THE DYNAMICS OF FUTURE LAW ENFORCEMENT OFFICERS' AWARENESS OF POSSIBLE RISKS IN SOCIAL NETWORKS

Assoc. Prof. Dr. Edita Butrimė

Lithuanian University of Health Sciences

Prof. Dr. Vaiva Zuzevičiūtė

Mykolas Romeris University

Abstract. The main purpose of the article is to investigate the dynamics of awareness of students, i.e. future law enforcement officers, who will be expected to provide security for other people on the risks for their own or personal safety in the digital space. The paper presents both theoretical considerations and empiric data from the study (completed in 2016, 2017, 2019) aimed at investigating whether future law enforcement students recognize the main risks of the safety in the digital space. The study is important in the light that so much of contemporary social, personal and professional life is being carried out in the digital space. If future law enforcement officers are unable to recognize safety risks, as a consequence, they will not be professional and ready enough to consult and to provide support for citizens on the issues that in some cases start dominating the functioning of a contemporary person in the contemporary world.

Keywords: social network sites, risks in social networks, safety of personal data, habits of higher education students on the Internet or social networks.

1. Introduction

As a phenomenon, the Internet was introduced without any clear rules or requirements. It was such an innovation that no one thought of introducing it together with the set of rules in order to guarantee a plan, control, and safety. Therefore, today, several decades later, it is sometimes difficult to ensure safety as many of the measures have to be introduced (and were introduced) at a later date as a compensation [1]. B. Schneier [2] noted that "computer security is not a problem that technology can solve. Security solutions have a technological component, but security is fundamentally a people's problem". Social networks have gained an immense popularity in the recent decade. This part of the Internet possesses a specific set of requirements for a user. It is estimated that as many as 2.51 billion users participate in social networks, and the estimation for 2020 is 2.95 billion users [3]. This popularity means that with an increased number of users, the likelihood for breaching personal data increases as well [4]. Therefore, the author states that only to some degree it is possible to guarantee one's rights in social networks. One of the reasons for this deficiency is the fact that the users still have gaps in the competences on the safety in social networks.

With the advancement of technologies and, consequently, with the advancement of the Internet (or rather materials/entries on the Internet) becoming a product of almost everyone on the globe, the safety in the digital space becomes a complex task that only joint efforts of users and IT professionals may face effectively. Seemingly, benign pranks may be transformed into a conscious and financially motivated activity [5]. An example of an intolerable behavior is the Tay [6]. Microsoft cancelled the testing of artificial intelligence because the software began generating racist entries in 24 hours [7].

The introspection of a rather recent and short history is provided for the arguments for the necessity not only to introduce but also to discuss with every student, a future law enforcement officer, the dimensions of safety in the digital space.

The **object** at the focus of this paper is the dynamics of awareness (future law enforcement officers who will be obliged to provide security for other people and be aware of the risks for their own/personal safety in the digital space) on possible risks in the digital space.

Therefore, the main **purpose** is to investigate the dynamics of future law enforcement officers' awareness of possible risks in the digital space.

The **objectives** of the paper are as follows:

1. To discuss and provide the terms (working concepts) of the social network site and the safety of the users' data;

2. Based on the critical analysis of scientific literature, to identify the perspectives of social network users on the safety risks of personal data;

3. To identify (though considering also the limitations of the study) the dynamics over the years on students' awareness of the risks for the safety on the Internet (specifically, in social networks).

For the development of this paper, the methods of critical scientific literature analysis and the empiric four-phase study (2016-2019) were employed. It should be taken into consideration, however, that the paper further elaborates the considerations that were already addressed in the previous publications ([8], [9]). The authors carry out an on-going study with the aim to identify tendencies, patterns and dynamics.

2. Social Network: History and Current Situation

It is possible to define social network sites as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. The nature, architecture and nomenclature of these connections may vary from site to site. The users of Classmates.com (started in November, 1995) did not have an opportunity to create their own profiles or the lists of friends. A statistical user of SixDegrees.com (started in May, 1996) was associated with a maximum of 6 joint associates. In about a decade, dramatic changes in the coverages of social networks were instigated by the Web.2.0 technologies. On the one hand, the improvements prompted even those people who were skeptical about joining the communities to do just so. On the other hand, such a fast invasion had its own consequences, because the users do not always use the technologies in a competent and safe way. The Web 2.0 tools enable the creation and sharing of spontaneous and horizontal information. Why is it important for an educationalist to monitor and step in the process? In many cases, information creation and sharing is uncontrollable, therefore - which is at the core of this paper - unsafe for sharing because almost anyone may share and access what is shared ([10], [11], [12]).

The lack of personal negative experience prevents users from being careful in the sphere, they do not protect personal data or their profiles and, surely, the entries within: pictures, movies and texts [13].

The analysis of recent studies in the field reveals that a number of studies on the Internet safety and social networks was impressive [14]). A group of studies was dedicated to the safety of information on the Internet. The Lithuanian National Computer Emergency Response Team (CERT-LT) has a task to promote security for the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security [15]. The agency cooperates with LITNET CERT (Computer Emergency Response Team of LITNET networks), SSDCN (Secure State Data Communication Network, the foundation for national information communication technologies (ICT) infrastructure that safeguards data exchange between state institutions and secure delivery of e-government services), Cyber-Police, and the Ministry of National Defence.

The Communications Regulatory Authority created the website esaugumas. It [16] with the main purpose to provide the information on safe behavior on the Internet and recommendations on avoiding the incidents. The website published several representative studies (completed in May-June, 2016) on the attitudes and awareness of parents of 5-18 or 14-18-year olds [17] and a sociological study on the impact of the project *Saugesnis internetas* (*Safer Internet*) on the awareness of the society completed in May, 2012 [16].

3. Dimensions of Safety in the Digital Space: Alarms and Routine

The EUROSTAT [18] data shows that in 2015 1 of 4 Internet users was alarmed by his/her safety on the Internet in the European Union. S. Jastiuginas [19] goes as far as to suggest that inability of individuals and organisations to manage safely the information-communication systems may result in problems for the states themselves, therefore, the ability to manage and use information safely may (and must) turn into a strategic priority for organisations and states. Only those states that ensure safety of information also provide the basis for other dimensions of safety and counter-measures for international risk management ([20], [21]). The most recent events (e.g., Panama Papers) illustrate the controversy that each organization and state faces. On the one hand, it was a leak of sensitive information which shows the shortcomings of information management systems, on the other hand, the leaking disclosed unethical and even potentially criminal process (which paradoxically may be considered a counter-criminal activity from a certain perspective) [22]. Those and other dimensions have already become and will only be a more dominant part of a law enforcement officer's work.

In 2008, when Facebook was still a relatively new technology, K. Lewis, J. Kaufman and N. Christakis invited 1,740 students from the USA to participate in a survey [23]. Out of a total, 1,710 students (98.3%) had Facebook profiles. K. Lewis, J. Kaufman and N. Christakis found that "a student is significantly more likely to have a private profile if (1) the student's friends, and especially roommates, have private profiles; (2) the student is more active on Facebook; (3) the student is female; and (4) the student generally prefers music that is relatively popular (high meaning) and only music that is relatively popular (low SD)" ([23], p. 94). Therefore, the authors concluded that the boundaries between the private and the public were transcended: "users venture too far into public space with private details, and the consequence is a crashed party, a lost job opportunity, or – at an extreme – sexual assault or identity theft" [23]. The authors, however, shared the conviction that the next generation may find the way in organising the digital space in a more safe way with the introduction of certain filters for safety; maybe the digital space will become "self-regulating systems".

Some authors state forcefully that ensuring the safety of computers is simply impossible without ensuring the safety of the Internet. On the one hand, superficially, the Internet provides a technical platform for self-realisation and the freedom of speech [1], on the other hand, we want – and even have legal rights – to be safe on the Internet the same way we want safety in the physical reality. Sometimes we expect the safety to be ensured without us investing in it. The Article 8 of the Charter of Fundamental Rights of the European Union stipulates the right to the protection of personal data [26], though this stipulation came into focus many years before the era of computers and the Internet. The advance of technology poses new challenges to activities, even very detailed explanations on procedures how personal data should be protected [25] may not be sufficient if each and any individual in this transparent to the extent of dangerous era of ever present Internet does not participate.

The anonymity of users contributes to the self-realisation and the freedom of speech. It is a great paradox: on the one hand, we all want to ensure safety on the Internet, and on the other hand, it is the anonymity that adds to the openness and freedom of speech. This is the paradox that comprises a large part of our contemporary life.

4. Methodology of Empirical Study

Phase 1. N=178 (80 in 2016, 67 in 2017, 31 in 2019). The respondents were 19-23 year old second- or third-year students of higher education. The students were invited to carry out a survey at the beginning of the semester. The data is not presented due to the limitation of the scope of the paper.

Phase 2. N=178 (as above). The test developed during the national project *Langas i ateiti* (*Window to the Future*) [25] was used for the purpose. The standards of the National IT proficiency of the Republic of Lithuania as well as the requirements set by the European Computer Driving Licence (ECDL), Microsoft Unlimited Potential Community Learning Curriculum and Microsoft Digital Literacy Curriculum V.2 were taken into consideration while developing this test.

The estimations were designed as follows: if a respondent received a score less than (<) 60%, he or she failed the test; if the score was 60%-70%, he or she was identified as a novice user; if the score was 70%-80%, he or she was identified an independent user; 80%-90% - a proficient user; 90% and more - an advanced user. This phase of the study was aimed at identifying the students' IT competence level according to a standardized objective perspective by using a standardized test. Due to the limitation of the study, the results are not presented in this paper.

Phase 3? 4?. N=89 (2017), 31 in 2019. Students were invited to share their perspective on safety in the digital space. The questions on Facebook were as follows: Closed questions: How many friends do you have on Facebook? To what extent do you know your Facebook friends? Open questions: What are the advantages and shortcomings of social networks? Please explain how do you protect your privacy in a social network. Do you know who receives the materials that you upload on your Facebook profile?

The comparison of the data from 2017 and 2019 is presented in the table below.

Data from 2017 (89 students)	Data from 2019 (31 students)	
Item: Please explain how do you protect your privacy in a social network.		
The analysis revealed that students may be grouped into the following three groups:	The analysis revealed that students may be grouped into the following four groups.	
 Students are not really sure that they control their safety/privacy on Facebook to a significant level from the perspective of what is available to other people ("I do not control anything"). Students admit that they are not safe on Facebook ("I try that the minimal number of people whom I do not know personally have access to the contents I upload, because I do not know in what way that may be used or for what purposes"; "I am not sure whether the information about me is accessible just to the level that I want and authorize"; "The problem is that I am not always sure who is behind the profile; therefore, there might be problems while sharing info in profiles. Information may get somewhere that I do not want and cause problems"; "So many people know what it is that you are interested in, what you do"; "My safety as a user on the scale of 1 to 10 is 4"). Students state that they control their safety on Facebook ("I feel safe in this environment because I may decide what is public and what is not. Facebook has its regulations and rules which ensure user safety"; "I control everything the way I want. That is what applications are for. Only my friends are allowed access to the whole account; it is only me who has access to contacts; I regulate the patterns for communication and access to information"; "Well, I control the access by using applications according to the necessity, including access to contacts, information and access to my profile"). 	 This group has most responses. Students are conscious about positive dangers in the digital space. 13 students expressed concerns that there might be threats, however, they try to implement some measures that were grouped into subgroups. The first one includes attempts to use strong passwords; the second one includes attempts to control what they upload on the platforms (e.g. avoid uploading personal information, such as address or bank account details); the third subgroup encompasses attempts to control whom they label 'friends'; the fourth subgroup includes only one contribution which equals 'safety' to 'safety from viruses. The second group has contributions of 9 students' answers proving that students feel safe in the digital space. The third group has 3 contributions revealing that students feel unsafe, e.g., "I do not think we are safe in the digital space in terms of what we upload". The last group (5 contributions) is comprised of the answers "do not know" or no information. 	
Item: Do you know who receives the materials that you upload on your Facebook profile?		

The answers to the second open question may be grouped into the following three groups:	The analysis revealed that students may be grouped into the following three groups.
grouped into the following three groups:	grouped into the following three groups.
 Students do not feel safe in the digital space (social networks). The contributions were allocated into this group as follows: "Others will have as much information about you as you share. It is impossible to trust a person, let alone a social network"; "I do not upload any materials"; "I do not send anything personal. If I need to do that, I use other channels". Students know that they do not have full control over the entries/materials that they share with friends in social networks: "I send something to a specific person but will also receive materials I do not know"; "Of course, a person to whom I send information receives it, however, I do not know what are the next steps for its travel". 	1. The majority (25 students) expressed uncertainty about who and how become the recipients of materials. The contributions were classified to three subgroups. The contributions that express a certain level of IT competencies were classified to the first subgroup. Students shared their opinion that any information or click is saved somewhere in servers, any information, even if it is addressed to a particular person and may also be viewed by a platform administrators. Also, students think that it is important to use all available tools for privacy in order to have at least any. The second subgroup include contributions, which show that any recipient may also serve as a sender, therefore, the uploaded materials may become publicly available (e.g. "I hope, but I am not sure at all. Even if I send
3. The greatest number of students were allocated into the group of those who did not know the mechanism of information flow and	something to a particular person, there is no guarantee the materials will not become available to others").
spread in social networks because they were (unfortunately and groundlessly) sure about who were the intermediate of the end recipients of their entries: "Those whom I indicate as	2. 3 students were sure about the final recipient (e.g. "Yes, because when I send something, I indicate who should receive and view it").
recipients get the entries; and my opinions and ideas are also available only for those pre-set recipients"; "Yes, I control those who may see my posts and pictures and everything that I share".	3. 3 students were not sure about the final recipient, however, they did not express concern about that.

5. Conclusions

The empiric study revealed that although in 2017 and 2019 the contributions were classified into three groups, the dynamics is positive. Students' contributions revealed that they became more competent and conscious about the safety in the digital space.

Notwithstanding the fact that two years ago the majority of students demonstrated a certain naivety about control in the digital space, the recent study revealed that students became more competent about the processes and mechanisms of the user's immediate actions.

Two years ago, young people (students) did not draw a line between 'private' and 'public' in their activities/information shared in the digital spaces. Some of them do, or think they do, but, obviously (and thankfully), the lack of personal experience in the dangers of being negligent in the digital space prevents them from being cautious. With the digital space comprising so much of a contemporary person's life, i.e. e-banking, studies, regulation/monitoring of loans/mortgages, etc., it is imperative to remind young people about the necessity to keep certain areas of life private and as safe as it is technologically possible. That especially applies to future law enforcement officers because they have to set a personal example and be ready to consult a citizen and community on the issue.

Recent study, however, revealed that students already know that everything published in the digital space remains there (at least in the backing systems). Also, students know that the efficiency of privacy tools is not absolute, therefore, they do not trust blindly their recipients even if they are 'friends'.

The recent stream of events associated with Facebook during the last two years changed general opinion. The new legislation either came into force or the discussions about the necessity to have stricter legal framework gained impetus nationally and internationally. Even so, still there are students, including future law enforcers, who lack either competencies or experiences or both to ensure their own safety in the digital space despite the positive dynamics of awareness.

Therefore, we, educational professionals in higher education, should be aware of the very fact that even though young people are quite proficient in using the Internet and its tools, it does not automatically mean that they are ready and proficient in using those tools safely. And, consequently, our educationalists' efforts to compensate for that are necessary, especially while educating future law enforcers, who, to add to the complexity, will be expected to consult other citizens on the issue.

References

1. Garšva, E., Skudutis, J. Secure Computer System Design. Electronics and Electrical Engineering. 6(55) p. 43-48, (2004).

2. Schneier, B. Secrets and Lies – Digital Security in a Networked World. John Wiley & Sons, (2015).

3. Number of Social Media Users Worldwide from 2010 to 2020 (in billions). Statista. The Statistics Portal. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

4. Malinauskaitė van de Castel, I. Duomenų subjekto teisės virtualiuose socialiniuose tinkluose (Rights of the Data Subject in Online Social Networks). Doctoral thesis. MRU, Vilnius, (2017).

5. Kalpokas, V., Marcinauskaitė, R. Identity Theft in Cyberspace: Technological Aspects and Criminal Legal Assessment. Teisės problemos. No 3(77) p. 30-52, (2012).

6. Lee, P. Learning from Tay's Introduction. Official Microsoft Blog. http://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/#sm.000jh14di12 9ee0ov1u1atn7zsco3 7. Vincent, J. Twitter Taught Microsoft's AI Chatbot to Be a Racist Asshole in Less than a Day. March 24, 2016. http://www.theverge.com/2016/3/24/11297050/ tay-microsoft-chatbot-racist

8. Butrimė, E., Zuzevičiūtė, V. Students' / Future Law Enforcement Officers' Perspective on Safety in the Digital Space // Kultura bezpieczeństwa: Nauka – Praktyka–Refleksje. Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego "Apeiron", Kraków, No 23, pp. 46–55, (2016).

9. Butrimė, E., Zuzevičiūtė, V. Possible Risks in Social Networks: Awareness of Future Law Enforcement Officers // Trends and Advances in Information Systems and Technologies: WorldCIST'18: World Conference on Information Systems and Technologies : 27-29 March, Naples, Italy : Conference Proceedings: Vol. 2/ Editors: Álvaro Rocha, Hojjat Adeli, Luís Paulo Reis, Sandra Costanzo. Cham: Springer, 2018. ISBN 9783319777115, (2018).

10. Anzai, Y. Digital Trends among Japanese University Students: Podcasting and Wikis as Tools for Learning. International Journal on E-Learning, 8(4), p. 453-467, (2009).

11. Davidson, A., L. Waddington, D. E-Learning in the University: When Will It Really Happen? eLearning Papers. No. 21, September 2010, (2010), http://www.elearningeuropa.info/files/media/media23710.pdf

12. Fraser, M., Dutta, S. Mano virtualieji aš. Kaip socialiniai tinklai keičia gyvenimą, darbą ir pasaulį (Throwing Sheep in the Boardroom: How Online Social Networking Will Transform Your Life, Work and World). Eugrimas, Vilnius, (2010).

13. Zibenienė, G., Brasienė, D. Using the Internet, Online Social Networks and Potentially Incurred Risk: Student Opinions. Social Technologies, 3(1), 53--67, (2013).

14. Bacys, B. Teenagers' Addiction to Social Networks on the Internet. Socialinė teorija, empirija, politika ir praktika, No. 7, 9–23, Vilnius University, Vilnius, (2013).

15. CERT-LT. Lithuanian National Computer Emergency Response Team, https://www.cert.lt/en/

16. Esaugumas. https://esaugumas.lt/lt/tikslas/89

17. Kiekybinis internetu besinaudojančių tėvų ir paauglių nuomonės tyrimas (Quantitative Survey of Parents and Teenagers Using the Internet), ITC Švietimo informacinių technologijų centras. Sprinter tyrimai, Vilnius, (2016), http://www.draugiskasinternetas.lt/repository/dokumentai/Ataskaita%20-%20SITC_bendras_201606.pdf

18. 20 proc. Lietuvos interneto naudotojų pernai susidūrė su saugumo problemomis, Penki, February 10, 2016, http://www.penki.lt/Sauga-saugos-sprendimai/20-proc-Lietuvos-interneto-naudotoju-pernai-susidure-su-saugumo-problemomis.im?id=354489&tid=449

19. Jastiuginas S. Information Security Management in Lithuania's Public Sector. Informacijos mokslai No. 57, pp. 7--25, (2011), http://www.journals.vu.lt/

informacijos-mokslai/article/view/3137/2755

20. CIO Magazine, CSO Magazine, PricewaterhouseCoopers. The Global State of Information Security 2010, http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_report.pdf

21. Ernst & Young's 12th Annual Global Information Security Survey, http:// www.ey.com/Publication/ vwLU Assets/12th_annual_GISS/ \$FILE /12th_annual_ GISS.pdf

22. The International Consortium of Investigative Journalists. The Panama Papers. Publication Date: 04/11/2016. Politicians, Criminals and the Rogue Industry That Hides Their Cash. http://community.globaleditorsnetwork.org/content/panama-papers-politicians-criminals-and-rogue-industry-hides-their-cash-0

23. Lewis, K., Kaufman, J., Christakis, N. Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. Journal of Computer-Mediated Communication. No. 14 79—126, (2008), doi: 10.1111/j.1083-6101.2008.01432.

24. Langas į ateitį (*Window to the Future*). Last modified in 2015. http:// www.epilietis.eu/index.php/about-the-project

25. Asmens duomenų apsauga-darbo tvarkos, rekomendacijos ir pavyzdžiai. Pačiolis, Vilnius, 2018.

26. Handbook on European Data Protection Law. European Union Agency for Fundamental Rights and Council of Europe, 2018.

BŪSIMŲJŲ TEISĖSAUGOS PAREIGŪNŲ GALIMŲ GRĖSMIŲ SOCIALINIUOSE TINKLUOSE SUVOKIMO DINAMIKA

Doc. dr. Edita Butrimė

Lietuvos sveikatos mokslų universitetas

Prof. dr. Vaiva Zuzevičiūtė

Mykolo Romerio universitetas, Viešojo saugumo akademija

Santrauka

Šio straipsnio paskirtis yra išanalizuoti būsimuju teisėsaugos pareigūnų galimu grėsmių socialiniuose tinkluose suvokimo dinamika. Būsimieji teisėsaugos pareigūnai ateityje ne tik konsultuos piliečius apie galimas grėsmes, iš pareigūnų bus tikimasi, kad jie užtikrins piliečiu sauguma skaitmeninėje erdvėje. Taip pat ir patys teisėsaugos pareigūnai šiuo aspektu turi rūpintis savo saugumu. Straipsnyje analizuojami teoriniai šaltiniai, taip pat pristatomi ir analizuojami kai kurie empirinio tyrimo, atlikto 2016, 2017, 2019 metais, rezultatai. Empirinis tyrimas buvo sukonstruotas ir įgyvendintas siekiant atskleisti, ar ir kaip būsimieji teisėsaugos pareigūnai supranta grėsmes skaitmeninėje erdvėje. Tyrime derinami keli tyrimo metodai: apklausa ir atvirieji pasisakymai. Daroma prielaida, kad dėl to, jog daug profesinės ir socialinės veiklos, taip pat asmeninio gyvenimo aspektų įkeliama į skaitmeninę erdvę, būtina, kad būsimieji teisėsaugos pareigūnai mokėtų atpažinti galimas grėsmes jau dabar, studijuodami aukštojoje mokykloje. Straipsnyje pateikiama kintančio suvokimo (atsižvelgiant i skirtingais metais pateiktos nuomonės analize), remiantis kokybinio tyrimo metodologija, pagristo tyrimo duomenimis, analizė

AUTORIAUS LYDRAŠTIS

Autoriaus vardas, pavardė: Edita Butrimė

Mokslo laipsnis ir vardas: daktaras

Darbo vieta ir pareigos: Lietuvos sveikatos mokslų universitetas, docentė Kalbų ir edukacijos katedroje.

Autoriaus mokslinių interesų sritys: el.mokymasis, duomenų apsauga. Telefonas ir el. pašto adresas: edita.butrime@lsmumi.lt

AUTORIAUS LYDRAŠTIS

Autoriaus vardas, pavardė: Vaiva Zuzevičiūtė Mokslo laipsnis ir vardas: daktaras

Darbo vieta ir pareigos: Mykolo Romerio universitetas, Viešojo saugumo akademija, Humanitarinių mokslų katedros profesorė

Autoriaus mokslinių interesų sritys: el. mokymasis, tarpkultūrinis mokymasis.

Telefonas ir el. pašto adresas: vaiva.zuzeviciute@mruni.eu

AUTHORS' COVER LETTER

Author's name and surname: Edita Butrimė

Academic degree and name: PhD

Workplace and position: Associate Professor, Department of Languages and Education, Lithuanian University of Health Sciences

Author's research interests: e-learning, protection of data Telephone and e-mail address: edita.butrime@lsmuni.lt

Author's name and surname: Vaiva Zuzevičiūtė Academic degree and name: PhD

Workplace and position: Professor, Department of Humanities, Academy of Public Security, Mykolas Romeris University

Author's research interests: e-learning, intercultural learning Telephone and e-mail address: vaiva.zuzeviciute@mruni.eu