PROTECTION OF PERSONAL DATA AND THE FREEDOM IN COMMUNICATIONS

Zoran Čekerevac[1], Nataša Bogavac-Cvetković[2], Milija Bogavac[3], Petar Čekerevac[4]

ABSTRACT

It seems that human rights, privacy and protection of confidentiality of communications, are never have been more discussed, and at the same time harder to preserve than today. In every city there are (hundreds) of thousands of cameras and it is virtually impossible to walk around unnoticed. While in the past century states tried to devise new ways in order to see letter contents unnoticed, today they do it (almost) publicly and without court authorizations. So, it is easy to ask: Is the world a better place? The work analyzes some protection problems while communicating over the Internet.

Key words:
Communications, human rights, data protection, property, privacy protection

ABSTRACT

Zdá sa, že ľudské práva, súkromie a ochrana komunikácie, neboli nikdy viac diskutované a zároveň ťažko dosiahnuteľné, ako dnes. V každom meste sú (stovky) tisíce kamier a je nemožné prejsť okolo virtuálne nezaznamenaný. Zatiaľ čo v minulom storočí sa štáty pokúšali vymyslieť nové spôsoby ako vidieť bez povšimnutia, dnes to robia (takmer) verejne a bez súdneho povolenia. Je teda ľahké pýtať sa: Je svet lepšie miesto? Práca analyzuje niektoré problémy ochrany pri komunikácii prostredníctvom internetu.

Key words:
Communications, human rights, data protection, property, privacy protectio

[1] Zoran Čekerevac, Prof. Dr, Faculty of Business and Industrial Management of the "Union" University in Belgrade, Serbia, zoran@cekerevac.eu, phone:+381 (11) 3391 641, fax: +381 (11) 823 24 27
[2] Nataša Cvetković-Bogavac, Prof. Dr, Faculty of Business and Industrial Management of the "Union" University in Belgrade, Serbia, nacasn@hotmail.com, phone:+381 (11) 3391 641, fax: +381 (11) 823 24 27
[3] Milija Bogavac, Prof. Dr, Faculty of Business and Industrial Management of the "Union" University in Belgrade, Serbia, nacasn@hotmail.com, phone:+381 (11) 3391 641, fax: +381 (11) 823 24 27
[4] Petar Čekerevac, MSc, Hilltop Strategic Services, Belgrade, Serbia, petar@cekerevac.eu, +381 (11) 307 6926

1 INTRODUCTION – LEGAL BASIS

According to the Law on personal data protection in the Republic of Serbia a term "'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 on 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." [1] Some other regulation acts use this term in a more extended form, for example: "Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organization has or is likely to have access." [2]

Although the personal data protection right is one of the basic human rights, in many countries it is still a relatively new concept. Even in the most democratic countries there are numerous examples of violations of this right. Very often, there appear titles as "Saudi hacker threatens to expose details of another million credit cards" [3], "Stolen Identity: A Consumer Nightmare" [4], "Ball State University confirms 80 identity theft victims" [5], etc.

The provisions of law are applied in most states to each data processing, whether it performs automatically or not. From certain provisions of the law are exempt [1]:

1. data that are available to anyone and published in newspapers and publications or available in archives, museums and other similar organizations;
2. data processed for family and other personal needs and that are not accessible to third parties;
3. data on members of political parties, associations, unions, and other organizations that are processed by these organizations, provided that the member gave a written statement that certain provisions of the Act shall not apply to the processing of data about him/her for some time, but not longer than the duration of his/her membership;
4. information that a person capable of taking care of its interests, concerning itself.

Personal data are private property and they don't belong to the "open data" category.[5] Art. 1 (1) Object of Directive 95/46/EC states: "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." [6] It is possible to discuss whether "personal data", "private data" and

[5] Meaning of the term "open data" is described in The Open Data Handbook [25]

“sensitive data” are synonyms or not, and what does “private” data means in today’s era at all.

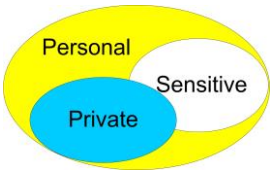

Figure 1 Personal, private and sensitive data

According to the EU Directive 95/46/EC Art 8 (1) & 8(5) the following data are in the group of sensitive data: racial or ethnic origin, political opinions, religious or philosophical beliefs, sex life, trade union membership, criminal records, as well as health data. In the USA, private is defined by the individual whereas sensitive is defined by the polity e.g. legislative process. In the UK sensitive can be considered as private or harmful. But those points of view are not fully accepted in other countries. In Australia, religion is not accepted as sensitive, and in Iceland the privacy of health data are considered more sensitive than the privacy of data about salary. [7] After research conducted on 1258 survey participants, McCullagh concluded that ‘personal’, ‘private’ and ‘sensitive’ are not synonyms, that ‘personal’ and ‘sensitive’ data are partly overlapping, and that both together are subcategories of ‘personal’ data as it is shown on figure 1.

2 COMMUNICATIONS AND DATA PROTECTION

At the present time, the use of the Internet and mobile communications are inevitable, but while using the Internet and mobile services, every person exposes their data to the risk of being taken by a person or an institution to which these data are not intended. A lot of relevant personal data is transmitted by e-mail, either as an attachment or as a part of the message content. Social networks are a gold mine for those who are engaged in collecting information. Until recently it was thought that only celebrities were subjects of monitoring, eavesdropping and other intelligence activities. The development of information technology has provided the "excess" capacities of eavesdropping systems, so lately email and social networks monitoring is practically brought down to any individual person. [8] The problems of privacy and security on the Internet came into the focus of attention when The Guardian's journalist Glenn Greenwald [9] started to publish about Edward Snowden, NSA, PRISM, GCHQ, Tempora, and monitoring of electronic communications. The publication of these secrets launched a flood of discussions that have confirmed that many (if not all) countries tapped telecommunication channels, and that the NSA only had the "misfortune" to be discovered first. [10] In this regard, in his statement, the Federal Commissioner for Data Protection, Peter Schar cited by name "Vodafone Deutschland" and "Deutsche Telekom". [11]. Certainly there are similar projects in other countries, for example in Italy, India and Canada. [12]

2.1 MONITORING OF COMMUNICATIONS

Much has been said about monitoring of all types of communications, including emails, socially networks, mobile telephony. Some of facts and discussions were presented also in [10], [13], [14], [15], and [16]. The latest in a series of controversial laws on the control of information, and that sparked mass demonstrations in major Canadian cities, is Bill C-51: "An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts", or, shortly, Anti-terrorism Act [17]. Summary of the Act is presented in the chapter Summary, but, briefly, Bill C-51 is planned to expand the powers of police and the nation's spy agency, especially when it comes to detaining terror suspects. But, like any other law of this kind, and Bill C-51 causes suspicion. The Globe and Mail, one of the oldest and most prominent newspapers in Canada, says: "On close inspection, Bill C-51 is not an anti-terrorism bill. Fighting terrorism is its pretext; its language reveals a broader goal of allowing government departments, as well as CSIS, to act whenever they believe limply defined security threats "may"—not "will"—occur." [18] The Globe continued: "Under the cloud of fear produced by his repeated hyperbole about the scope and nature of the threat, he (Prime Minister Stephen Harper – author's note) now wants to turn our domestic spy agency into something that looks disturbingly like a secret police force." That things about Bill C-51 are not quite clear shows a comment of one of the protesters: "I'm really worried about democracy, this country is going in a really bad direction, [Prime Minister] Harper is taking it in a really bad direction." [19] "Freedom to speak out against the government is probably [in] jeopardy...even if you're just posting stuff online you could be targeted, so it's a really terrifying bill." [20]

2.2 HOW TO PROTECT PRIVATE COMMUNICATIONS?

Bearing in mind that it is practically impossible to protect one's communications from eavesdropping, each Internet user is advised to publish only what he can comfortably tell to court. Everything else is associated with risk. However, much can be done to reduce the risk.

2.2.1 E-MAIL

Encrypting e-mail today is still not widespread. Most of a typical e-mail messages continue to be sent in plain text which allows messages to be easily intercepted. In the year 2013 a little more than a third of users, 35%, had a possibility to encrypt messages. The situation was even worse in the year before when the corresponding percentage was 27. [21] To ensure encrypted data transfer between the user and the Internet Service Provider (ISP) there should adjust the Secure Socket Layer (SSL) and Transport Layer Security (TLS) encryption. SSL connections can be activated in the web browser or email program. Messages can (and should) be encrypted during transmission, but to make it possible, it is necessary to be done at the sender's and also at the recipient's place. [15] To encrypt e-mail messages functions embedded in the e-mail service can be used, or one can download the software for

encryption or client add-ons (such as those using the OpenPGP [22]). In an emergency, Web-based services for e-mail encryption as Sendinc or JumbleMe can be used, although with these users are forced to trust a third party, the particular company. [23] For email encryption End-to-end encryption, Server-server encryption and Client-server encryption are options

2.2.2 SOCIAL NETWORKS

Social networks are giving "free" services because they are selling access to users! This any user have to bear in mind all the time it shares its contents. This fact each user has to bear in mind all the time he shares his private contents. Every picture tells much more than owner wants to show.

No matter which service one uses, it must consider [24]:

- Who can read his profile, and see his posts and activities;
- What information is shared with external sites and businesses;
- Which applications can access his data;
- What information his friends can share about him;
- Who can see his pictures and/or location;
- Which sites integrate with his social network (for example, Facebook's Like feature).

More about these risks is discussed in Mogull's: Protect your privacy: take control of social networking [24].

2.2.3 MOBILE TELEPHONY

Mobile devices, phones, are small computers, and they can do almost everything as PCs do. But, phones are also exposed to all attacks as PCs are. The problem is that phones because of batteries capacities have smaller resources than PCs. To try to protect privacy, user needs to activate all security features of his device, to install security software, to use own password, to use encrypted Wi-Fi networks, and to switch off Bluetooth connection when he doesn't use it, and finally not to leave the device unattended. It is always useful to note IMEI (International Mobile Equipment Identifier), and use remote tracking. This can allow to find stolen or lost device.

CONCLUSIONS

Modern life is related to the massive use of electronic communications, especially the Internet and mobile technologies. To single person is virtually unable to carry out his everyday activities without the use of these technologies. However, many dangers lurk online. Data are vulnerable during their transfer as well as in storage in terms of protection of their integrity and in terms of their secrecy. Extraordinarily rapid development of information technology enables their efficient implementation, but also brings an increased risk of eavesdropping and espionage. This paper discussed the current state of using the Internet and gave a look to some legal aspects of private data protection, as well as some recommendations for privacy protection.

WORKS CITED

[1] Zakon, "Law on personal data protection," 01 Jan 2009. [Online]. Available: http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/SERBIA_DPLAW_EN.pdf. [Accessed 08 Mar 2015].

[2] PDPA, "Personal Data Protection Act 2012," *Government gazete of the Republic of Singapore,* no. 26, 2012.

[3] O. Yaron and O. Primat, "Saudi hacker threatens to expose details of another million credit cards," *HAARETZ,* 06 Jan 2012.

[4] F. T. C. FTC, "Stolen Identity: A Consumer Nightmare," 04 May 2010. [Online]. Available: http://www.infoplease.com/ipa/A0903927.html. [Accessed 12 Mar 2015].

[5] S. Slabaugh, "Ball State University confirms 80 identity theft victims," 10 Mar 2015. [Online]. Available: http://www.indystar.com/story/news/2015/03/10/ball-state-identity-theft-anthem/24734003/. [Accessed 12 Mar 2015].

[6] European Parliament, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal,* vol. 38, no. L281, pp. 31-50, 24 Oct 1995.

[7] K. McCullagh, "What is 'private' data?," [Online]. Available: http://ukcle.typepad.com/digital_directions/files/McCullagh.pdf. [Accessed 12 Mar 2015].

[8] Z. Čekerevac, P. Čekerevac and J. Vasiljević, "Internet sigurnost MSP sa aspekta sigurnosti elektronske pošte," *FBIM Transactions,* vol. 2, no. 1, pp. 45-56, 15 Jan 2014.

[9] G. Greenwald and E. MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian,* 07 06 2013.

[10] Z. Čekerevac, Z. Dvorak and P. Čekerevac, "Internet sigurnost u svetlu otkrića Edvarda Snoudena," *FBIM Transactions,* vol. 2, no. 2, pp. 68-78, 15 07 2014.

[11] T. Jungholt, "FDP-Minister will "Datenuntreue" bestrafen," *Die Welt,* 03 08 2013.

[12] L. Mirani, "Think U.S. Snooping Is Bad? Try Italy, India or Canada," 11 06 2013. [Online]. Available: http://mashable.com/2013/06/11/nsa-privacy-italy-india-canada/.

[13] E. Piermon, "Microsoft helped the NSA bypass encryption, new Snowden leak reveals," 12 07 2013. [Online]. Available: http://rt.com/usa/microsoft-nsa-snowden-leak-971/.

[14] PAA, "Protect America Act of 2007," 05 Aug 2007. [Online]. Available: http://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm. [Accessed 16 Mar 2015].

[15] Z. Čekerevac, Z. Dvorak and P. Čekerevac, "Internet safety of SMEs and e-mail protection in the light of recent revelations about espionage of internet communication system," vol. 10, 2014.

[16] Z. Čekerevac, "Small an medium sized enterprises data seccurity in cloud computing," in *ITEP 2013*, Chernivtsi, 2013.

[17] Parliament of Canada, "BILL C-51," 30 Jan 2015. [Online]. Available: http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6932136. [Accessed 16 Mar 2015].

[18] Globe Editorial, "Anti-terrorism bill will unleash CSIS on a lot more than terrorists," *The Globe and Mail,* 05 Feb 2015.

[19] RT, "'Freedom in jeopardy': Thousands rally across Canada against new anti-terror law," 16 Mar 2015. [Online]. Available: http://rt.com/news/240821-canada-protest-

terrorism-bill/. [Accessed 16 Mar 2015].
[20] Anon, "Tisuće na ulicama diljem Kanade protiv novih rigoroznih anti-terorističkih zakona: "Ugrožena nam je sloboda i demokracija, ovo je zakon o stvaranju tajne policije"," *advance*, 15 Mar 2015.
[21] Osterman Research, "Why Should You Encrypt Email and What Happens if You Don't?," 07 2013. [Online]. Available: http://www.ostermanresearch.com/whitepapers/orwp_0194.pdf.
[22] L. Constantin, "OpenPGP JavaScript Implementation Allows Webmail Encryption," 21 11 2011. [Online]. Available: http://www.pcworld.com/article/244406/openpgp_javascript_implementation_allows_webmail_encryption.html.
[23] E. Geier, "How to encrypt your email," 25 04 2012. [Online]. Available: http://www.pcworld.com/article/254338/how_to_encrypt_your_email.html.
[24] R. Mogull, "Protect your privacy: take control of social networking," 23 Feb 2011. [Online]. Available: http://www.macworld.com/article/1158122/protect_privacy_social_networks.html.
[25] T. O. D. Handbook, "What is Open Data?," [Online]. Available: http://opendatahandbook.org/en/what-is-open-data/. [Accessed 12 Mar 2015].

Článok recenzovali dvaja nezávislí recenzenti.

KRÍZOVÝ MANAŽMENT
CRISIS MANAGEMENT

Ročník 14 Číslo 1/2015

Vedecko-odborný časopis
FAKULTY BEZPEČNOSTNÉHO INŽINIERSTVA ŽILINSKEJ UNIVERZITY V ŽILINE

Scientific-technical magazine of
FACULTY OF SECURITY ENGINEERING UNIVERSITY OF ŽILINA IN ŽILINA

Viac informácii na: http://fbi.uniza.sk/kkm/stranka/casopis-krizovy-manazment