POSSIBILITIES OF PROTECTING PERSONAL DATA PUBLISHED ON SOCIAL NETWORK SITES IN THE LIGHT OF THE LAW ON PERSONAL DATA PROTECTION

Vida M. Vilić[1],
Ivan Radenković[2]

[1]Clinic of Dentistry Niš,
Niš, Serbia
[2]Law Office „Stanković"
Niš, Serbia

Abstract:

Aside from being a typical place for everyday activities and social communication, social networks are a unique place where various types of social behaviour and interactions can be observed. The majority of social network users leave a lot of their personal data on their social network accounts as they believe that they will be visible only to their friends and good-willed users, *i.e.* that they will not be misused or perverted. Unfortunately, misuses of personal data collected by social networking sites are far from being rare. Violation of the right to privacy most often occurs on the most popular social networking sites with the highest number of registered users. The Law on Personal Data Protection of the Republic of Serbia sets out the requirements for personal data collection and processing, as well as the limits for such data collection and database creation, the mechanisms aimed to maintain security of the collected data and the issue of data keeping surveillance. The authors shall attempt to determine whether this law applies to personal data collection on the Internet and whether it can ensure adequate and efficient legal protection of users.

Key words:

right to privacy, personal data, social networks,
law on personal data protection.

1. INTRODUCTION

The right to privacy is one of the basic human rights. It is both an international and constitutional right of public and civil law significance, affecting everyone (*erga omnes*) and providing people with protection against disturbances coming from the state authorities and other people. Unlike publicity, privacy entails confidentiality and non-disturbance. It applies to an individual's private life which should justifiably involve peace and tranquillity, as well as undisturbed intimacy. [1] The right to privacy gives an individual a chance to selectively present himself/herself to the world up to the desired level. [2]

The Law on Personal Data Protection (hereinafter referred to as: the Law) [3] sets out the requirements for personal data collection and processing, the rights and protection of the rights of persons whose data is being collected and processed, limitations to personal data protection, proceedings before the authority responsible for data protection, data

Correspondence:
Vida M. Vilić

e-mail:
vila979@gmail.com

DOI: 10.15308/Sinteza-2016-62-65

security, data filing, data transfers outside the Republic of Serbia and enforcement of this Law (Art. 1). *Does this Law apply to the personal data collection on the Internet, especially on social networking sites, and can it ensure legal protection to the users?* Social networks very often share the personal data of their users with different companies, most often with the companies involved in marketing and advertising, supplying them with their users' personal data together with their interests, thus invading their personal rights and violating their privacy. [4]

2. PERSONAL DATA AND RIGHT TO PRIVACY

The use of information and communication technologies has infiltrated into all spheres of human life, work, entertainment and numerous other private and business activities, so that almost everything in the society has become available online, from signing contracts to committing crime. By the help of the Internet and other accompanying technologies our society undergoes transformation in three specific areas: privacy, freedom of expression and free flow of information. The social changes in the modern society arising from the information and communication technologies of the 1970's brought an entirely new phenomenon into limelight – the information society. Information has become an important element of the freedom and right to spread information which largely depends on the actual lawfulness and ability to manage data collections. In the modern information society, technological advancement enables processing, keeping, accessing and transferring information in any form regardless of the distance, time and quantity.

In the previous period, virtual space was full of interesting and useful information, but the instruments to make that space interactive and to actively participate in data creation were very limited. Nowadays, social networks serve as a means to connect people across the planet. Aside from the advantages of the Internet and social networking, there is a growing evidence of misuses of virtual space. One of the issues arising in connection with computer misuse is the issue of protection of each individual's personal right – the right to privacy. Certain groups of people are particularly exposed to computer misuse of privacy. These are the people who have already enabled collection of a considerable amount of their personal data through their frequent use of certain social services, or the people with deviant or criminal behaviour.

Personal assets such as life, freedom, name, honour and reputation used to be regarded as an inseparable part of one's personality. Personality rights also include the right to privacy which protects one's personal data and records connected with one's private life from public disclosure. In its original sense, privacy embodies one's wish not to be disturbed. [5] Privacy in electronic communications (involving collecting, processing and sharing the user's information with third persons) can be understood as the right not to be systematically observed and not to have one's activities or personal data recorded, *i.e.* as a right of individuals to personally decide on issues like when, how and to what degree the information on the accounts should and could be made available to others, while some authors [6] define privacy as a complex concept that encompasses personal autonomy, democratic participation, managing of one's own identity and social coordination. At the heart of this multidimensional entity there is a wish to keep one's personal data for oneself so that other people cannot access them.

In the context of social networking, privacy and personal information include all the data entered by a person in his/her profile, such as pictures, comments, data on their whereabouts, socializing and the like. [7] Some of the reasons for voluntary disclosure of personal data that some authors have recognized include one's need for attention, disinterest or a loose attitude regarding one's own or other people's privacy, incomplete presentation of information, trust in the safety of data on social networking sites, as well as trust in one's network friends. [8]

Speaking about the right to privacy, it should be emphasized that the rights observed as opposite from this right include the right to be informed and the right to access information that should not jeopardize the right to privacy. Legal regulation of these two rights should lead to their balanced and non-opposing quality. In certain cases, there is a legitimate interest of the public into gaining an insight into certain information, as well as the citizens' right to be „left alone", *i.e.* to make the data on themselves inaccessible to the public. In such cases, it is necessary to make an estimate as to which of the principles should be given priority, but in a way that would affirm the other principle to the highest possible degree.

The growing popularity of social networking sites has led to more extensive debates regarding privacy protection. Spokeo is not a classical social network, but rather a search engine for connecting people based on the data collected by aggregation. Namely, the website

contains information regarding the age, relationship status, income, data on close family members, as well as addresses of the registered users. Such information is collected from the data already existing on the Net, as entered by the social networks' users, but the site does not guarantee the data accuracy. [9]

The most frequent ways of disrespecting personal data on the Internet include unauthorised access, collecting and processing of users' data, abuse of collected data and interception of distributed data.

3. LAW ON PERSONAL DATA PROTECTION

In terms of Article 3 of the Law, personal data means any information relating to a natural person, regardless of the form of its presentation or the medium used (paper, tape, film, electronic media *etc.*), regardless of whose order, on whose behalf or for whose account such information is stored, regardless of the date of its creation or the place of its storage, regardless of the way in which such information is learned (directly, by listening, watching *etc.*, or indirectly, by accessing a document containing the information *etc.*) and regardless of any other characteristic of such information.

The purpose of the Law is to enable every natural person to exercise and have recourse to protection of their right to privacy and other rights and freedoms in the context of personal data protection (Art. 2). Under this Law, personal data protection is ensured to any natural person, regardless of their nationality and residence, race, age, gender, language, religion, political and other affiliations, ethnicity, social background and status, wealth, birth, education, social position or other personal characteristics.

It is interesting that the Law does not apply to the data available to everyone and published in mass media and publications (Art. 5, par. 1, item 1), as well as to the data published on oneself by a person capable of taking care of his/her interests (Art. 5, par. 1, item 4). The above provisions provide ground for a conclusion that this Law cannot be applied to the protection of the users of social networks in cases of abuse of the published personal data by a third person.

Nonetheless, Article 8 of the Law states that processing shall not be allowed if a physical person did not give his/her consent to processing, if processing is carried out without legal authorization, if the processing method is inadmissible or if the purpose of processing is not clearly defined. Data processing means any action taken in connection with data, including: collection, recording, transcription, multiplication, copying, transmission, searching, classification, storage, separation, crossing, merging, adaptation, modification, provision, use, granting access, disclosure, publication, dissemination, recording, organizing, keeping, editing, disclosure through transmission or otherwise, withholding, dislocation or other actions aimed at rendering the data inaccessible, as well as other actions carried out in connection with such data, no matter is those actions are automated, semi-automated or otherwise performed. Thus, the Law still leaves a chance for protection of personal data that have been published without the user's explicit approval, which is fully in accordance with a ban set in Article 146 of the Criminal Code that sanctions unauthorized collection of personal data.

The Law allows data collection without the consent of the person concerned only if such processing is necessary for the protection of anyone's life, health and physical integrity, as well as in order to ensure compliance with legal regulations (Art. 13).

4. CONCLUSION

Although a great number of users of social networks is aware of the fact that privacy on social networking sites can be violated, or at least jeopardized, a huge corpus of personal data keeps being accumulated on such sites. The existing legal regulations are not sufficiently „up-to-the-point" when it comes to defining the mechanisms for protecting the Internet users in general, particularly the users of social networking sites who willingly leave their personal data, thus making them available to the millions of Internet users throughout the world.

Each user who has an active account on any of the popular social networking sites must be aware that a danger of misusing the entered data is always present, as well as that he/she must „dose" the quantity of published personal data and decide with whom they will share data in the virtual world. The best way to protect privacy of all Internet users is the principle of controlled disclosure of personal data. The users who want better protection of their privacy may try internet anonymity as an option that gives you a chance to use the Internet without giving third persons an opportunity to connect with the internet activities for users' personal identification. The feeling of closeness that virtual space offers to its users can be very dangerous because, on the one side, the users are not always those they claim to be and do not always have good intentions. On the other hand, social

networks live on account of advertising companies with whom they share their users' personal data in order to be offered their services in return.

The protective measures that reduce the risk of misuse of the entered personal data are available on several social networks, thus reassuring the users that their data and personal information will not become available to everyone without their will and approval. Adjustment of one's privacy settings is a necessary step in using any social network, and each user has privileges to use such adjustments when leaving his/her own personal information on the Internet.

REFERENCES

[1] Surco, Ramo: Pravo na privatnost s posebnim osvrtom na internetsku društvenu mrežu Facebook, www.rijaset.ba/.../05_pravo_na_privatnos... retrieved on 20/10/2015

[2] Jovanović, Svetlana: "Privatnost i zaštita podataka na internetu", EU Twining Project – collection of works "Veze cyber kriminala sa iregularnom migracijom i trgovinom ljudima", Ministry of Interior Affairs of the Republic of Serbia, 2014, p.94, http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/Cyber%20kriminal,%20iregularne%20migracije%20i%20trgovina%20ljudima.pdf, retrieved on 23/07/2015

[3] Law on Personal Data Protection („Official Gazette of the Republic of Serbia" no. 97/2008, 104/2009. 68/2012 - decision US & 107/2012)

[4] Catanese, A. S., De Meo, P., Ferrara, E., Fiumara, G., Provetti, A.: "Crawling Facebook for Social Network Analysis Purposes", 2011., http://arxiv.org/pdf/1105.6307.pdf, retrieved on 15/02/2015

[5] Nikolić, Milan: „Praktični aspekti zaštite privatnosti korisnika i bezbednosti elektronskih komunikacionih mreža i usluga u Srbiji", 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, retrieved on 15/06/2014

[6] Cho, Hichang, Rivera-Sánchez, Milagros, Lim, Sun Sun: "A Multinational Study on Online Privacy: Global Concern and Local Responses. New Media & Society", vol.11, 2009., pp.395-416, http://nms.sagepub.com/content/11/3/395.short, retrieved on 12.11.2014.

[7] King, Jennifer, Lampinen, Airi, Smolen, Alex: " Privacy: Is There An App for That?", Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA, 2011, https://www.truststc.org/pubs/864.html, retrieved on 23/11/2014

[8] Gross, R., Acquisti A. : "Information revelation and privacy in online social networks", In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005., str. 71-80., ACM, http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf, retrieved on 15/02/2015

[9] About Spokeo, http://www.spokeo.com/blog/about, retrieved on 12/8/2012