Center for Open Access in Science ▪ https://www.centerprode.com/ojls.html
Open Journal for Legal Studies, 2018, *1*(1), 9-24.
ISSN (Online) 2620-0619 ▪ https://doi.org/10.32591/coas.ojls.0101.02009v

Users' Considerations About Possibilities of Self-protection on Social Networks

Vida Vilić

Clinic of Dentistry, Niš

Received 16 February 2018 ▪ Revised 8 May 2018 ▪ Accepted 18 May 2018

Abstract

The modern world of the Internet has changed significantly with the emergence of social networks. With their popularity and a large number of users, social networks have created a kind of "control" of the everyday activities of people, their habits, their movability and socializing. In Serbia, social networks became popular in 2006, while in 2007 the real expansion of social networks begins. The Internet and social networks provide countless opportunities for getting to know new people, acquiring and developing personal and professional relationships, creating different social circumstances; but the opportunities for abuse/misuse of the Internet and social networks also increased. Discussing the abuse/misuse of the Internet and social networks, arose the issue of protecting individual personal rights – the right to privacy, and about how the users of social networks can contribute in prevention of privacy violation. Certain groups of people are more likely to be exposed to privacy violation.

Keywords: social networks, social networks' users, privacy, information privacy, privacy protection.

1. Introduction

1.1 *The scope of perceived problem*

The Internet is being used by many people all around the world, who communicate with each other, enter into different social relations and liaisons, and develop personal and professional relationships for communication, social networking, and participation in different social events. According to the Statistical Office of the Republic of Serbia, 63.2% of households owned a computer in the household in 2014, while 62.8% used the Internet (Statistical Office of the Republic of Serbia, 2014). The invention and development of the computer are one of the most outstanding and fascinating results of human thinking and innovation: computers are omnipresent, absolutely invaluable in all areas of work (Vilić, 2013). The Internet is a global information system in modern society; it is the World Wide Web, or the "network of networks", which consists of a large number of separate computers connected in a network structure. As a global worldwide network, the Internet gives a global dimension to the virtual space, which means that it provides an interface between any two points on the planet through cyberspace (Vilić, 2017: 1). Concurrently, cyberspace represents a social space created by merging two types of communication: communication through computer networks and business communications, supported by a computer system.

Correspondence: Vida Vilić, Zetska 6/63, 18000 Niš, SERBIA. E-mail: vila979@gmail.com.

In the short history of the Internet, one of the most powerful innovations is the emergence of social networks, which further expand the possibilities of communication between people, no matter where they are. Some Internet applications have given rise to issues concerning the protection of privacy, opening the debate whether social networks actually serve commercial interests or create new communication opportunities and connect people around the globe. Individual privacy, on the other hand, encompasses a whole spectrum of different rights, but the most exposed part of the right that relates to personal data is exposed to the abuse on the Internet. The risks of personal data abuse are primarily related to identity theft and theft through the misuse of personal data (online shopping, secure password, secure e-mail), but also on the misuse of personal data for commercial purposes (unauthorized sale, unwanted "spam" e-mails, etc.).

- The use of information technologies worldwide and in Serbia is very widespread and has a tendency for further intensive development.
- The emergence of the Internet and social networks has had a multiplier effect on contemporary life and the development of specific forms of criminal behavior, which is reflected in the abuse of information communication technology and its systems.
- Social networks on the Internet, as widespread and most popular way of communication in the modern world, made private life an integral part of public life since there is no privacy guarantee for data posted on the Internet and social networks.
- The serious lack social networks are the large exposure of users to various forms of abuse, such as identity theft, fraud, digital violence (sexual violence and harassment, peer violence, stalking, cyber mobbing, hate speech), terrorism, vandalism, human trafficking and human organs selling, piracy, as well as the replacement of the real world with virtual followed by pathological dependence on the use and abuse of the Internet.
- Privacy has got a new dimension in one new concept – information privacy, which refers to the collection, processing, storage and sharing of data about an individual.

The subject of this paper is the theoretical and empirical examination of one of the most widespread forms of computer crime, involving the violation of the right to privacy by misuse of social networks, as well as the awareness and attitudes of social network users about their exposure to personal data abuse and potential victimization.

The basic aim of the paper is to contribute to the development of a better system of protection and greater safety of social network users, based on theoretical and empirical research on computer crime and social network abuse. In order to build a better system for protecting social network users from the many types of criminal behaviors they are exposed on a daily basis, it is necessary to point out the need of criminological victim-based study of social networks, given the widespread use and the large number of abuses of data transmitted through these networks, but also the awareness of users about the vulnerability of the personal data that they publish on the Internet, the mechanisms for (self)protecting their privacy and published data, and improving mechanisms that provide protection and sanctions.

1.2 *The right to privacy and social networks – Privacy and information privacy*

In the original sense, privacy signifies the desire of a person not to be disturbed (Nikolić, 2014). In theoretical consideration of the term "privacy" and the content of this term in Anglo-Saxon literature, Judges Louis Brandeis and Lawyer Samuel Waren, firstly in 1890 in the article *The right to privacy* formulated the most accurate and well-defined concept of privacy, as "right to be left alone" (*Harvard Law Review*, Vol. 4, No. 5, in Šurlan, 2015). In this sense, privacy implies the protection of personal autonomy, moral and physical integrity, the right to choose life style and way of life, interaction between people, etc.

The right to privacy is one of the fundamental human rights, both in national and international level, guaranteed by the constitutional law, public law and civil law, which acts towards everyone (*erga omnes*) and protects person from harassment by state authorities and other people. Opposite of publicity, privacy implies secrecy and indifference. It refers to the private life of an individual in which it is justifiable to expect peace, tranquility and intimacy (Surco, 2015). The right to privacy allows an individual to selectively show as much as that individual wants (Jovanović, 2014: 94).

Theoretically, the term "privacy" has not undergone significant changes over time. However, the changes occurred in practical application of this right in the modern era, characterized by global society and information technology. The availability of information, in particular in the form of electronic data, jeopardized the respect of the right to privacy, both by individuals and by the authorities. The privacy in electronic communications involves the collection, processing and provision of user information to third parties, whereby individuals when recording activities and personal data about themselves determine when, how and to what extent the information about their private sphere needs and may be available to others (Jovanović, 2014: 94). The central place of this multidimensional construction is the desire to keep personal data personal and not freely available to other people.

Modern communication systems can fully fulfill their role if they are reliable and also available to users. Confidentiality of information shared by users in virtual space must not be compromised, and the users must be sure of the sender's identity and that the information received must be identical to the sent information. Any departure from this rule diminishes the trust of users.

Privacy can be divided into spatial, communicational and informational privacy (Boban, 2012: 595). Spatial privacy refers to maintaining 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. Communicational 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. In the narrow sense, informational privacy 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 share with others (Vilić & Radenković, 2016: 63). In a broader sense, informational privacy includes informational security, meaning that informational society exists when each individual can decide how to dispose his personal data, regarding his needs and community requirements (Boban, 2012: 582). Informational privacy consolidate legal values of protecting the rights of an individual in society that have developed information technology and the concept of personal data, referred to as "e-privacy" (Boban, 2012: 585).

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 (Drakulić, 1996: 65).

The right to privacy, as an individual right, can be defined as a control, editing, managing and deletion of information about any individual, when the owner of the personal information decides (Westin, 1970: 97). In the context of social networks, privacy and personal information include all information that an individual publishes on its profile, which includes pictures, comments, location, and social information (King, Lampinen & Smolen, 2011: 97). Thus, the possibility of abuse of the right to privacy on social networks can be viewed through two conceptual categories: social abuse or organizational abuse of this right (Krasnova et al., 2009: 97).

The most common ways of misuse the right to privacy on the Internet are: unauthorized access, collection and processing of personal data, misuse of collected data, interception of sending information. Likewise, the difficulty is the fact that users voluntarily and on their own initiative publish a large number of their personal data on the Internet, without considering whether this data will be misused or not.

1.3 *Social networks and privacy*

1.3.1 *The concept and development of social networks*

The modern world of the Internet has changed considerably with the emergence of social public networks, which have become one of the most popular services on the Internet. The virtual space was previously full of interesting and useful information, but there were very few opportunities to make this space interactive and to actively participate in the creation of data, which is enabled by the emergence of social networks. Today, there is a growing mass of social network users, who is not well informed and educated about the security risks and protection options in the cyberspace.

As the number and popularity of social networks increased, the number of users also increased, leading to the emergence of negative consequences and special form of criminality that manifests itself through social networks and virtual space in general, as well as creating a new form of dependency – Internet and social network dependency. Nowadays, social networks are connecting people around the globe. By social networking, the world is able to visualize relationships between individuals (*Top 10 Social Networking Sites*, 2012).

In the last few years, the number of social networks has grown rapidly, as the need for this kind of networking and the exchange of various content through social networks has increased. In the Republic of Serbia, available data showed the existence of the same tendency in increasing the number of social networks and their users. A survey on the use of information and communication technologies of the Statistical Office of the Republic of Serbia in accordance with the Eurostat methodology published in the business portal "Economy" (*Poslovni portal "Economy"*, 2012) in early 2012, showed that in Serbia social networks have 92.1% users of the population between 16 to 24 years.

The development of modern technologies greatly jeopardized personal privacy in the virtual space. The very fact that personal data can be collected, stored, distributed, duplicated, published and available to a wide circle of people has created insecurity and a sense of insufficient protection. A decade ago, while computer technologies were still in development, all of these data were transferred from virtual space to various digital media, making "digital files".

Social networks and social networking are the simple act of maintaining and/or strengthening an existing circle of friends and/or acquaintances, and also the tendency of spreading these circles (Kušić, 2010: 103). There are also concepts according to which social networking contributes to the quality of social interactions; complements and encourages communication in the "real" world; encourages the development of tolerance of diversity, by overcoming classical, religious, cultural, political differences; encouraging creativity, academic abilities, social skills, maturation and development of personal identity (Žunić-Pavlović, 2013: 139).

The social network is usually defined as a social structure, consisting from individuals or organizations, called "knots", which are linked to one or more specific types of interdependence, such as values, visions, ideas, financial interests, friendship, kinship, common interest, financial exchange, non-corruption, sexual relations or relationships of trust, knowledge or prestige (Vidanović, 2006: 437-438).

Social networks can also be defined as a set of internet programs that serve to connect people in communication with their friends, relatives, colleagues and clients, where their interests can be social, business or mixed (*Social networking*, 2014). Their purpose is to allow people to be a part of a virtual community in which they can develop different relationships, as well as the form of human interaction, in which, through existing acquaintances, new persons are introduced to create social or business contacts (*Sigurnosni rizici društvenih mreža*, 2015).

Often referred to as the "virtual community" or "a set of personal profiles of different people", the social network is a presentation of the Internet that connects people in one place, in order to exchange opinions, talk, share ideas and interests and create new contacts (*Social networking*, 2014). Such activity on the Internet is a characteristic social medium, whose content, unlike other media, is created by hundreds and even millions of people.

1.3.2 *The privacy of social networks' users*

Social networks have created real detailed personal databases, consisting of the lives of their users (Viégas, 2005: 18), and these databases are supplemented every day, which increases the amount of information that is public and available to all actors of virtual interaction in cyberspace. As soon as personal information is published on the Internet, it becomes public and accessible to everyone to read it and use it, so the user loses control who has insight into his intimacy and published information. Users most often overestimate their control over the information they publish via social networks, and they are not aware of their technical knowledge about the use of social networks, and the privacy settings of their virtual profiles.

The main purpose of social networks is interaction and communication in cyberspace, and users interact with each other on their own pages (so-called "profiles") and thus visualize their relationships. The relationship between the privacy and the user profile on the social network is multiple: in some cases, users want the information they publish about themselves to be accessible only to a narrow circle of people, while in some other situations users are willing to reveal their secrets to strangers and even to anonymous strangers. All this information, if misused, can cause severe consequences, ranging from identity theft to harassment and stalking, from embarrassed and shame, through various types of discrimination, or even to blackmail. Despite the awareness that all privacy on social networks may be violated, personal data are still voluntarily published on such sites.

Modern countries have faced the problem how to balance between the individual's right to privacy and the public's right to be informed; two rights that, although they act in the opposite way, are constituted parts of the foundation of a modern democratic society in which the state has the right to limit the right of individual privacy. In the context of computer crime, a new, sophisticated, unobtrusive, technically educated profile of the perpetrators of a criminal act has been created, which is difficult to confront because of its "invisibility" and "intangibility". Due to the extremely large number of users, accessibility of data, openness in communication, and insufficient legislative both on the national and international level, social networks represent a great hideaway for the perpetrators of this type of crime.

There are four main reasons why there is a possibility of violating the right to privacy on social networks (Shah, 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 cyberspace so once something gets published it goes public this very moment;

(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, such as the theft of personal data, creation of fake profiles, etc.;

(3) Inadvertent disclosure of personal data: personal data on social networks can be reached by the method of exclusion (e.g. on the basis of the year of graduation, we can conclude how old the user is, even tough it is not written in the profile);

(4) Conflict of interest: most social networks gain financial benefits from variety of ads placed by an advertising agencies, which create a conflict of interest regarding collecting personal data that advertising agencies can access.

By the definition given by Joseph Cannataci (1987), data protection means protecting an individual from misuse or inadequate use of personal data by a person, private organization or state. Internet users can protect their privacy through controlled disclosure of personal information. Those users who want to protect their privacy better, must try to achieve Internet anonymity – only this way it is possible to use the Internet without giving the possibility to a third party to connect with Internet activities for personal identification of Internet user.

Most social network users publish a large amount of private and personal data, which are immediately available to countless users around the world. Interestingly, numerous studies have shown that users of various social networks consciously share their private data via social networks: among the 4,000 students who have a Facebook profile, a small percentage has changed the basic privacy setting by which all data is public and accessible to all Internet users (Gross & Acquisti, 2005, in Utz & Kramer, 2009), and among the 20,000 profiles on the MySpace social network only 27% made their profiles private (Thelwall, 2008, in Utz & Kramer, 2009).

In electronic communications privacy can be considered as "the freedom from systematic surveillance and recording of activities and personal data; that is, the right of individuals to determine when, how and to what extent information about their communications should and may be available to others" (Nikolić, 2014). The best way to protect the privacy of all Internet users is precisely the principle of controlled disclosure of personal information. Publishing "posts" and personal information on the Internet can be detrimental to the privacy of an individual, because the information (blogs, images and web pages) that are published on the Internet is permanent.

1.3.3 *Most common rules of privacy policy on the social networks*

Social networks and companies that provide social networking sites, their wealth and popularity build by observing the behavior and relationships in society, as well as with targeted advertising, using the collected data on social network users and by monitoring their regular activities on social networks. This is precisely the reason why social networks often share the personal information and interests of its users with different companies, most often with marketing and advertising companies (Catanese et al., 2011).

Even though a large number of social network users are aware of the facts that privacy on social networks can be violated or at risk, users still publish many personal about themselves. Some of the reasons for the voluntary disclosure of personal data have been recognized as the desire for attention, disinterest or relaxed attitude towards respecting privacy, incomplete information, trust in the security of data on the social network, and trust in friends on the social network (Gross & Acquisti, 2005: 77).

Social networks with the largest number of registered users, such as Facebook, Twitter and LinkedIn, has the most number of the violation of the privacy right. The questions that arise

are whether social network users are still the owners of all the information and whether it is possible to permanently remove social networks' accounts and delete one published information?

1.4 *Security risks on social networks and recommendations for their reduction*

Accelerated technology development has enabled faster data processing and efficient functionality, as well as the availability of numerous information, while providing the individual to remain "anonymous". The famous New Yorker magazine began publishing a comic strip in 1993 that said that "... on the Internet, no one knows that you are a dog" (Hargittai, 2007: 276), and that it is difficult to reveal someone's identity on the Internet because the possibilities for the abuse are innumerable. Social networks can be misused in various ways, and the criminal act that occurs this way can take the form of any of the traditional types of criminality. The concern of the most of the Internet users is caused by the fact that their personal information are automatically generated, collected, stored, interconnected and used for various purposes, including commercial ones, as well as illegal ones (Spasić, 2010: 78).

Personal data, which are unauthorized supplied by misuse of information systems, can be manipulated in various ways. By revealing their personal data, users actually consciously renounce of the part of their privacy. Additionally, uploading of photographs can enable user identification by using the face recognition software tools, but also the location of the user in that photo. Another potential danger lies in the fact that it is not possible to delete all the information contained in the user profile on certain social networks: it is only possible to deactivate the profile, which keeps the data still stored somewhere in the virtual space.

In Europe, the number of social network users who reported being a victim of an attack on privacy on one of the social networks was about 6% (during 2009), then firstly increased to 12% (in 2010), and then in year 2011 to 15% (Cybercrime on social networks continues to climb, 2013). In the US, this figure rose from 8% in 2009 at 18% in 2011 (*Ibid.*).

Internet users can protect their privacy through controlled disclosure of personal information. Publishing "posts" and personal information on the Internet can be harmful for the privacy of an individual, because the information (blogs, images and web pages) that are published on the Internet are permanent. The misuse of data can be various, but most often, depending on the impact of potential attackers, it is characterized as active (changing the content of the information, as well as modification of network packs, production of unauthorized network packs or information flow interruption), and passive (which includes all forms of influencing the flow of information without active changes in the course itself, e.g. illegal supervision, monitoring, etc.) (Spasić, 2010: 80).

The question is to what extent the modern society requires the justification of collecting personal data, as well as the extent of the rights of other social network users when using and disposing personal data of other users. Modern countries have faced the problem of how to balance between the individual's right to privacy and the public's right to be informed: two rights that, although they act opposite, still constitute the same foundations of a modern democratic society, in which the state has the right to limit the privacy right of an individual. According to the terms of use of the most popular social networks, the use of personal data is permitted only to registered users.

The privacy on social networks depends also on the degree of control that the social networks' user has over access and use of personal data. Basically, users must accept the Terms of Use (Terms of acceptance) when accessing different social networks, before use their services. It is interesting that precisely this document often contains clauses that permits the administrators of social networks not only to store user data, but also to share them with third parties, most often marketing companies (Bangeman, 2010). The majority of users makes mistakes when they accept

these policies without previous reading, because they are incomprehensible and too complicated to the user, and often only in English language, which makes it rather difficult for the average user to understand it.

A solution that would reduce the possibility of misuse/abuse of the right to privacy on the Internet, especially on social networks, must be based on three different levels: solving social problems that result in abuse of the right to privacy, overcoming technical problems due to which it is possible for unauthorized persons to access personal data and creating an adequate legal framework and mechanisms for detecting, preventing and sanctioning committed criminal acts. The policy of each social network is to take into account the technical capabilities that would prevent or minimize the misuse/abuse of personal data (Duffy, 2006). Adequate legislation at the supranational level would facilitate the detection of violations of the right to privacy, as well as the sanctioning of the perpetrators of these criminal acts.

2. The results of empirical research

2.1 *The subject, object and the methodology of the research*

The subject of the research was to find out the considerations and attitudes of users of various social networks about the possibility of misuse/abuse of the right to privacy on the social networks, of using/not using appropriate protection mechanisms, as well as the determination of the safest methods of preventive action, in order to prevent the victimization of social network users. The main objectives of the research were: to determine the frequency of use of certain social networks by respondents and their activities on social networks; to obtain data on recognizing violence on social networks and the possibilities of protection; to determine the exposure of respondents to various forms of cyber victimization and the possibilities for timely protection of their right to privacy.

The research had the character of a pilot or a trial research and was done on a suitable deliberately chosen sample. The duration of the research was from January 2014 to April 2014, and the results of the research enabled the elaboration of a valid hypothetical basis for new, wider and deeper research. The research was conducted in two phases. In the first phase, selected social network users (612 of them) were interviewed. One part of the respondents consisted of students from selected primary schools, secondary schools and faculties, while the other part of the respondents were active users of social networks selected by sending questionnaires to certain e-mail addresses. Pupils and students filled in the questionnaires at classes and then returned them to teachers/professors. Social network users filled out the survey online by responding directly to a database that was subsequently processed and analyzed. In the second phase of the research, the collected data were selected and statistically processed, followed by analysis and interpretation of data.

For this research, the questionnaire was made, containing general questions related to the independent variables, like gender, age, education, place of residence. The second type of questions was related to: the frequency of using the Internet and communication via social networks, personal information shared in cyberspace, possible forms of abuse, misuse and violation of the right to privacy in social network communication, forms of protection that can be applied and suggested measures to prevent the violation of the right to privacy via social networks.

The data obtained by the research are encrypted and entered into the matrix. The analysis used the xi-square test to determine the statistical significance of the observed differences between the crossed features. Data processing was done in the SPSS program.

2.2 *Participants*

Considering the different structure of social network users, in order to achieve representativeness, the research was conducted by sending the questionarries to randomly selected email addresses or via social networks (217 or 35.5%), while a larger number of respondents (395 or 64.5%) were randomly selected from students of University of Niš (Faculty of Law, Faculty of Philosophy – Departments: English, Sociology and Psychology), secondary school students (High School "Stevan Sremac", High School of Arts, Food Chemistry High School) and elementary schools' students ("Bubanjski heroji", "Jovan Jovanovic Zmaj" – Malča).

The respondents were of different ages. The prevalence of 20-30 years is predominant (271 or 44.4%), which is understandable, because the largest number of active social networks' users are precisely of this age. The age range of 9-19 years (197 or 32.2%) is fairly common, while the lower numbers of respondents were in the age range between 51-60 years (15 or 2.5%) and 61-65 years (7 or 1.1%). This structure of respondents by age compared to the number of users of social networks show that the users of social networks are mostly younger.

The distribution of respondents shows a significant numerical advantage of female respondents (398 or 65.0%) compared to male respondents (214 or 35%), which is understandable, because women are more active on social networks than men. Considering that the research did not include the comparison of respondents according to the frequency of use of the social networks by gender, these data are not statistically significant.

Respondents have various education. Students (38.1%) were predominant, followed by respondents with finished secondary education (30.5%) and university degree (20.1%).

Regarding the place of residence, the majority of respondents have a place of residence in the city (87.6%), while in rural areas there are significantly fewer respondents (12.4%).

3. Results and discussion

Most of the respondents are active in two to five social networks (54.9%), while 5.4% of the respondents are active in more than five social networks. This result does not differ from general population data which show that most of the users of social networks use a larger number of social networks, indicating greater opportunities for abuse of users' privacy. Respondents who use social networks exhibit a different interest in certain social networks. The largest percentage of respondents use Facebook (23.3%), Youtube (19.8%), Skype (16%), Gmail – Google Talk (9.8%). Only 0.7% of respondents use MySpace.

When answering the question of whether they read the privacy policy on social networks, the majority of respondents answered with "Sometimes" (50.8%) or that they do not read the privacy rules at all (26.3%), which shows that this type of primary preventive protection respondents insufficiently apply. Only 21.2% of all the respondents answered that they always read the privacy policy on any social network.

The inability to indicate personal data on a Facebook profile was also seen when answering the question of whether the profile contains data on the age of the respondent. The vast majority of respondents answered that their social networks' profile show their real age (60.9%) and that this personal information exists on some of their profiles (10.0%).

The research showed that most of the respondents share within the social network pictures/videos on which they are with their friends (59.6%) or where they are alone (25.0%). Only 13.6% of respondents said that they do not upload photos or videos to social networks. This indicates that the respondents did not develop the system of self-protection of private and personal data.

Unlike in answering the previous question when respondents showed unwillingness to protect their personal data, 65.5% of respondents said that they have never shared a photo or a video of any other person without their consent.

As the reason for rarely uploading the photos and videos on social networks, most respondents (89.7%) perceived the belief that both photos and videos could easily become the subject of misuse. Much less respondents (9.0%) believe that no such misuse has been ever possible. This finding shows that respondents are largely aware of the increased risk of abuse of privacy if photos or videos are shared and stored on the social network they use.

Respondents were asked how the photos or videos shared on social network could be used for the wrong purpose. As possible types of abuse, respondents stated: identity theft and fraud; manipulating personal data; use of the photograph for the purpose of sexual exploitation, pornography and pedophilia; sexual harassment; blackmail, stalking, mocking, etc.

Even though most of the respondents were not victims of violence on social networks, they stated in their responses what, according to their opinion, can be the cause of any kind of violence in cyber community such as a social network. The cause of potential violence or violation of certain right could be: a psychological problem or frustration (135 respondents or 22.1%), courage in the virtual world because of the anonymity (50 or 8.2%), boredom or fun (37 or 6%), too much openness in communication between people who do not know each other in the real world (11 or 1.8%), absence of sanctions (5 or 0.8%), access to personal and private data (5 or 0.8%).

When asked "Do you feel safe/secure when using a social network?" most of the respondents answered that they: feel absolutely safe when using social networks (116 or 17.3%); feel safe because they have never had any inconvenience on social networks (192 or 28.6%); feel safe because they always managed to solve the problem when it happens (61 or 9.1%); mostly feel safe because they had bad experiences from which they learned to be careful (22 or 3.3%). Some respondents are very cautious when using social networks and they say they never feel safe because "the danger is always present" (92 or 13.7%).

The respondents noted that users were exposed to various threats when using social networks. The most commonly mentioned were: photography misuse (362 or 17.0%); hate speech (342 or 16.1%); threatening (305 or 14.3%); different kind of harassment (280 or 13.2%); unauthorized use of photos (278 or 13.1%); sexual harassment in chats, chat rooms or email communication (196 or 9.2%); unwanted sexual content (195 or 9.2%); stalking and forced/unwanted communication in the cyberspace (169 or 7.9%).

The respondents, in general, take care about the information they are publishing, which can be seen from the answer to the question "Have you ever published something that you were later ashamed of?". Most of the respondents (405 or 66.2%) answered that they did not, and only 23.4% responded that they published something that they were later embarrassed about.

The cautions/unreliability of the respondents when using social networks and the accuracy inaccuracy of the data they publish on social networks can be seen through the following questions:

- 114 or 18.6% made their users' profile public while 437 respondents (71.4%) did not;
- 505 (82.5%) did not write their home address on their social networks' profile and only 6.7% did;
- 398 (65%) did block a person on social networks so far;
- 232 (37.9%) deleted or disabled their profile on the social network at least once so far;

- 116 (19%) have given incorrect data about their age when it comes to communication on social networks;
- 206 (33.7%) never added an unknown person to the list of contacts/friends so far, 197 (32.2%) made it 1-5 times, 152 (24.8%) did it more than 5 times, 30 (4.9%) always add an unknown person to the contact list;
- as many as 372 (60.8%) gave information on the name and surname to unknown people, showing that the respondents are fairly sincere in communicating with sharing their data;
- 284 (46.4%) through social networks gave information to unknown people about where they work or study;
- 462 (75.5%) never gave the information about where usually go out with friends to unknown people;
- 380 (62.1%) have never sent personal photos and photos of close friends to unknown people via social network, while 188 (30.7%) always do so;
- 417 (68.1%) never sent an e-mail address to an unknown person via social networks, while 25.2% always do so;
- 546 (89.2%) never gave an information about home address and 486 (79.4%) never gave information about a phone number to unknown person via social network.

About privacy protection, the majority of respondents stated that the privacy settings were "effective, but insufficient" (221 or 36.1%) and "not effective enough to protect users" (175 or 28.6%). A smaller number of respondents (111 or 18.1%) know that privacy settings exist, but have never read it, while 38 respondents (6.2%) do not know that these rules even exist. Only 56 respondents (9.2%) stated that the rules on the protection of privacy on social networks were completely effective.

The respondents also commented about the possibilities of reporting abuse or harassment on the social network, using the report abuse buttons. The majority of respondents knows that there are rules for reporting violence or harassment on the social network, but never read them (195 or 31.9%), a slightly lower number think that these rules are not effective enough to protect users (143 or 23.4%) or that they are efficient, but insufficient (137 or 22.4%). Only 33 respondents (5.4%) evaluated the rules on reporting violence or harassment on the social network as completely efficient, while 91 (14.9%) did not know that there was a possibility of reporting violence or harassment on the social network.

Regarding the efficiency of legal protection of privacy on the Internet and on social networks in Serbia, a small number of respondents believe that they are protected by the existing legal provisions (40 or 6.5%). Most of the respondents (211 or 34.5%) think that the legislation is not completely satisfactory, cannot protect the users and that it must be changed (117 or 19.1%) or that the legislation is not bad, but do not fully protect the users (90 or 14.7%). Even 141 (23%) of respondents do not know that there are legal possibilities for privacy protection, which shows that the users of social networks must be more familiar with the legal provisions in this area.

The respondents suggested different recommendations for increasing the level of safety on social networks: introduction of appropriate relevant legislation, combined with greater activity of state authorities; reporting abuses and punishing perpetrators; education of users in order to increase their level of awareness for their own personal data; suggesting to the users to share and publish the less personal data possible; to organize education of children about the dangers that exist on social networks; to improve the policy of protecting children from all types of violence in cyberspace and on social networks; to teach social network users to protect themselves from the attacks they are exposed to; to organize and to conduct the education of

parents/legal guardians, teachers/professors in order to make them capable to detect the phenomenon of cyber violence among children/pupils/students; to prohibit access to certain websites; to establish centers that would legally and practically handle harassment, insulting and stalking in cyberspace and on social networks; to restrict the use of the Internet for persons younger than 14 years, etc.

The respondents, also as the recommendation, mentioned that the social network users must protect themselves by denying the communication with persons they don't know in real life, as well as better checking the identity of the persons whose user profile they are communicating with.

4. Conclusion

The emergence of the Internet, as an interpersonal medium and the projection of society into a virtual space, was created as the consequence of social transformation, mobility and basic social need of people to interact and to share information. By using the Internet, new connections can be established between people, the old ones can be renewed, values and norms can be spread, a new culture created, money earned, but it could also be manipulated, abused, stolen and cheated.

Nowadays, social networks are the way of connecting people around the globe. In addition to the advantages that the Internet and social networks provide, there has been an increase in abuse related to virtual space. A large number of users are exposed to daily victimization if the data transmitted through social networks are abused or misused. In connection with cyber abuse, the issue of protecting individual personal rights – the right to privacy – was raised. Certain groups of people are particularly exposed to cyber abuse of privacy, for example celebrities, those who are most commonly used by certain social services and whose behavior is deviant or criminal.

Most of the increasingly frequent global privacy attacks have the goal the abuse/misuse of the personal and private information about an individual. Based on this information, it is possible to identify an individual, persons' personal life, group affiliation, everyday activities and behavior – it is possible to reconstitute the life and personality of each subject based on the collected data. The privacy on the Internet includes the right to personal information relating to the storage, use and displaying the personal information over the Internet, as well as the identification information relating to the visitor of a particular website.

Confidentiality of information shared by users in virtual space must not be compromised, and the users must in each particular case be sure of the sender's identity and that the information received must be identical to the sent information. Any departure from this rule diminishes the trust of users and may violate their right to privacy.

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, can try to achieve Internet anonymity – this way, it is possible to use the Internet without giving the possibility of a third party to connect with the Internet activities, in order to personally reveal the identity of a certain Internet user. Publishing "posts" and personal information on the Internet can be detrimental to the privacy of an individual, because the information that are published on the Internet (blogs, images and web pages) is permanent. The fact is that most of the acts of computer crime are committed because of ignorance or insufficient knowledge of the social networks' users about the computer systems. Some of the most common causes of abuse might be poorly programmed computers and computer systems, set of codes that are easy to detect and with low level of security protection, as well as the lack of collective awareness of how effectively all computer and communication systems are vulnerable and likely to collapse. In order to overcome

this segment of the problem, education of Internet users should be done at different levels (schools, Internet providers, media, manufacturers and distributors of computer equipment and programs, etc.), because most of the users make mistakes that often lead to the acts of computer crime.

In order to reduce the number of abuse and misuse of computer systems which endanger the privacy rights of their users, it is necessary to create appropriate legal mechanisms consisting of a legislative for detecting, preventing and sanctioning these socially unacceptable criminal behavior. Also, it is very important to report all criminal offenses related to computer crime to the competent authorities, in order to reduce the "dark figure" of the criminality rate and to achieve better preventive action that would lead to recognition and monitoring of such acts, as well as overcoming the problem of non-reporting of these crimes.

Acknowledgements

At this point, I would like to thank all those people who contributed to the implementation of this research, because without their contribution it could not have been completed.

Conflicts of interest: none.

References

Bangeman, E. (2010). *2010. Report: Facebook caught sharing secret data with advisers*. Retrieved 4 October 2017, from http://arstechnica.com/tech-policy/2010/05/latest-facebook-blunder-secret-data-sharing-with-advertisers/.

Boban, M. (2012). Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu [Privacy right and right for access to information in modern information society]. *Zbornik radova Pravnog fakulteta u Splitu*, *49*(3), 575-598.

Cannataci, A. J. (1987). *Privacy and data protection law: International development and Maltese perspectives*. Complex series.

Catanese, A. S. et al. (2011). *Crawling Facebook for social network analysis purposes*. Retrieved 14 February 2018, from http://arxiv.org//1105.6307.pdf.

Cybercrime on social networks continues to climb (2013). Retrieved 4 October 2013, from http://www.net-security.org/secworld.php?id=11464.

Drakulić, M. (1996). Osnovi kompjuterskog prava [Foundations of computers' law], Beograd: Društvo operacionih istraživača Jugoslavije – DOPIS.

Duffy, M. (2006). *A dad's encounter with the vortex of Facebook*. Retrieved 23 January 2018, from http://www.time.com/time/magazine/article/0,9171,1174704,00.html.

Gross, R., & Acquisti, A. (2005). *Information revelation and privacy in online social networks*. Proceedings of the 2005 ACM workshop on Privacy in the electronic society, ACM, retrieved 15 February 2018 from http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

Hargittai, E. (2007). Whose space? Differences among users and non-users of social network sites. *Journal of Computer-Mediated Communication*, *13*(1), 276-297.

Jovanović, S. (2014). Privatnost i zaštita podataka na Internetu [Privacy and data protection on Internet]. Tvining projekat EU – zbornik *Veze cyber kriminala sa iregularnom migracijom i trgovinom ljudima*, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd.

King, J., Lampinen, A. & Smolen, A. (2011). Privacy: Is there an app for that? *Symposium on usable privacy and security* (SOUPS), Pittsburgh, PA, USA.

Krasnova, H. et al. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39-63.

Kušić, S. (2010). Online društvene mreže i društveno umrežavanje kod učenika osnovne škole: navike facebook generacije [Online social networks and social networking in primary school students: Habits of Facebook generation]. *Život i škola*, *24*(2), 56.

Nikolić, M. (2014). Praktični aspekti zaštite privatnosti korisnika i bezbednosti elektronskih komunikacionih mreža i usluga u Srbiji [Practical aspects of users' privacy protection and security of electronic communication networks and services in Serbia]. Retrieved 30 July 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.

Poslovni portal "Economy" (2012), from http://www.economy.rs/.

Republički zavod za statistiku Republike Srbije [Statistical Office of the Republic of Serbia] (n.d.) from http://webrzs.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=2.

Shah, M. (2013). Online social networks: Privacy threats and defenses. *Springer*, XVI (2013).

Sigurnosni rizici društvenih mreža [Security risks of social networks] – Hrvatska akademska i istraživačka mreža (2015), from www.cert.hr.

Social networking (2014), from http://www.investopedia.com/terms/s/social-networking.asp.

Spasić, V. (2010). Onlajn bezbednost [Online security]. *Zbornik Pravnog fakulteta u Nišu*. Niš: Pravni fakultet, Centar za publikacije, 56 (2010).

Surco, R. (2015). Pravo na privatnost s posebnim osvrtom na internetsku društvenu mrežu Facebook [Right to privacy with special look at Facebook]. Retrieved 20 October 2017 from www.rijaset.ba/.../05_pravo_na _privatnost.

Šurlan, T. (2015). Međunarodnopravna zaštita prava na privatnost [International legal protection of privacy right]. Retrieved 28 October 2017, from www.spmisao.rs/mp-content/uploads/2014/03-tijana-surlan-pdf.

Top 10 Social Networking Sites (n.d.), from http://news.discovery.com/tech/top-ten-social-networking-sites.html.

Utz, S., & Kramer, C. N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyber psychology: Journal of Psychosocial Research on Cyberspace*, *3*(2), 1.

Vidanović, I. (2006). Rečnik socijalnog rada [Dictionary of social work]. Udruženje stručnih radnika socijalne zaštite Srbije, Društvo socijalnih radnika Srbije, Asocijacija centra za socijalni rad Srbije, Unija Studenata socijalnog rada, Beograd. 437-438.

Viégas, B. F. (2005). Blogger's expectations of privacy and accountability: An initial survey. *Journal of Computer–Mediated Communication*, *10*(3).

Vilić, V. (2013). Possibilities of privacy rights abuses in social networks and practical protective measures ("О возможньх нарушениях права на неприкосновенность частной жизни и социальных сетях и практических мерах защиты"). Интернет, власть и политика" - International scientific and practical conference »Internet – Government - Politics«, Кемерово, 2013. ЗАКАЗ No. 458. 187-192.

Vilić, V., & Radenković, 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

Vilić, V. (2017). CYBERCRIME: Basic criminological characteristics and legislation. LAP - LAMBERT Academic Publishing – International Book Market Service Ltd., member of OmniScriptum Publishing Group. -166. ISBN 978-620-2-01800-5

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

Žunić Pavlović, V., Kovačević Lepojević, M., & Mentus, T. (2013). Negativne posledice socijalnog umrežavaja na internet [Negative consequences of social networking on Internet]. *Komunikacija i ljudsko iskustvo* – tematski zbornik radova, Filozofski fakultet Univerziteta u Nišu, 137-150.


C O A S