3-rd INTERNATIONAL SEMINAR ON INFORMATION LAW, "An Information law for the 21-st century", Corfu, 25-26. June. 2010.

RIGHT ON PRIVACY IN THE REPUBLIC OF SERBIA

Dr. Nataša Tomić, Mr. Dalibor Petrović

INTRODUCTION

Fast technological development presents a challenge for the protection of personal data and the right on privacy. In this paper we have analyzed privacy protection and examined domestic and European legal acts on the privacy protection. We have analyzed privacy protection on the Internet with special regards to the most popular social networking sites (SNS).

One of the most discussed topics today, when we speak about social consequences of the new information communications technologies (ICT) utilization, and first of all Internet is certainly the problem of privacy protection of users of these technologies. Unexpected high number and speed of the data flow which those technologies have brought the danger of different forms of abuse of data transferred through ICT. That this is not the one of many groundless fears, in the best way testify the series of recommendations and guides for the protection of privacy on Internet made by different regulatory bodies throughout the world. Many public protests, different petitions, as well as official legal actions for endangerment of privacy of users of the most popular social networking sites testify about that.

Anyway the sale of personal computers in the world according to American media, has grown in the first quarter of the year 2010.[1] for 27,4% in relation to the same period of the last year because of the increased demand in Europe, Africa and in the Middle East. In our country the sale of computers has also grown. In Serbia, according to the data of the Institute for statistics of the Republic of Serbia, 46, 8% households have computer[2], and in 2006. that percentage amounted to 26,5%. While during 2006. percentage of households that have access to Internet was 18,5%, that number has been gradualy increased and in 2009. the 36,7% households in Serbia had access to Internet.[3] Today still one-third of Serbia does not have access to fast Internet, although surfers in

[1] The highest sale has realized the company »Hewlett Packard « and that is 15,3 million pieces.

[2] Personal computer is in 93,2% cases the device for access to Internet, mobile phone in 25,4% etc.

[3] According to data of Ratel (Republic Telecommunication Agency) in Serbia is registered 199 internet providers who cover almost all larger inhabited places in the country.

our country more and more follow the world trends. In the meantime, in the world in June 2009. in the research Centre Jilich in Germany the supercomputer with power of 50.000 personal computers was solemnly set in motion. It was called the Jugene[4] and it is the fastest in Europe, after Roadrunner-and Jaguar-a in the United States of America. It will be used for different purposes for example for the weather forecast and for the research of the Universe.

In the Republic of Serbia many legal acts deal with the protection of privacy of individuals and groups, and the expanded regulatory framework for the fight against these kinds of abuses exists. Additional problem represents that, by voluntary giving away of confidential personal data in their profiles, users became accomplices in these abuses. If you are not sure that you will do really well, try, at least, not to make harm, wrote A. Huxley (1894-1963).

Recently the public has been informed about many abuses, so we also found out that for Google the privacy is not a holy place. It was announced that famous American company illegaly took data from the users in Germany[5], so the question is if the same thing is happening here in Serbia.

Finally, in this paper are emphasized different recommendations for the prevention of personal data abuse.

ON THE LEGAL REGULATION OF THE RIGHT ON PRIVACY

It is important to stress that the right on privacy is one of the basic human rights. “Right to be left alone” means storing of smb's data secrecy, unless, there is an obvious need to reveal these data. This question requires carefull access in many areas (especially in the area of health and finances, but also on the occasion of Internet utilization). Riley T. has offered proposals for the protection of the man's right to be left alone [1]. These proposals are:

- internal use of information technology, development of personal policy that will protect rights of employees on privacy, contrary to the right of public to find out;
- adoption of laws and carring out of the policy which will explain the right on access of each individual organization to certain information on individuals;
- provision of mechanisms for removal or change of incorrect or obsolete information; and
- acceptance of new technology, building of the system of privacy protection immediately, and not after the problem appears.

---

[4] This supercomputer performs 1 billiard operations in second.

[5] In Germany there is a high conscience on the importance of data protection, as well as the strict legal penalties. Germany had demanded from Google to deliver them the hard discs with collected data, but this has not been done yet.

In the Republic of Serbia many legal acts deal with the privacy protection of individuals and groups, so it may be concluded that there is expanded regulatory framework for the fight against those forms of abuse.

Constitution of the Republic of Serbia[6] adopted in year 2006. guarantees the protection of personal data, and collection, keeping, processing and utilization of personal data is regulated by law.

The utilization of personal data besides the purpose for which they were collected is prohibited and punishable in accordance with law, except for the needs of the management of criminal proceedings or the protection of security of the Republic of Serbia, in the manner predicted by law. Everybody has the right to be informed about the data collected on his/her person, in accordance with law, and the right on legal protection because of their abuse.

The Constitution of the Republic of Serbia guarantees the inviolability of correspondence and other means of communication, and derogations are legal only in fixed time and on the base of the court decision, if they are necessary because of the management of criminal proceedings or the protection of security of the Republic of Serbia, in the manner predicted by law.

By the Law on the protection of personal data[7] are regulated conditions for collection and processing of personal data, procedure in front the body competent for protection of the data on person, security of data, records, taking out of data from the Republic of Serbia and supervision over the enforcement of the law. Protection of personal data is ensured to each natural person, disregarding citizenship and residence, race, age, sex, language, religion, political and other conviction, nationality, social origin, financial status, birth, education, social situation or other personal qualities. The aim of this law is to ensure to every natural person, in connection with the processing of personal data, realization and protection of the right on privacy and other rights and liberties.

With right on privacy and other personal rights deals also the **Law on free access to information of public importance**[8] which predicts that authorized body will not provide for realization of the right on access to information of public importance to the claimant, if by that would be injured the right on privacy, the right on reputation or any other right of the person to whom asked information personally refers to, unless:

1) if person agreed with that; 2) it is the person, phenomenon, or event of interest for the public, and expecially if it is about the holder of state or political function and if information is important with regard to the function that person performs; 3) if it is about the person who

[6] «Official Gazzete of the Republic of Serbia», no. 98/2006.

[7] «Official Gazzete of the Republic of Serbia», no. 97/2008.

[8] «Official Gazzete of the Republic of Serbia», no. 120/2004, 54/2007.

by his/her behavior, especially in connection with private life, gave the pretext for request of information.

Law on telecommunications of the Republic of Serbia[9] in performance of the control over carring out of activities in the area of telecommunications predicts authorization of the Agency to check, in addition to everything else, acting of public telecommunication operators in relation to duties predicted by this law in the area of privacy and security of information and undertakes measures to eliminate fixed omissions in acting of operator.

Licence, in addition to other data and conditions, contains also rules on the protection of personal data and privacy, which are specific for cerain area of telecommunications. Public telecommunication operator is obliged to undertake appropriate technical and organizational measures in order to provide for confidentiality and security of his services and it is prohibited to him to give information on contents, facts and conditions of messages transmission, except the minimum necessary for offering the services on the market or in the cases predicted by law. Data on the traffic related to individual users and which are being processed in order to establish connection, public telecommunication operator may keep and process only in the scope necessary for invoice to the user.[10] All activities and utilization of devices which endanger or disturb privacy and confidentiality of messages which are transmitted through telecommunication networks are prohibited, except when there is a consent of the user or if these activities are performed in accordance with the court order issued in accordance with law. Public telecommunication operator is obliged, as part of the system, to form, at his own expense, subsystems, devices, equipment and installations for by law authorized electronic supervision of certain telecommunications. Users of public telecommunication services or public telecommunication networks have the right on undisturbed utilization and high-quality public telecommunication service, as well as the right on privacy and security of information.

Besides mentioned laws, the Government of the Republic of Serbia during October 2006. adopted also two Strategies which, in addition to everything else, treat also the area of the protection of privacy. **Strategy for development of telecommunications in the Republic of Serbia** from year 2006. to year 2010.[11] predicts that working of national regulatory bodies includes also the protection of privacy, protection of users traffic, data on location, prevention of unwanted communication.

---

[9] «Official Gazzete of the Republic of Serbia», no. 44/2003, 36/2006, 50/2009.

[10] However, public telecommunications operator is obliged to provide for access and analysis of cited data to the authorized state bodies, in accordance with law. (Article 54. Law on telecommunications, „Official Gazette RS", no 44/2003, 36/2006, 50/2009.).

[11] «Official Gazzete of the Republic of Serbia», no. 99/2006.

Besides the right on undisturbed utilization and high-quality public telecommunication service, for users of public telecommunication services or public telecommunication networks is necessary to ensure also the right on privacy and security of information.

With aim to strengthen all aspects of security and safety of telecommunication sector the provision of multiple levels of protection of telecommunication systems from malicious attacks is performed, i. e. telecommunication systems must be safe enough to build trust of clients in electronic payment and transactions. In **Strategy for development of information society in the Republic of Serbia**[12] is pointed out that electronic networks must be ensured from hackers and viruses and must be safe enough in order to build trust of clients in electronic payment, and the issue of security must be balanced with the possible violation of privacy of citizens.

Government as the national regulator is responsible for setting of national rules for utilization of technology. They are also made of national standards which regulate privacy and security of data, like laws related to access to sources of information, national and international, including also the Internet. The main aim of the activity in the area of security infrastructure is to define and build mechanisms, like public key infrastructure, that will provide for the protection of privacy of citizens, make electronic transactions safe and increase trust in e–government. Solutions that have to be developed should be in accordance with the international standards in this area.

At the end, it is important to mention that at the moment the public hearing on the new **Law on electronic communications**[13], that should replace **Law on telecommunications of the Republic of Serbia** is under way. In contrast to the existing **Law on telecommunications** in the **Draft of the Law on electronic communications** the area of users privacy protection is mentioned in the basic provisions as well as in the principles of the new law. Besides that, one whole chapter of the Draft of the Law (XIV) is devoted exclusively to the users privacy protection and the security of electronic communications networks and services. However, the lack of regulation related to the privacy of data on Internet is still noticeable, so the existing law proposal should be supplemented in that direction.

When we speak about European legislation, we have examined few key Directives which regulate the area of protection of data security in electronic communications, and of special importance is **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 movement of such data.**[14] Free movement of goods, persons, services and capital requires not only that personal data freely circulate from one member state to another, but also that the personal

[12] «Official Gazzete of the Republic of Serbia», no. 87/2006.

13 http://www.mtid.gov.rs/upload/documents/konsultacije/zek/ZEK%20nacrt%2022.10.pdf

14 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

rights of individuals are protected. Progres in information technologies significantly facilitated the processing and exchange of these data. However, different levels of protection of rights and liberties especially the right on privacy, taking into consideration the processing of personal data collected in the member state, can prevent the transmission of those data from the territory of one to the territory of another member country. In order to remove obstacles for exchange of personal data, level of protection of rights and liberties of individuals with regard to processing of such data must be eqivalent in all member states. Principles of protection should be applied on the processing of personal data of individuals whose activities are regulated by laws of the Community, while the processing of data performed by natural persons in carring out of activities of excusively personal and family nature, like correspondence and keeping data on addresses, is excluded.

In accordance with Directive 95/46/EC member states protect the basic rights and liberties of natural persons, and especially their right on privacy with regard to the processing of personal data. Directive will not be applied on processing of personal data which concerns public security, defence, state security, including economic welfare of states, when processing relates to the issues of state security, as well as the activities of the state in the area of criminal law. This Directive will not be applied also on the processing of personal data of natural persons during exclusively personal or family activity. Member states will define more precisely, in the limits of provisions determined by this Directive, conditions under which the processing of personal data is legal.

Because of intensive development of telecommunications a need to further strengthen and state precisely conditions of. disposition, storing and distribution of personal data appeared, so during year 1997. the Directive of the European Parliament and Council on the processing of personal data and the protection of privacy in telecommunication sector (**Directive 97/66/EC**)[15] was adopted. However, the key Directive which is completely dedicated to the protection of privacy in the domain of electronic communications is so-called ***Directive on e-privacy*** or under the full title **The Directive on Privacy and Electronic Communications 2002/58/EC**.[16]

One of its main roles is to harmonize provisions of the member states necessary for provision of the same level of protection of basic rights and liberities, and especially the right on privacy, with regard to the processing of personal data in the sector of electronic communications, as well as the provision of free transmission of these data, equipment for electronic communication and services in the Community. This Directive is applied on the processing of personal data in connection with the provision of services of electronic communications in the networks of public communications inside the Community. The duty of provider of the service of electronic communications is to take appropriate technical and organizational measures in order to provide for

15 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML

16 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

security of his/her services, if it is necessary in connection with provider of the network for public communications, and with regard to the security of the network. In the case of special risks of disturbing of the network security, the provider of the service of electronic communications has to inform subscribers on the risk and when the risk is out of the spectrum of measures taken by the provider, on the possible means, pointing to the possible expenses.

By this Directive, in addition to everything else, is regulated the issue of sending of unwanted electronic mail (spam) in the European Union. The question is in what extent the protection assigned to subscribers in this Directive should be spread on the corporative subscribers? For example, according to the valid regulations when the enterprise provides for mobile phones for its employees for business purposes there is no right to prevention of unwanted marketing calls, because the subscriber is the enterprise, and not the employee. Regulations are formulated in such a way that in special circumstances the wishes of users of the service (legal person) can prevail the wishes of individual users. In order to get consent for the data processing, providers should offer to users clear information that will enable them to get explanation of presumable consequences for them in the case of consent.

However, since the phenomenon of on-line social networking appears and intensively spreads after the adoption of mentioned directives, the need emerged for making additional sub-laws that will especially deal with protection of data privacy on web platforms for social networking (PSN). In that sense, the most important act that we shall mention here is the **Opinion 5/2009** on on-line social networking adopted on the 12th of June 2009. that deals with the manner how functioning of the social sites on the network can fulfill request of the Europian Union legislation on the data protection.[17] It is, first of all, intended to give guidelines to providers on the measures that should exist in order to provide for harmonization with the European Union laws. The Opinion underlines that the service giver and, in many cases, third persons as service providers, controllers are responsible toward the users. It is emphasized that the great number of users is moving inside the purely private sphere, and in such cases rules that regulate the management of data controllers are not applied.

PRIVACY POLICY ON THE SITES FOR SOCIAL NETWORKING

The problem of the privacy protection on SNS is the subject of many research studies, discussions and recommendations of wider public, as well as of scientists, governmental and non-governmental organizations.

17 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf

The reason for such great interest for this topic lies down in the fact of unimagined speed of increase of the number of people who, more or less, ex gratia share information of different levels of confidentiality through SNS.[18] What concerns is the fact that information stored on SNS can forever stay there and like such be available to different individuals and interested groups and organizations. Besides that, information, once released through the network, is instantly transmitted and becomes globally available to everybody.

Additional problem, on which points out the majority of analysts who deal with the problem of the data privacy protection on Internet, represents the fact that users on their initiative and ex gratia give information on themselves (name and family name, addresses, phone numbers, photographies, etc.), and that in the process think little on the consequences of such acting. For example, Gross & Acquisti in their research study show that almost 82% of active users of Facebook reveal confidental information on themselves like the date of birth, number of mobile phone, address, political and sexual orientation and the name of partner [2]. Similar results reached Young & Quan-Hasse investigating the behavior of students in Canada [3]. The results show that incredible 99,35% of students use real name in their profiles; 97,4% cite the name of school they attended; 92,2% the date of birth; 83,1% e-mail address; 80% the name of the town they live in.

In addition, almost all students put their photographies on profiles (98,7%) and photos of their friends (96,1%). However students are little more careful when it comes to giving the right address (that does only 7,9%) or the number of mobile telephone (10,5%).

Such great frankness of SNS users is stimulated by the providers of these services who encourage the publication of personal data by creating illusion of their complete safety. That situation is just not so innocent, as probably thinks the majority of SNS users, testify many analysis, guides and recommendations with aim to regulate better this sphere of social activity. But, the most of all, on the possibility of data abuse, testify also concrete doubts, public petitions, and even lawsiuts against the most popular SNS, Facebook.

The first great discussion on the topic of manipulation with personal data of facebook users, happened after the introduction of the contraversial system for advertising »**Beacon»**. Introducted in November 2007, this service was set up to record the activity of all Facebook users on Internet (purchase, application for different services, etc.) and then forward these information to the list of friends from the profile of this person. The idea was to advertise companies on a more personal, personalized way, by recommending friends the services and products that their friends use.

---

[18] According to the newest report Facebook has more than 300 millions active users, http://www.facebook.com/press/info.php?statistics

After the lawsuit and under the pressure of users complaints, only two months later**,** Beacon service with apologies of the founder Mark Zuckerberg[19] becomes optional, and in September 2009. it was published that it will be completely abolished.[20]

During the year 2009. Facebook was two more times the subject of wide discussion and public complaints. New controversy (February 2009.) caused the announcement by the Facebook, that their policy concerning the privacy of data will be changed. This announcement especially excited public by one paragraph by which Facebook reserves the right to possession of users personal data even in the case when the user disables his/her profile and erases data from it. However, after many protests and wide campaigns around the world and the threat of a lawsuit, the creators of the Facebook were once more forced to give up from intended changes.[21]

Much more serious consequences for the problem of the Facebook privacy policy caused the lawsuit of one Canadian non-governmental organization dealing with the Internet policy and public interest (Canadian Internet Policy and Public Interest Clinic - CIPPIC) sent to the »Office of the Privacy Commissioner»-(OPC). This organization submitted a complaint on the Facebook users data privacy policy on several levels [4]. From the complaint for unauthorized collecting («phishing») of data on birth of users, to the complaining on unauthorized giving of users personal data to the third persons for the purpose of advertising. In the response to the complaint OPC has made several reports and during March 2009. gave 20 recommendations related to the removal of the noticed irregularities in the connection with the privacy policy of their users to the Facebook [5]. As the result of all this, the Facebook corrects one part of its privacy policy related to the standard /default/ adjustment of the security mechanisms on the profile, as well as in the field of advertising, but the important part of the complaints concerning the application of third persons, deactivation and deleting of profiles, profiles of deceased users and personal information of non-users, remained unsolved till today.

RECOMMENDATIONS FOR REDUCTION OF THE SECURITY RISKS ON THE SITES FOR SOCIAL NETWORKING

Just problems like the so far presented, created the need for adoption of appropriate standards when the privacy of SNS users data is in question. One of the most voluminous analysis of this problem was made by the European Network and Information Security Agency - ENISA. In

[19] http://blog.facebook.com/blog.php?post=7584397130

[20] http://www.dailymail.co.uk/sciencetech/article-1215470/Facebook-turns-controversial-advertising-Beacon.html

[21] http://www.cnn.com/2009/TECH/02/18/facebook.reversal/index.html

its Report «Security problems and recommendations for online social networks» from 2007. the following threats, divided in four categories [6] are cited:

- *Threats for privacy:*
- *Traditional danger for networks and the information security;*
- *Threats for identity;*
- *Social threats.*

In accordance with the identified threats ENISA gives recommendations and contra measures for increasing of the security level of persons and data and that means:

- *Recommendations in the area of Governmental regulatory policies (for example,* raising of conscience and educational campaigns),
- *Recommendations for providers and their business policy (for example,* establishing of the appropriate settings of profiles that will really protect the privacy of users),
- *Technical recommendations (for example,* providing for better control of privacy during searching of personal data)
- *and Recommendations in the area of research and standardization.*

One year later (2008) **"International working group for data protection in telecommunications",** so called **Berlin group,** published its Report and Guide on the protection of privacy, for the creators of SNS and users of these applications [7]. In this report, more famous by the name ***Roman Memorandum***, the risks for privacy and security of SNS users are especially emphasized, and in accordance with identified risks, Working group made recommendations for these who regulate, give and use services of social networking.

- *For regulatory bodies:*

1. Make possible the right on utilization of pseudonyms instead of the real names;
2. Provide for service providers who are sincere and clear in the respect of information needed for the basic service, so the users can judge if they are going to give those information, and possibility that users may not allow any secondary utilization of their data, especially not for targeted marketing;
3. Introduction of the duty of informing on breaking into the SNS users data;
4. Revision of the existing regulatory framework in regard to the management by personal data published on SNS;
5. Integration of the privacy issues into the educational system.

- *For providers of services of social networking*

1. Transparent and open informing of users;
2. Introducing the posibility of creation and utilization of profiles under pseudonym;
3. Keeping the promises given to users;

4. Default settings which are directed to privacy protection;
5. Improving the control of users over utilization of their data from profiles;
6. Introducing of appropriate mechanisms for users complaints management;
7. Improving and maintaining the systems for information security;
8. Finding and/or further advancement of measures against illegal activities, like spaming and theft of identity;
9. Offering of encrypted connections for maintainance of profiles;
10. Providers of social networking services, who operate in different countries or globally, have to respect standards on privacy protection everywhere they offer their services.

- *For users:*

1. Be careful, think twice before you publish the personal data in your profile;
2. Think well before you use your real name. Use pseudonym;
3. Respect privacy of others;
4. Be informed on the service provider;
5. Use settings which enable your privacy protection;
6. Use different identification data (user name and password) from those that you use on other sites;
7. Use possibility to control how the service provider uses your personal data;
8. Pay attention to the behavior of children on Internet and especialy on SNS.

When we speak about recommendations we should also mention here the research of OPC conducted during 2008 and which after identification of the more or less known threats on SNS, gives even 71 recommendations for the improvement of privacy protection of their users [8].

In already mentioned opinion (**Opinion 5/2009)**[22] there are series of recommendations with aim to increase the data security on PSN. The basic recommendations relate to the duties of service providers to harmonize with Directive on the data protection and to confirm and strengthen the rights of users. Very important is that service providers notify users about different purposes for which they are processing personal data.

The special attention service providers should pay on the processing of personal data of minors. It is recommended that users may use pictures and information on other individuals, but with consent of that individual and it is considered that service providers also have the duty to give advices to users of services on the right on privacy of other persons. To the providers of services on PSN, as well as to the third persons who offer different applications is suggested that it is necessary to notify users on their identity and different purposes for which they are processing personal data

22 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf

in accordance with the provisions of article 10. of the Directive on data protection including, but not only:

- utilization of data for direct marketing purposes;
- possible sharing of data with certain categories of third persons;
- review of profiles: their creating and main sources of data;
- utilization of sensitive data.

It is recommended that service providers on social networks provide for appropriate warnings to users on the risks for their privacy and the privacy of other persons when taking over information from the network. Users should be also reminded that taking over of information on other individuals may violate their privacy and the right on data protection.

It is necessary to advice users of services on social networks that if they want to take over photos or data on other individuals, that should be done with their consent. Data which reveal ethnic origin, political attitude, religious or philosophical beliefs, membership in unions or data on health or sexual orientation are considered sensitive. Sensitive personal data can be published on the Internet only with explicit consent of the subject to whom this data refer to or if the subject himself/herself made those data public.

When user does not use the service in certain time period, the profile should become inactive, i. e. invisible for other users or external world, and after certain period the data from the abbandoned account should be erased. Service providers on social networks should inform users before under taking of these steps with all means they have on disposal. Access and correction as the rights of users are not limited only to users of the service, but to every natural person whose data were processed. The members of social networks and those who are not must have means to perform the rights of access, corrections and erasing.

The basic homepage of the service provider's sites on the social networks should clearly point at the existance of the «service for settling complaints» founded by the provider because of the data protection and settling of the question of privacy and complaints of members and of those who are not.

EXPERIENCES OF SERBIA

Participation of the Internet connection is the biggest in the capital city of Belgrade and it amounts to 48,6%, in Vojvodina 37,9%, in Central Serbia 30,50%, according to the data of the

Institute for statistics of the Republic of Serbia. Of course, the significant differences are present between city and village settlements all over the country.[23]

Working group of the Register of the national Internet domains of Serbia has started to collect proposals, in order for Serbia to get the network address in Cyrillic letters, what will provide for creating and searching of the Internet sites on Vuk's[24] Cyrillic writing. As the proposal the most often appears: **срб.** In October 2009 in Seul was adopted the decision that the languages which are not written in Latin letters get their Internet domains. From the 16th of November 2009 the acceptance of new domains proposals[25] has started and till now 19 countries have delivered their proposals.

When we talk about Serbia, certain legal regulation, that should regulate the problem of privacy protection of persons and data on Internet, exists, but, besides that, in our public so far we have not heard for the lawsuits in this area. When we talk about utilization of SNS, Serbia is the first in the region by the number of registered profiles on Facebook with even million of these profiles. This number should not be mixed with the real number of SNS users which is certainly smaller, but nevertheless tells that this phenomenon is widespread among domestic users of Internet. At the other side, in contrast to the good results achieved in the field of networking, Serbia is at the bottom when we talk about the trade by Internet. Even 87,4% of Internet users in Serbia were never shopping by Internet [9], what points to the fact that SNS are not understood as potentially risky for users in the contrast to trading on Internet.

In Serbia till today research studies dealing with the protection of privacy on Internet are rare. Of course, we should mention one of the pioneer's research studies on this subject conducted by Popović V. during 2001. on more than 1073 interviewed persons.[10] Already in this early stage of Internet utilization in our country, as the results of Popović's study show, users of that time have demonstrated unexpectedly strong willingness to leave their personal data on Internet. Here we should emphasize that at that time SNS did not exist, so their frankness can not be understood as the expression of some kind of fashion, but more likely as the absence of expressive conscience on potential dangers watching for on Internet. So, even 75,7% of interviewed persons say that they would leave data on the year of their birth, profession (82,3%), sex (92,1%), etc. on Internet. One half of the interviewed persons is ready to reveal name and surname and e-mail, while even 22,4% would also reveal the home address, and little less the phone number (15,2%) too. We have to add

[23] In urban areas 46, 9% of inhabitants use Internet, and in rural areas only 22%.

[24] Vuk Stefanović Karadžić (1787-1864) is the great Serbian reformer in the field of culture.

[25] It is important for the domain to be shorter, to contain at least 2 letters. For example, Russia gave the proposal **рф** (as Russian Federation) for their domain.

also 14% of those who are ready to leave so confidential fact as it is the identification number on some of the sites.

Recent research directly dealing with SNS was conducted during 2008. by Jovanović S. with associates and it concerned student's population in Serbia and their utilization of Facebook and My Space.[11]. The research was conducted on the sample of 1664 interviewed persons and the reached results were similar to those related to their colleagues on the West. The most interesting finding is that only 5% of users keep their profile hidden for all users, while even 56% of students allow that their profile is visible by all Facebook users, no matter if they are on the list of their friends of not. The number (35%) of those who reveal full name and surname, date of birth, e-mail address or phone number on their profiles is not small.

Results of these studies show that Serbia, when we talk about behavior of their Internet users is part of the global world. Although we are shopping far less by Internet, what may be also shows unjustified fear from the risk of such form of trading, from other side the great popularity of SNS with our users and their unconcern for the possibility of manipulation with personal data shows that in the future it will be very important to work on the raising of conscience on the risks that such behavior on SNS brings.

CONCLUSION

As we have already mentioned in our country till today research studies on the protection of privacy on Internet were rare.

The social networking sites, in our opinion, are paradigm of the risky society of today. Ad captum, having in mind that Internet draws up the plans for society in its virtual shape, it is understandable that by anlogy in the virtual world of Internet are projected also the risks of the real world. However, through this paper we tried to demonstrate that, before mentioned, risks for privacy of persons and data can be reduced on several levels.

Take care, never do anything against your will, wrote Seneca.[26]

On the legislative plan solutions that could enable uninterrupted exchange of information and transactions by Internet should be offered. It is necessary to start with utilization of the electronic signature, allow identification and authorization of participants in transaction, operations with credit cards and establish jurisdiction over Internet transactions. Along with that, it is necessary to insure protection of the personal data and privacy, transfer of information through international systems, cryptographic protection and protection of users from insulting, illegal and unwanted Internet contents. In our country there are still no fundamental rights on video-

[26] Da operam, ne quid umquam invitus facias.

supervision. The Commissioner for informations of public importance and data protection of Serbia expressed his concern, because the theft of identity has dramatic proportions in the whole world.

That what can be done already now is raising of awareness of the users of the social networking sites, but not through calls for boycott of SNS, because these calls will not have results, but through the permanent promotion of personal care for data given to others at disposal, in extent in which the individual worries not to lose identity card or his mobile phone. When users understand that the personal data which they leave in the virtual space of Internet are very real and that consequences of their abuse can reflect on their real, and not virtual profiles, then they will be more careful, in the matter to whom these data can be entrusted for keeping, and to whom not.

Providers of the social networking services should also, besides the wish for getting the profit, think about those persons who indirectly bring that profit, i. e. on their users. If the mechanisms for personal data protection are not raised on the level of the really safe stay on SNS, users will start to look for alternative ways for their connection.

LITERATURE

[1] Riley T, *Privacy in the digital age*, Washington, 1997.

[2] Gross R. and Acquisti A, „Information revelation and Privacy in Online Social Networks", *ACM workshop on Privacy in the electronic society, Alexandria*, VA, USA, 2005.

[3] Young A. L and Quan-Hasse A, „Information revelation and internet privacy concerns on social network sites: a case study of face book", *Fourth international conference on Communities and technologies*, University Park, Pa, USA, 2009.

[4] http://www.cippic.ca/uploads/CIPPICFacebookComplaint-29May08.pdf

[5] http://www.priv.gc.ca/cf-dc/2009/2009-008-0716-e.pdf

[6] http://www.ifap.ru/library/book227.pdf

[7] www.datenschutz-berlin.de/attachments/.../WP-social-network-services.pdf

[8] http://www.priv.gc.ca/information/pub/sub-comp-200901-e.pdf

[9] http://webrzs.statserb.sr.gov.yu/axd/dokumenti/ict/2009/ICT2009s.zip

[10] Popović V, „*Zaštita privatnosti na Internetu kao jednom od servisa multimedijalnih komunikacija*", Magistarski rad, Saobraćajni fakultet, Beograd, 2004.

[11] Jovanović S, Drakulić M, Drakulić R, „Privatno - Javno? Sumrak privatnosti u eri društvenih mreža", *56. Naučno-stručni skup psihologa Srbije – Sabor psihologa*, Kopaonik, 2008.