Proceedings of the International Conference on
Information Technologies (InfoTech-2017)
20-21 September 2017, Bulgaria

OPPORTUNITIES OF THE DIGITAL SPACE AND CHALLENGES FOR PRIVACY AND INDIVIDUAL'S SECURITY

Radi Romansky

Technical University of Sofia, Department of Informatics
e-mail: rrom@tu-sofia.bg
Bulgaria

Abstract: The purpose of this article is to summarize some specific features of the contemporary digital world and the relation of the new network technologies to the privacy and protection of the individual's life. A brief survey of the actual opportunities of the global network as e-services, cloud and social computing, Internet of Things (IoT), Machine to Machine communications (M2M), etc., is made in the paper. The implementation of these technologies in distributed information systems and environments could create some problems for individuals and disturb their privacy. In this reason, some important challenges for individual's privacy and security are determined and summarized in the paper.
Key words: digital age, information servicing, privacy, secure access.

1. INTRODUCTION

Information Society (IS) is a society which accepts the information as a basic product and the main goal is to increase the economical, social and cultural levels based on using Information and Communication Technologies (ICT). The organization of the 'IS' is based on the different *information resources*, which unite information and all needed technical equipment, software and network tools for information servicing supporting. Morales et al. define in [1] the term "information resources" as *"an element of infrastructure that enables the transaction of certain selected significant and relevant data, prepared so as to provide content and information services that can be used directly by the user. It is necessary to establish some minimum socio-technical requirements for an element to qualify as a resource".*

The new opportunities of the digital space are related to some important technologies as cloud services [2], social computing [3], Internet of Things (IoT) [4], Machin to Machin (M2M) communication [5], etc. They extend the role of the

Information Society in the life of individuals and in the business processes and resources management.

However, all these technologies require many personal data which should be uploaded in the unknown places (nodes in the global network) for creating personal profiles. This fact could create some problems for the user's privacy – individuals or business organizations, in the age of information [6]. For example, a security framework for business cloud is discussed in [7] and a survey of opportunities and challenges of the security in cloud computing is made in [8]. Practically, all processes in the global network and network services should be analysed on the base of privacy and personal data protection [9]. On the other hand, the problems with user protection, security in cyberspace and data protection are discussed in different forums of Council of Europe [10] and European Commission [11].

The purpose of this article is to make a survey of the important opportunities of the digital space and to summarize the basic challenges for user's security and privacy at access to personal data and other personal information uploaded in the digital spaces. In this connection, a brief survey of main features of the contemporary network technologies is made in the section 2. Section 3 presents some important challenges for privacy and user's security, and discusses the basic problems that the digital spaces could create for individuals and organizations.

2. OPPORTUNITIES OF DIGITAL SPACE – A BRIEF SURVEY

e-Governance components and environments

The idea for digitalization of processes in governance is not new, but it is in growth continuously. The main goal of e-governance is to approve the principles of the constitutional state at the processes in the society. This government of law includes the right for access to information, privacy and protection of personal data, better relations between citizens and public authorities, effectiveness of state governance, increasing quality of services, etc.

E-governance is an approach for realization of the processes in the society by using contemporary ITC and it requires new strategies and policies for democratic governance. Some of the basic components of the e-governance are presented in Fig. 1 and they determine some features:

- the components of e-governance are realized on the base of remote access to information resources and distributed processing via Internet;
- e-governance must be realized by using all democratic principles in the society;
- the social and economic aspects should be reflected in the structures of e-governance;
- e-government is an important component of e-governance and the main participants are the groups of administration, government structures, citizens and business which determine the basic relations in the e-government model.

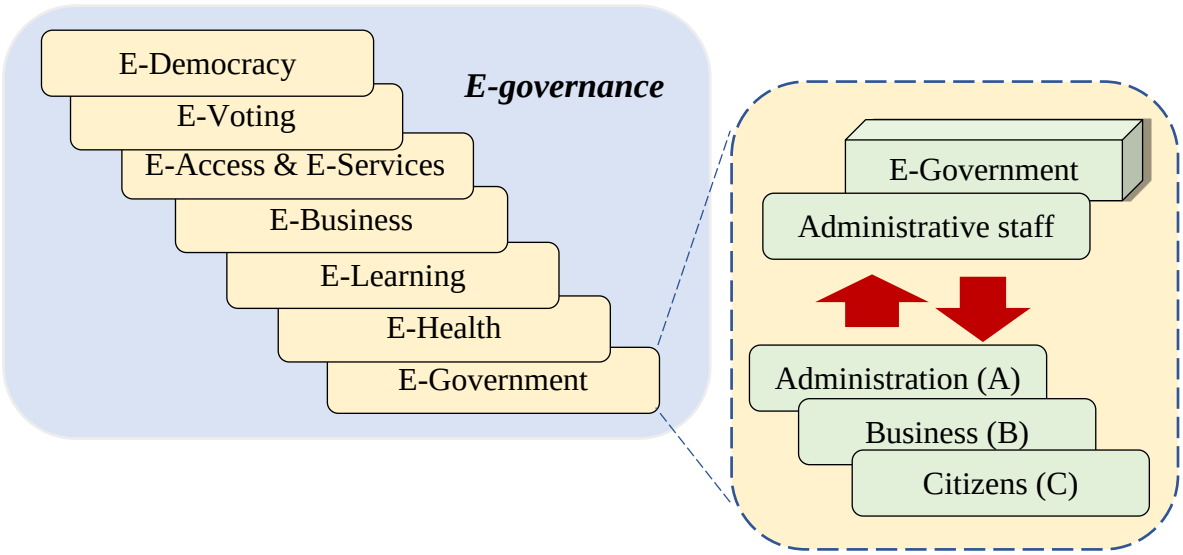

Fig. 1. Some basic components of e-governance

All components of the e-governance could be realized by using contemporary ICT and they should be regarded as a structures and technologies for giving, storing, accessing and processing different types of information, including personal data. In this reason, the opportunities of e-governance (presented by the components) should be discussed in the frame of possible challenges for privacy and user's security.

Cloud Services

One of the main opportunities of the digital space is the cloud services that could be used based on multitenancy. In [12] is written "*The cloud service model intrinsically caters to multiple tenants, most obviously not only in public clouds but also in private clouds for large organizations* ". On the other hand, [2] declares "*In cloud environment, heterogeneity, uncertainty and dispersion of resources encounters problems of allocation of resources, which cannot be addressed with existing resource allocation policies*". An analysis of resource scheduling in cloud computing is presented in this article with a goal to help researchers in the process of selecting "*suitable algorithm for scheduling a specific workload*".

Hashem et al. [13] discuss another side of cloud computing – big data. They determine the cloud computing as "*a powerful technology to perform massive-scale and complex computing. It eliminates the need to maintain expensive computing hardware, dedicated space, and software"* and note the "*massive growth in the scale of data or big data generated through cloud computing*" The authors introduce in this article definition, characteristics, and classification of big data and determine that the addressing big data "*requires a large computational infrastructure to ensure successful data processing and analysis*".

Another opportunity of cloud computing is so called "cloud manufacturing" introduced in [14]. The authors determine the cloud manufacturing as "*a new manufacturing paradigm as well as an integrated technology, which is promising in transforming today's manufacturing industry towards service-oriented, highly collaborative and innovative manufacturing in the future*". A critical review of the

contemporary manufacturing technologies which permits to evaluate the proposed new side in the cloud environments is made in this paper.

Chang et al. [7] propose a cloud computing adoption framework (CCAF) "*to meet the requirements of business clouds and ensure that all implementations and services deliveries overcome all the technical challenges*". The authors' proposal is based on the conception that the security, trust, and privacy should be actual tasks at each system organization with cloud computing and big data. The business on the cloud has some important advantages at moving their data to the cloud and data centers – this permits to centralize the management of data centers, cloud services and applications. These opportunities reduce the cost for business processes organization and realization, and increase operational efficiency but could make some problems for user's privacy and personal data protection.

Social Computing

What is the social computing? An acceptable vision of the social computing is that it collects different forms of social environments as social media, social networks, social bookmarks, and social aggregators. The Oxford Living Dictionaries gives the following definition for the term social network [16]: "*A network of social interactions and personal relationships*" and in addition "*an online community of people with a common interest who use a website or other technologies to communicate with each other and share information, resources, etc.".* Daniel Nations in [17] proposes the following definition "*Social media are web-based communication tools that enable people to interact with each other by both sharing and consuming information*". The author asks in [17] very important question about the definition of the social computing – "*But if we use the term to describe a site like Facebook, and also a site like Digg, plus a site like Wikipedia, and even a site like I Can Has Cheezburger, then it starts to get more confusing. Just what is social media anyway*? And finally, the article makes a conclusion that there is not a common understanding what must be determined as a social computing environment.

It is well known that the social networks and media are very popular in the world and Fig. 2 presents "… *the top of 15 most popular social networking worldwide*" [18].

The components of the social computing are very popular and give useful opportunities for contacts and exchange of information between different users through the digital space [19]. This is valid not only for the individuals but also for business organizations, managers, traders, etc. Different investigations present statistical assessments for using social networks and media from companies for searching clients, staff, etc. On the other hand, the individuals upload their personal data to create a profile, but these data could be used by traders, managers, employers, etc. without permission of the data owner. This rises raises the ethical side and disturbs the principles of privacy and personal data protection.

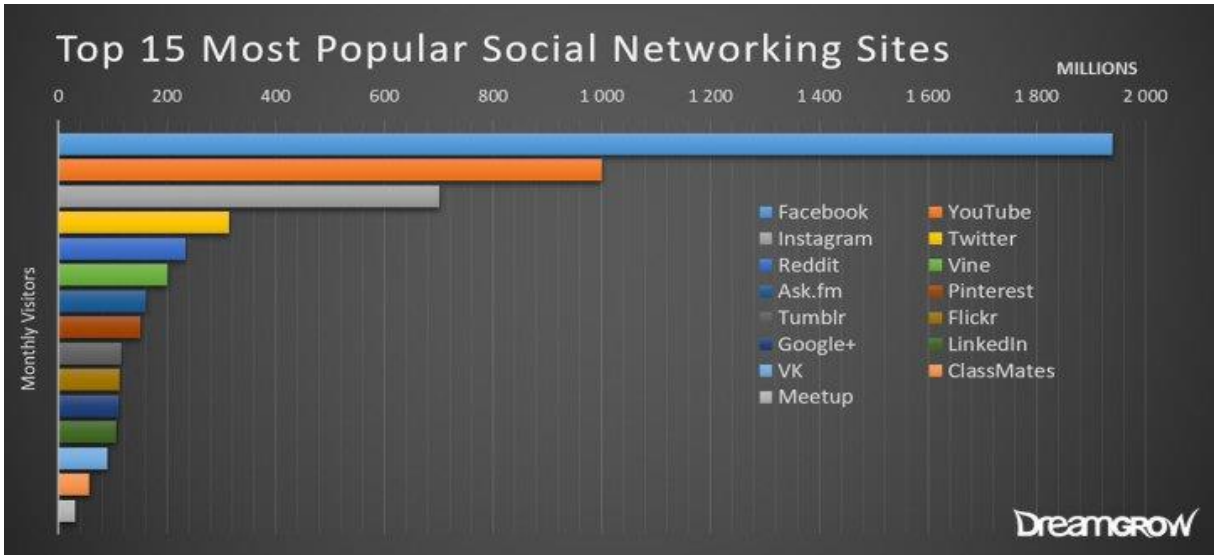

Fig. 2. Usage evaluation of the most popular social networking sites [18]

Internet of Things (IoT) and M2M communications

Whitmore et al. [4] determine the IoT as "*a paradigm where everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to accomplish some objective*" and discuss the current state of research on IoT in [4]. A generalized functional structure of IoT system is presented in Fig. 2, which unites the main groups of components – sensors, applications, access methods, data processing applications, means and tools for access control and information security. Two sub-systems could be determined – IoT-core and collection of tools for access regulation and data protection.

On the other hand, it should be noted that the developing many IoT applications with different nature and characteristics creates three directions in this sector for increasing the opportunities of IoT architecture. The common part of these directions is the group of elements included in the IoT-core (see Fig.2) but there are differences and specific features at communication between them.

Direction (1): Wireless sensor network (WSN) – it includes distributed sensors for monitoring physical parameters or parameters of the state of the environment. The data of this monitoring are sent via the network, which ensures processing and storing the information used for control of the other units in the system.

Direction (2): M2M communications (so called M2M model) ensure communications without human participation. This opportunity is based on the IoT architecture and permits to extend the services. M2M model is realized by smart systems, many active computers, sensors, and mobile unites for collection, sending, and processing monitored data. Application of the M2M model is to build smart cities, smart homes, smart networks, intelligent transport systems (for example see [15]), etc.

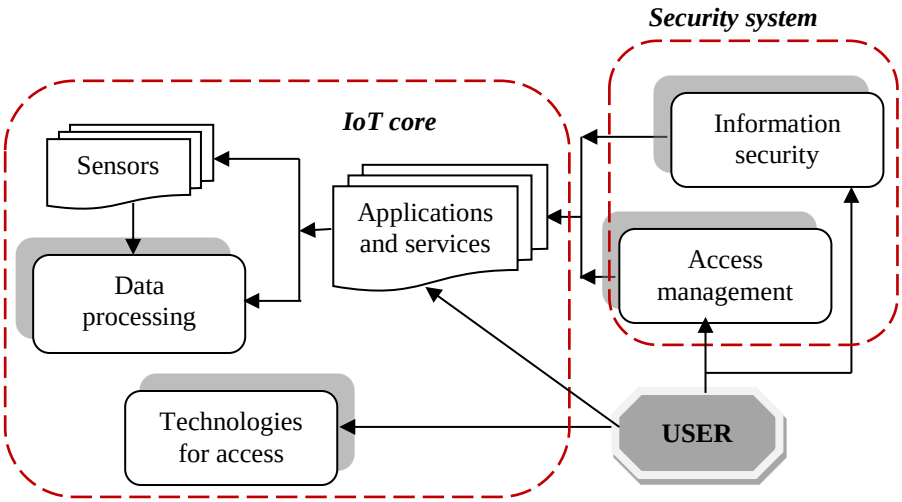

Fig. 2. Functional structure of IoT system

Direction (3): It is defined as an extension of the M2M-model for possible increasing information processing by using the new technologies and coordination between elements of the IoT-core. This direction is called "cyber-physical system".

The actualization of the M2M model is proved by the conclusion in [5] when is written "*Machine-to-Machine (M2M) communication is a promising technology for next generation communication systems. This communication paradigm facilitates ubiquitous communications with full mechanical automation, where a large number of intelligent devices connected by wired/wireless links, interact with each other without direct human intervention.*". In addition, the authors extend the area of application and add smart grids, e-healthcare, home area networks, and industrial automation. As a conclusion, the authors of [5] declare that "… *distinctive features in M2M communications form different challenges from those in human-to-human communications. These challenges need to be addressed, or otherwise it is not easy for this paradigm to gain trust of people."*

3. CHALLENGES FOR PRIVACY AND USER'S SECURITY RIGHTS

The contemporary technologies realized in the global network create challenges for user's privacy and protection of personal data uploaded in the digital environment (social media and networks, for example) or stored data in cloud, data centres, etc. Some of these challenges are discussed in this section.

Chang et al. [7] determine that the system design and deployment must be made based on the principles of "*current security practices*". The goal must be protection of user's privacy and confidentially, integrity, and availability of data. In this reason, it is very important to develop a suitable framework for integration of the resources on the base of guidelines, policies, standards, and rules for user's security and privacy. The authors cite some research in this field as 'Usage-Based Security Framework' (UBSF) for collaborative computing systems, 'TrustCloud framework' which is focused on accountability, 'comprehensive security framework', 'wireless sensor networks model', etc., but "… *there are no details on the actual use of the proposals and also*

no clear evidence of adoption of these proposals to business clouds". In this direction, the proposed in [7] CCAF is used for developing cloud storage, bioinformatics solution, and authorized access to the resources. This permits development of guidelines for financial modelling, best practices, and change the risk.

The free information moving and remote access to knowledge, learning, information and other resources create several challenges for privacy and user's rights protection. Haggard & Jablonski [20] write that "*free flow of information creates markets by exposure to intellectual properties, while copyright secures economic benefit to copyright holders from the flow"* and in addition write "*All knowledge regulation policies involve balancing access and restriction*". On the other hand, Bode & Jones [21] discuss the proposed new paradigm so-called "right to be forgotten" and they determine it as "*a legal right that allows citizens to petition to have information about them taken down from the Internet*". The authors investigate in this paper the problems of privacy in the information age and conclude that "*the law should apply only in minors*".

The same problems could be determined in all digital environments and technological structures in digital world, including social computing, IoT, M2M communications, distributed mobile e-learning, e-governance realizations, etc.

Kelvin Claveria presents their on-line publication "13 stunning stats on the Internet of Things", 28 April 2017 (https://www.visioncritical.com/internet-of-things-stats/) the comment that "*in 2015, there were about 15,4 billion connected devices and this number will grow to 30,7 billion in 2020, and 75,4 billion by 2025*". The author writes that some of the used units as industrial sensors, connected manufacturing machines, in-store analysis devices and workspace management applications are already on the market and concludes "*These B2B IoT devices will fundamentally transform the way organizations do business with other companies*". On the other hand, the collection and analysis of data from connected devices for identifying human location, devices status and connections will increase – for example for 2017 the part of global manufacturers that use analytics data is about 60%.

A summary of the main challenges of digital spaces which could disturb the user's security and privacy are presented below.

(1) The legislation in the field of privacy and data protection determines three categories of persons which take part in the personal data processing – data controller, data processor and data subject. The right over the personal data has the data subject which is an owner of the personal data. On the other hand, the Directive 95/46/EC determines as an obligation of the data controller defining the goal for personal data processing and the processed categories of personal data. It is very difficult to control these obligations because at several digital environments is impossible to specify what is the role of each participant at communications – data subject, data processor or data controller. This is one of the problems of the digital word (social media, clouds, e-business, etc.), because the functions of customer, vendor and provider and the relation between them could be defined for specific case only. In addition, the service providers

have no legal obligation to protect personal data if they are not defined as data controllers or data processors.

(2) The users with a role of "data subject" (owner of his/her data) have many rights and providers and vendors must protect their personal data collected during the registration procedure and/or during the communications. The first step before starting personal data collection and processing is determining the goal. There are cases for extension of the set of categories of required personal data which must be uploaded in the created profile (for example, names, birth date, address, phone number, social life, gender, country, hobbies, relationships, etc.). This data collection needs restriction and regulation.

(3) The data protection law permits revision by the data owner of all personal data uploaded in his/her profile. The data subject can make access to own data, blocking of incorrect data and delete these data that are not valid, not actual or are not used yet. Data controller must guarantee that each user could define restriction for the own profile accessing. This will prevent unauthorized access and incorrect dissemination of personal information. This action could be realized by making the profile private from the user by selection of the people who can visit the page and to restrict all accesses by using authentication procedure.

(4) Another right of the data subject is to demand deletion of several or all personal data in the profile if the goal is realized (personal data must be canceled at a refusal of environment/service using). The problem is that if any user wants deletion of her/his own data from the personal profile he/she will be not sure that these data are really deleted. The reason is that the data are often transferred to other places in the digital space and there not guarantee that all copies of the data in these places (nodes) have been actually deleted. This problem could be extended with the case of transfer of personal data to third party before required deletion. In this case the destination place will keep the received copy of data and the user will not be aware of that. This will be a problem of privacy for the individual. Data protection legislation gives strong rules for deletion of personal data in the traditional cases, but for the digital spaces (cloud, social environments, mobile network communications, e-business sites, etc.) this is not clearly determined.

(5) The information sharing between potential unknown users could be determined as another challenge for individual's privacy and security. It is well known that sharing information is traditional activity for the network society, but this information (including, for example, and sensitive personal data) could be accessible by unknown users from different places of the world. This could cause serious problems as data loss, integrity destroying, problems with accountability, hackers' attacks, etc. In these cases the data owner does not know what IT security policy and measures are used for counteraction to eventual attacks.

(6) The next challenge for privacy is the data transfer to other countries. According the Directive 95/46/EC the transfer of personal data to third country could be made only if the level of personal data protection in the destination is adequate to this in the EU countries. There is a practice the data to be transferred to different

locations in different countries, for examples for storing data (data centers, cloud infrastructure), between service providers (social media), changing information between collaborators, etc. A request of data protection low is the owner of data to be informed for all transfers of their data.

(7) And finally, another important obligation for all data controllers (providers, vendors, etc.) is to implement appropriate measures for information security and to protect user's privacy. Who will check and control if this obligation is respected? Can the user determine what measures are implemented? Can he/she oppose to illegal access to the information resources and/or unauthorized using private information or personal data? All service providers must guarantee an effective protection of data integrity and data availability in supported digital environment.

4. CONCLUSION AND FUTURE WORK

The first part of the article presents a survey of some opportunities of the digital spices organized as heterogeneous environments based on contemporary technologies as cloud and social computing, e-services and e-management, IoT and M2M, etc. The second part discusses important challenges for user's security and privacy. These challenges are determined on the base of European directives and the rules for data protection and their extension in the point of view new processes in the cyberspace. These challenges define several problems which must be decided for securing privacy of individuals as users of the network services.

As a future work a suitable organization of procedures for secure access and privacy protection could be developed. These procedures should be realized in a united environment which combines traditional infrastructure (own processors and storages) and components of the digital world (cloud, data centers, social networks & media, etc.). This heterogeneous environment must secure adequate identification, verification, authentication and authorization.

REFERENCES

[1] Morales, J. C. (**2008**). Campus as a Framework for Networked University. Chapter in *Encyclopedia of Networked and Virtual Organizations*, Publ. by IGI Global, p. 129-135 (https://www.igi-global.com/chapter/campus-framework-networked-university/17603)

[2] Singh, S. & I. Chana (**2016**). A Survey on Resource Scheduling in Cloud Computing: Issues and Challenges. *Journal of Grid Computing*, Vol. 14, No. 2 (June), pp. 217-264.

[3] Ngai, E. W. T., S. S. C. Tao, K. K. L. Moon (**2015**). Social media research: Theories, constructs, and conceptual frameworks. *International Journal of Information Management*, Vol. 35, No. 1, pp. 33-44.

[4] Whitmore, A., A. Agarwal, L. D. Xu (**2015**). The Internet of Things – A survey of topics and trends. *Information Systems Frontiers*, Vol. 17, No. 2, pp. 261-274.

[5] Verma, P. K., R. Verma, A. Prakash et al. (**2016**). Machine-to-Machine (M2M) communications: A survey. *Journal of Network and Computer Applications*, Vol. 66, May, pp. 83-105.

[6] Acquisti, A., L. Brandimarte & G. Loewenstein (**2015**). Privacy and Human Behavior in the Age of Information. *Science*, Vol. 347, No. 6221, pp. 509-514.

[7] Chang, V., Y-H Kuo, N. Ramachandran (**2016**). Cloud Computing Adoption Framework: A Security Framework for Business Cloud. *Future Generation Computer Systems*, Vol. 57, pp.24-41.

[8] Ali, M., S. U. Khan, A. V. Vasiliakos (**2015**). Security in Cloud Computing: Opportunities and Challenges. *Information Sciences*, Vol. 305, June, pp. 357-383.

[9] Friedewald, K., D. E. Moriani (**2012**). Privacy and Data Protection in the Global Network. *Proceedings of the International Conference on Globalization*, 23-25 June, France, vol. 1, pp.61-67.

[10] Fischer, A. E. (**2014**). Improving User Protection and Security in Cyberspace, *Report of Committee on Culture, Science, Education and Media*, Council of Europe, 12 March. Available at: http://www.statewatch.org/news/2014/mar/coe-parl-ass-cyberspace-security.pdf

[11] Aced Félez, E. (**2015**). The Proposal of the European Commission for a Data Protection Directive in the Police and Criminal Justice Field. *International Journal on Information Technologies and Security*, Vol. 7, No. 2, pp. 37-58. (http://ijits-bg.com)

[12] Tang, B., R. Sandhu & Qi Li (**2015**). Multi- tenancy Authorization Models for Collaborative Cloud Services. *Concurrency and Computation: Practice and Experience*, Vol. 27, No. 11, pp. 2851-2868.

[13] Hashem, I. A. T., I. Yaqoob, N. B. Anuar et al. (**2015**). The Rise of "Big Data" on Cloud Computing: Review and Open Research Issues, *Information Systems*, Vol. 47, No. 1, pp. 98-115.

[14] Ren, L. et al. (**2017**). Cloud manufacturing: Key Characteristics and Applications. *International Journal of Computer Integrated Manufacturing*, Vol. 30, No. 6, pp. 501-515 http://dx.doi.org/10.1080/0951192X.2014.902105

[15] Ivanova, Y. (**2017**). Modelling the Impact of Cyber Threats on a Traffic Control Centre of Urban Auto Transport Systems, *International Journal on Information Technologies and Securit*y, Vol. 9, No. 2, pp. 83-95.

[16] https://en.oxforddictionaries.com/definition/social_network

[17] Nations, D. (**2017**). What Is Social Media? Explaining the Big Trend. Take a closer look at what 'Social Media' is really all about, *Lifewire*, 30 May 2017, available at: https://www.lifewire.com/what-is-social-media-explaining-the-big-trend-3486616

[18] Kallas, P. (**2017**). Top 15 Most Popular Social Networking Sites and Apps, *Dreamgrow*, 20 May, available at: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/

[19] Romansky, R. (**2014**). Social Media and Personal Data Protection. *International Journal on Information Technologies and Security* (ISSN 1313-8251), Vol. 6, No 4, pp.65-80.

[20] Haggart, B., M. Jablonski (**2017**). Internet Freedom and Copyright Maximalism: ContradictoryHypocrisy or Complementary Policies? *The Information Society. An International Journal*, Vol. 33, No. 3, pp. 103-118.

[21] Bode, L., M. L. Jones (**2017**). Ready to forget: American Attitudes Toward the Right to be Forgotten. *The Information Society*, Vol. 33, No 2, pp.76-85