on the later adoption of international conventions on human rights and domestic legal provisions at the national level. Article 12 of the Universal Declaration provides that 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks'.
2. *The International Covenant on Civil and Political Rights* also contains provisions on the protection of the right to privacy, as in Article 17 provides that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation'.
3. *The European Convention on Human Rights* is the most important international legal document on human rights in the territory of Europe, which, together with its Protocols, establishes the most comprehensive and the most effective system for the protection of human rights and fundamental freedoms. Given that private life is an intimate sphere of life, every individual has the right to live as he wants, to be protected from the public and from the attack on the spiritual and moral integrity, to have the right to establish communication and emotional relationship with other people in order to satisfy the needs and for personal development. Therefore, the Convention as one of the fundamental rights and freedoms provides the right of the individual to respect his/her private and family life, his home and his correspondence, with 'no interference by a public authority with the exercise of this right except such as 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' (article 8). The Convention provided also certain restrictions on the right to privacy, as stated in the Article 8 of the Convention. This defines the scope of private life: the right to respect private life shall be limited to the extent as the individual himself/herself brings his/her private life into contact with the public or in connection with other protected interests. Related guarantees concerning the right to privacy are reflected in the freedom of thought, conscience and religion (article 9) and freedom of expression (article 10).
4. *The Convention on the Rights of the Child* in article 16 provides that 'no child shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his or her honor and reputation'.
5. *The Resolution of the Parliamentary Assembly of the Council of Europe* defines right to privacy as a set of individual rights (live with a minimum impact on the third unauthorized parties that concerns private), family life at home, physical and moral integrity, honor and reputation, libel inadmissibility, unauthorized publication of private photographs, protection from disclosure of information that are part of secret communicated between individuals.
6. *The Charter of fundamental rights of the European Union* in article 8 paragraph 2 stipulates that the data processing needs prior consent of the owner of personal data. This way, the application of these provisions prohibits the social networks to take any action in order to change the purpose and objective of the published information, without the consent of the owner of personal data.
7. *Directives of the European Union.* The European Union has adopted several Directives concerning the protection of privacy through the protection of personal data. The most comprehensive is *Directive 95/46/EC*, as an alternative vision to protect the right to

privacy, particularly through the protection of individuals as consumers, as well as the protection of privacy which is threatened by the economic interests of large corporations and the state. The directive applies to automatically and processing collected data, as well as to data collected by traditional methods that do not require computer processing. Personal data must be collected in accordance with the law and fairly, and should only be used for exactly certain purposes envisaged in the law. The Directive aims to encourage the development of national legislation that would allow proper protection of collected personal data. This construction of the right to privacy, especially emphasizes the protection of the privacy rights due to computer misuse and in the virtual space. The legal application of this directive in practice is very important in cases of violation of the right to privacy on the social networks. Most of these violations are: the lack of unambiguous and explicit consent of the social network user to the data processing and collecting, collecting the data without having given opportunities to users how to respond in case of violation and by setting the privacy option through the Privacy policy option settings, which is often at a very low level of protection and not easily replaceable.

8. When it came to the intensive development of telecommunications and computer procession of personal data, the need occurred to specify the conditions under which personal data can be disposed, stored and distributed (Tomic, N., & Petrovic, D., 2009), so the European Parliament and the Council in 1997 passed the *Directive 97/66 / EC*, and a few years later the *Directive 2002/58 / EC* concerning the processing of personal data and the protection of privacy in the electronic communications sector. This directive was changed in 2009 with the amendments concerning violation of confidentiality of personal data, the use of 'cookies' and the authority of the operators' to take action against broadcasters' unsolicited messages and spamming.
9. *The Anti-Counterfeiting Trade Agreement – ACTA (2011)* represented one of the threats to privacy and the right to free access to information in the cyberspace. The agreement was signed on October 01, 2011, by the following countries: USA, Japan, Canada, Morocco, New Zealand, Singapore and South Korea. The agreement was signed in 2012. by some of the member states of the European Union: Austria, Belgium, Bulgaria, Czech Republic, Denmark, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Slovenia, Luxembourg, Malta, Poland, Portugal, Romania, Spain, Sweden and the United Kingdom. Although the aim of this Agreement at first hand was to tighten the fight for the respect of intellectual property rights as well as combating Internet piracy and forgery of any kind, some member states have begun with allegations that this Agreement does violate some of the basic human rights such as the right to privacy, freedom of expression, the right to medical treatment and access to medication and the right to a fair trial (Maletic, V., & Dakic, J., 2012: 774). The final text of the agreement contains provisions relating to the protection of intellectual property rights that could lead to the adoption of inappropriate national legislation in the field of Internet communications and online services, which can seriously endanger the privacy and freedom of expression of Internet users. In particular, the worry was that the provisions of the Agreement could lead to a number of consequences, such as the violation of basic human rights and the rule of law (like forwarding the collected personal data of Internet users to certain institutions without previously issued court decision), non-standard ways of sanctioning that are not in accordance with the rule of law,[1] the suspicion

[1] Article 27 of the Agreement stipulates the obligation of States to support the implementation of criminal and civil sanctions in the Internet environment, which even include the police procedure and punishment outside regular court proceedings, based at the request of private companies that might even implement end execute these sanctions. The agreement, on the other hand, does not provide effective legal remedies for protection in order to protect fundamental human right on a fair trial by the principles of the rule of law.

that there is a mass surveillance of personal data that are not in accordance with the Charter of human rights,[2] the undermining of democracy, fundamental freedoms and the rule of law,[3] the introduction of severe criminal punishments etc. The Agreement caused considerable discussion by the European Parliament, because of the threats to fundamental human rights. The European Union decided to forward this document to the European Court of Justice, in order to declare whether there is indeed a possible violation of civil human rights and that the implementation of this Agreement is in accordance with the fundamental rights and freedoms of the European Union.

10. In the legislation of the Republic of Serbia, different dimensions of the right to privacy are guaranteed by the Constitution of the Republic of Serbia (Ustav Republike Srbije, 2006), Law on Personal Data Protection (Zakon o zastiti podataka o licnosti, 2008), Act on Free Access to Information of Public Importance (Zakon o slobodnom pristupu informacijama od javnog znacaja, 2004), Electronic Communications Act (Zakon o elektronskim komunikacijama, 2010), Public Information and Media Act (Zakon o javnom informisanju i medijima, 2014) and the provisions of the Criminal Code of the Republic of Serbia (Krivicni zakonik Republike Srbije, 2005). All these documents together form the overall regulatory framework for the establishment and understanding of the right to privacy but differ in the way of application, interpretation and sanctioning. Protection of privacy rights at the international and national level refers to the private sphere of life, family life, the inviolability of the home and correspondence, honor and reputation of individuals.
    a. Constitution of the Republic of Serbia *(Ustav Republike Srbije, 2006)* guarantees the right to be informed (article 51), meaning that everyone has the right to be accurate, completely and timely informed about all issues of public importance and that everyone, in accordance with the law, has the right to access information held by the state authorities and organizations entrusted with public authorization. Several articles of the Constitution of the Republic of Serbia are guaranteeing the rights arising from the right to privacy. Privacy encompasses, inter alia, the right to inviolability of the home, the right to secrecy of letters and the protection of personal data. According to the constitutional provisions, the right to inviolability of the home shall be inviolable and no one may, without the written court decision, either enter against the will of the owner or specific permission or search it without a court warrant. The Constitution also guarantees the inviolability of the secrecy of letters and other means of communication, with the exception based only on a court decision (article 41).
    b. Law on Public Information and Media *(Zakon o javnom informisanju i medijima, 2014*) states in article 1 that the public information is accomplished through the media, but that the private information or personal records may not be disclosed without the consent of the person whose private life the information contains, or of the person whose words, image, or voice it contains, if such publication could be harmful to the person's right to privacy or any other constitutional right. Minors are in particular protected by that provision (article 80). This Act has, however, provided a long list of exceptions, which

[2] The agreement requires from the Internet intermediaries to disclose personal data of all those who think they may have done some legal violation, which makes problem for citizens across Europe. Because of this contention, the Agreement is criticized that it gives priority to various state holders, and not to the freedom of speech, privacy and some other fundamental rights. Another criticism is due to the possibility that the agreement may allow monitoring of millions of individuals and internet users, regardless of whether they are under suspicion or not.

[3] The provisions of the Agreement endanger the freedom of speech, the right to privacy and freedom of communication and association, by giving the priority to the protection of the private sector and the implementation of repressive measures aimed at protection of intellectual property, which is in contradiction with the European Convention on Human Rights.

imposes limits on the rights to privacy (article 82).

c. Law on Personal Data Protection *(Zakon o zastiti podataka o licnosti, 2008)* provide the conditions for collection and processing of personal data, the rights of individuals and the protection of the rights of individuals whose data is collected and processed, the restrictions of third unauthorized parties for protection of personal data, the procedure before the competent authority for protecting the personal data, data security, data records, transfer of data out of the Republic of Serbia and supervision over the implementation of this law (Article 1). Article 3 defines the concept of personal data as any information relating to a civilian individual, regardless of the form in which it is expressed (paper, tape, film, electronic media, etc.) at whose order, behalf or benefit the information is stored, the date of the information creation and storage, the way of learning the information (directly, by listening, watching, etc.), or indirectly (through the access to a document containing the information) or regardless of other characteristics of the certain information. The aim of the Act is that, when processing personal data, every individual, regardless of citizenship, race, age, gender, language, religion, political or other opinion, nationality, social origin and status, property, birth, education, social status or other personal characteristics, ensure the realization and protection of the right to privacy and other guaranteed rights and freedoms (article 2). The Act explicitly states that its provisions are not applicable in cases when data are published in the public media and different kind of publications, which lead to conclude that the Act cannot be applied to the protection of users of social networks in the misuse of published personal data by a third party. In article 8, the Act state that data processing is not allowed when an individual has not given clear consent to the processing of data. This way, the Act still leaves the possibility for protection of personal data that have been published and for which there is no explicit consent given by the owner, which is in full compliance with the prohibition of an Article 146 of the Criminal Code of Serbia which sanction unauthorized collection of personal data. The exception can be made only when it is necessary to protect someone's life, health or physical integrity, as well as for the purpose of compliance with legal regulations (article 13).

d. Law on Free Access to Information of Public Importance *(Zakon o slobodnom pristupu informacijama od javnog znacaja, 2004)* provides the right of access to information of public importance held by public authorities, in order to achieve and protect the public interest to be familiar with certain data and to attain a free democratic order and an open society. This Act also establishes the function of the Commissioner for Information of Public Importance, as an autonomous state body whose duty is, among other things, to monitor compliance with the obligations of the authorities regarding the collecting the information of public interest and to give reports to the public and the National Assembly.

e. Law on Electronic Communications *(Zakon o elektronskim komunikacijama, 2010)* defines a series of concepts that relate to electronic communications (‘Definitions’, article 4). The Act set up a number of provisions regulating the issue of privacy, personal data in electronic communications, delivering data and the protection of confidentiality, security and integrity of public electronic communications networks and services, confidentiality of electronic communications, lawful interception and data retention.

f. Criminal Code of the Republic of Serbia *(Krivicni zakonik Republike Srbije, 2005)* incriminates every violation of privacy rights done by the authorities, other individuals and institutions, including the mass communication. In all criminal acts and offenses, the target of a criminal act may vary (an apartment, room, person, letter, shipment, file, photo, a computer), but the object of protection is the same – the privacy. Legal protection of the right to privacy is a subsidiary in its nature, which means that in most cases it applies only when privacy protection cannot be achieved by any other means. Criminal Code specifies the protection of privacy rights by providing certain legal measures which

protect the following rights: (1) the privacy of belief and religion (violations of freedom of religion and performance of religious rituals - article 131); (2) the privacy of home (violation of principle of the inviolability - article 139, unlawful search - article 140); (3) personal data (unauthorized disclosure of secrets - article 141, unauthorized collection of personal information - article 146, disclosure of business secrets - article 240, unauthorized access to a protected computer, computer network and electronic data processing - article 302, violation of proceedings confidentiality – article 337, disclosure of business secrets – article 369); (4) the privacy of letters and personal correspondence (violation of the secrecy of correspondence and other items - article 142); (5) the privacy of personal conversation (unauthorized wiretapping and recording - article 143); (6) the privacy of personal character and personal life (unauthorized photographing – article 144, unauthorized publication and presentation of someone else's file, portrait and images – article 143); (7) personal honor and reputation (an insult - article 170); and (8) the privacy of family life (disclosure of personal and family matters - article 172).

6 CONCLUSIONS

The principle of controlled disclosure of personal information is the best way to protect the privacy of all Internet users. Users who want to protect their privacy, even more, could try to achieve complete Internet anonymity - to use the Internet without giving an unauthorized person the possibility to connect to someone's Internet activities involving its personal identity. 'Posts' on social networks and published personal information could be harmful to privacy of the individual because the information (blogs, images and web pages) that were once posted on the Internet last forever and can not be removed from the virtual space.

Being that computer crime has become a transnational problem triggering impacts that reach far beyond the borders of any singular country and go deeply into the cyberspace, it is clear that the mechanisms to counter fight this type of crime should not merely focus on the changes in national criminal law legislation, but should also involve undertaking appropriate technical, structural and educational measures (Vilic, V., 2015), as well as adoption of relevant international technical and legal instruments and ways of raising awareness regarding importance of the information that can potentially generate a risk for the emergence of computer misuse activities.

According to all of the mentioned above, it has become obvious that the protection of the privacy of the internet users and the security of information and communication technologies are not solely a problem of guaranteed human rights and freedoms, but it also represents a serious socioeconomic, political and security issue for each national legislation. Clearly, addressing privacy and security issues in electronic communications requires a comprehensive approach, involving a wide range of stakeholders that must match many, often different needs and interests. Considering the development of the legislation of the European Union, together with the national legislation of the member states, Republic of Serbia has made a major shift in the past 12 years, but it still has a lot of European standards for the protection of privacy and security of information and communication technologies to deliver and to meet.

WORKS CITED

Alen, R. (2009). *Informacijsko upravno pravo*. Hrvatska: Hrvatska javna uprava, 9

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11* (9). doi:http://dx.doi.org/10.5210/fm.v11i9.1394

Boban, M. (2012). Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom drustvu. *Zbornik radova Pravnog fakulteta u Splitu*, 49 (3), 575- 598.

Bork, R. (1990). The Tempting of America: The Political Seduction of the Law. New York: Simon and Schuster

Cannataci, J. A. (1987). Privacy and Data Protection Law: International Development and Maltese Perspectives. Norwegian University Press: Complex series 1/1987

Charter of fundamental rights of the European Union. (2000).

Convention for the Protection of Human Rights and Fundamental Freedoms. (Roma, 1950). *Sluzbeni list SCG - Medjuarodni ugovori,* 9/2003

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995).

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. (1997).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector – „Directive on privacy and electronic communications". (2002).

Drakulic, M. (1996). *Osnovi kompjuterskog prava*. Beograd: Drustvo operacionih istrazivaca Jugoslavije – DOPIS

European Commission - Special Euro barometer 404: Cyber Security Report. (2013).

Garfinkel, S. (2000). Database nation: The death of privacy in the 21st century. Sebastopol, Calif.: O'Reilly

International Covenant on Civil and Political Rights. (1966). *Sluzbeni list SFRJ.* No. 7

Jovanovic, S. (2014). *Privatnost i zastita podataka na internetu*, Ministarstvo unutrasnjih poslova Republike Srbije: Tvining projekat EU – zbornik Veze cyber kriminala sa iregularnom migracijom i trgovinom ljudima. Retrieved January 21, 2017, from https://www.scribd.com/document/329419991/Cyber-Kriminal-Iregularne-Migracije-i-Trgovina-Ljudima

King, J., Lampinen, A., & Smolen, A. (2011). Privacy: Is There An App for That? *Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA*. Retrieved January 23, 2017, from https://www.truststc.org/pubs/864.html

Krasnova, H., Gunther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social Networks. *Identity in the Information Society*, 2 (1), 39-63.

Krivicni zakonik Republike Srbije. (2005). Sluzbeni glasnik RS no. 85/2005, 88/2005, 107/2005, 72/2009, 11/2009, 121/2012, 104/2013, 108/2014

MacKinnon, C. (1989). *Toward a Feminist Theory of the State*. Cambridge: Harvard University Press

Maletic, V., & Dakic, J. (2012). Internet, socijalne mreze i ljudska prava. *INFOTEH-JAHORINA* 11 (2012), 771-776

Nikolic, M. (2009). Prakticni aspekti zastite privatnosti korisnika i bezbednosti elektronskih komunikacionih mreza i usluga u Srbiji. Retrieved January 22, 2017 from http://www.telekomunikacije.rs/arhiva_brojeva/peti_broj/milan_nikolic:_prakticni_aspekti_zastite_privatnosti_korisnika_i_bezbednosti_elektronskih_komunikacionih_mredja_i_usluga_u_srbiji_.305.html#_ftn18

Posner, R. (1981). *The Economics of Justice.* Cambridge: Harvard University Press

Resolution of the Parliamentary Assembly of the Council of Europe. (1970). Council of Europe, Cons. Ass: Twenty-First Ordinary session (Third Part), Collected Texts, Strasbourg, 1979.

Schement, J. R., & Curtis, T. (1995). Tendencies and tensions of the information age: The production and distribution of information in the United States. The USA, New Brunswick, N.J.: Transaction Publishers

Shah, M. (2013). Online Social Networks: Privacy Threats and Defenses. *Springer*, vol. XVI

Spinello, R. (2011). Privacy and Social Networking Technology. *International Review of Information Ethics*, Vol. 16 (12/2011), 41-46

Surlan, T. (2014). Medjunarodnopravna zastita prava na privatnost, Srpska pravna misao, doi: 10.7251/SPM1447047S

The Anti-Counterfeiting Trade Agreement – ACTA. (2011).

The Universal Declaration of Human Rights. (1948).

Thomson, J. J. (1975). The Right to Privacy. *Philosophy and Public Affairs*, 4, 295–314

Tomic, N., & Petrovic, D. (2009). Drustveno umrezavanje i zastita privatnosti korisnika interneta. *XXVII Simpozijum o novim tehnologijama u postanskom i telekomunikacionom – PosTel 2009, Beograd.* Retrieved January 15, 2017 from http://postel.sf.bg.ac.rs/simpozijumi/POSTEL2009/RADOVI%20PDF/Menadzment%20procesa%20u%20postanskom%20i%20telekomunikacionom%20saobracaju/9.%20N.%20Tomic,%20D.%20Petrovic.pdf

Ustav Republike Srbije - Constitution of the Republic of Serbia. (2006). *Sluzbeni glasnik RS no. 98/2006*

Viegas, F. B. (2005). Blogger's expectations of privacy and accountability: An initial survey. *Journal of Computer-Mediated Communication*, 10 (3), 12th ser.

Vilic, V. (2015). Mechanisms for Protecting the Right to Privacy and Personal Data on Social Networks. Synthesis 2015 - International Scientific Conference on ICT and E-Business Related Research, Belgrade, Singidunum University, Serbia, 2015, 10-13. doi: 10.15308/Synthesis-2015-10-13, ISBN 978-86-7912-595-8

Vilic, V., & Radenkovic, I. (2016). Possibilities of Protecting Personal Data Published on Social Network Sites in the Light of the Law on Personal Data Protection. Synthesis 2016 - International Scientific Conference on ICT and E-Business Related Research, Belgrade, Singidunum University, Serbia, 2016, 62-65. doi: 10.15308/Sinteza-2016-62-65

Vujnovic, A. (2015). Kako informacijsko –komunikacijska tehnologija utjece na zenska prava. *Vox Feminae*, 3-8/11

Westin, A. (1970). *Privacy and Freedom*. London: Bodley Head

Zakon o elektronskim komunikacijama. (2010). *Sluzbeni glasnik RS no. 44/2010, 60/2013, 62/2014*

Zakon o javnom informisanju i medijima. (2014). *Sluzbeni glasnik RS no. 83/2014, 58/2015*

Zakon o ratifikaciji Konvencije UN o pravima deteta. (1990). Sluzbeni list SFRJ – Medjunarodni ugovori no. 15/90, Sluzbeni ist SRJ- Medjunarodni ugovori no. 4/96, 2/97

Zakon o slobodnom pristupu informacijama od javnog znacaja. (2004). *Sluzbeni glasnik RS no. 120/2004, 54/2007, 104/2009, 36/2010*

Zakon o zastiti podataka o licnosti. (2008). *Sluzbeni glasnik RS no. 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US, 107/2012*

Zikic, B. (2014). 'O online komunikaciji: intervju sa dr Snjezaom Milivojevic, *Srpski kulturni centar 'Danilo Kis'*. Retrieved January 24, 2017 from http://dkis.si/o-online-komunikaciji-intervju-sa-prof-dr-snjezanom-milivojevic/

Received for publication: 30.07.2017
Revision received: 29.10.2017
Accepted for publication: 10.01.2018

How to cite this article?

Style – **APA** *Sixth Edition:*
Vilic, V. (2018, Jan 15). International and Serbian legal framework of the right to privacy in cyberspace. (Z. Cekerevac, Ed.) *MEST Journal, 6*(1), 119-131. doi:10.12709/mest.06.06.13

Style – **Chicago** *Sixteenth Edition:*
Vilic, Vida. 2018. "International and Serbian legal framework of the right to privacy in cyberspace." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 6 (1): 119-131. doi:10.12709/mest.06.06.13.

Style – **GOST** *Name Sort:*
Vilic Vida International and Serbian legal framework of the right to privacy in cyberspace [Journal] // MEST Journal / ed. Cekerevac Zoran. - Toronto : MESTE, Jan 15, 2018. - 1 : Vol. 6. - pp. 119-131.

Style – **Harvard** *Anglia:*
Vilic, V., 2018. International and Serbian legal framework of the right to privacy in cyberspace. *MEST Journal,* 15 Jan, 6(1), pp. 119-131.

Style – **ISO 690** *Numerical Reference:*
International and Serbian legal framework of the right to privacy in cyberspace. **Vilic, Vida.** [ed.] Zoran Cekerevac. 1, Toronto : MESTE, Jan 15, 2018, MEST Journal, Vol. 6, pp. 119-131.