PRIVACY AND DATA PROTECTION IN THE CONTEMPORARY DIGITAL AGE

Radi Romansky *

Department of Electronics and Electro-energetics
Technical University of Sofia
Bulgaria

* Corresponding Author, e-mail: rrom@tu-sofia.bg

Abstract: The aim of the article is to review the development of the contemporary information society based on growing informatization of social processes and to systematize the main challenges for user's privacy and personal data protection. In this reason a brief overview of features of digital age based on the main privacy issues is made and the possible problems for the personal data are discussed.

Key words: informatization, information resources, digitalization, data protection, privacy, security.

1. INTRODUCTION

The constant increase in the application of information and communication technologies (ICT) in modern social processes affects the development of the information society and determines the need to know their features and capabilities, as well as the impact on privacy [1, 2]. One of the topics for discussion in the digital age is the level of competence of users of digital services in the network space and their digital literacy of [3, 4]. This is related to the informatization of society, which builds the basis of the information society and is a continuous process for social, economic and scientific and technical development of the social information environment [5]. The aim is to create opportunities to meet the information needs of people in the realization of the rights of citizens, authorities and organizations. This requires ensuring adequate personal data protection (PDP), both for users using ICT, such as social media [6], and for the transfer, storage or remote access to distributed information resources in the global digital space, including in the cloud [7].

The aim of the article is to review the development of informatization in the contemporary digital age and to systematize the main challenges for the privacy and PDP of citizens using modern ICT and the various technological capabilities of the global digital space. To fulfil the task in the next section, a brief overview of the development of the information society and the role of global informatization is made. Section 3 deals with the main features of privacy and data protection in the information society, including the historical development of processes for informatization of the society. Section 4 discusses the contemporary principles of remote access to information resources and the need for a clear policy for personal data protection, and section 5 summarizes possible privacy issues in the digital world, addressing possible problems in Internet communications, cloud services, IoT and Big Data.

2. DEVELOPMENT OF THE INFORMATION SOCIETY

The introduction of the concept of "information society" was made simultaneously in Japan and the United States in the 1960s, and in the 1970s and 1980s different terms were launched, differently related to the consistent informatization of society through the advent of ICT. The word "informatization" is offered in two independent works by Marc Porat (1977) and S. Nora & A. Minc (1978). Later, Academician A. P. Ershov (Russia) defined informatization as "*a set of measures to ensure the full use of reliable and comprehensive knowledge in all socially significant activities*", and G. Wang (1994) linked it to the processes of promoting information and accelerating its dissemination in order to raise the economic, political, social and cultural status of society.

At the beginning of the 21st century, various authors define informatization as a basis for building a modern information society and define it as a process for more significant use of contemporary ICT (Everett Rogers, 2000). Kim (2004) proposes measuring the level of informatization in individual countries based on the criteria (parameters): “Education”, “Research”, “Agricultural sector”, “Intellectual property” and offers 3 approaches for its conceptual definition: (1) Economic information; (2) Technological capabilities (ICT data and number of computers per unit of population); (3) Awareness (number of published technological journals). A summary of the informatization of society at the present stage is made in [8], defining it as "*development, high-quality improvement, radical strengthening by means of modern information and technological means of cognitive social structures and processes*".

Two main approaches to public informatization can be determined [9]: (a) a technocratic approach in which ICT are mainly aimed at ensuring higher efficiency of work in the field of production and management; (b) sociological approach, considering informatization as a process for development of human activity in all spheres and perceived as a set of interrelated technical, economic, social, political and spiritual-cultural factors.

At today's stage of development it can be assumed that the real modern information society "starts" from the beginning of the XXI century, defining several discussed criteria: *Technological* – analysis of information technologies used in production, administration, education and everyday life for increasing the efficiency of processes realised in the network environment and information management [10, 11]; *Social* – investigation of processes that are an important stimulator for changing the quality of life [12]; *Economic* – analysis of information, a key factor in the economy such as resources, services, goods, source of added value and employment [13]; *Political* – freedom of access and dissemination of information and ideas related to political processes, allowing consensus between different classes and social strata of the population [14]; *Cultural* – recognition of the cultural values of information in the contemporary digital age, because "*the advent of digital technology has significantly transformed human lives and added new dimensions to our consumption behaviors*" [15], that are constantly changing the socio-cultural dynamics of the society.

The main goal of the contemporary information society is the effective implementation of ICT and using the opportunities of the global network space to improve the social, economic and cultural status of society by implementing fast and efficient data exchange between different organizations, administrative structures and businesses, as well as providing citizens with various electronic services. This sets the main task of providing conditions for effective and modern management based on the development of information environments, systems and platforms for remote access to distributed information resources and protection from various malicious attacks [16]. The realization of this goal is based on the following components of the digital age: ✓ Information and Communication Technologies; ✓ Information Resources; ✓ Information Security.

Unfortunately, the so-called "information avalanche" related to the abundance of information resources and the information offered can also create side effects, as a discussion on the topic was made in [1]. The article emphasizes the negative impact of informatization and globalization in modern society, which leads to an "anthropological crisis" and causes structural transformations in various spheres of public life, changing their social status to no sociality. To this opinion must be added the problem of possible breaches of security and privacy of consumers [17], which requires serious measures to protect privacy and personal data, as well as a policy for digital literacy of society.

3. FUNDAMENT OF PRIVACY AND DATA PROTECTION

Privacy is a fundamental human right recognized in many international agreements and documents, but the important question is "What is privacy?" The scope and content of the concept can be determined on the basis of national culture and individual characteristics of the population, but there are also common things, such as the inviolability of personal information and its protection (access, use, dissemination, transfer, etc.). In this reason, everyone has the right to the protection of personal data and two forms of protection are defined, which reflect on the subject – "right to privacy" and "right to data protection".

There are not many attempts to define "right to privacy", and some comments are as follows:

✓ The term should not be defined as a separate legal right, and existing laws related to privacy should be sufficient.

✓ In order to define personal inviolability (privacy), it is necessary to find a common connection between the different essences of the court case on the topic.

✓ Another comment treats privacy as "digital privacy" and suggests that the right to privacy be seen as an independent right deserving of regulation.

A summary of the comments in the literature is that right to privacy is the right to protect all things that are directly related to the person (body, home, property, thoughts, feelings, secrets, identity, correspondence, etc.). This right allows the individual to choose for himself what part of the personal space to make available to others, as well as to determine the manner and time of use.

A study of the evolution of the concept of the right to privacy, together with a comparative analysis of the right to its global protection, was made in [18]. The book assesses international law in the field discussed in both historical and contemporary contexts, emphasizing the impact of technology on the right to privacy and ways to protect it in the contemporary digital age.

Personal data protection (PDP) is a right that is determined by the relationship between the individual and society, including government institutions, companies and other entities and is directly related to privacy (GDPR defines "right to data protection" as an important category). The Charter of Fundamental Rights of the European Union (CFR), which became binding on 1 December 2009, recognizes the right to privacy in Article 7 and the right to the protection of personal data in Article 8. In addition, Article 8 confirms the principle that personal data must be processed fairly and for specific purposes on the basis of the consent of the individual concerned or for other lawful purposes determined by law.

The real start of the development of a European legal framework for data protection began with the adoption of the first PDP law in the state of Hesse in the Federal Republic of Germany (1970), followed by the national laws of Sweden (1973), Germany (1977) and France (1978), in 1979 and in Austria, Denmark, Luxembourg, Norway. Spain, Portugal and Austria include the principles of the PDP as fundamental human rights in their Constitutions. The United States has passed a federal privacy law (Privacy Act of 1974 - 5 U.S.C. §552) [1], which regulates "the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies." and sets specific requirements for the publication and disclosure of such data.

In the 1980s and 1990s, the current legal PDP framework for Europe was created by developing recommendations for the cross-border flow of available data (1980), the founding Convention 108 of the Council of Europe (28 January 1981) on the protection of individuals with regard to automated processing personal data, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995), Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector (1997).

In the 21st century, the basic PDP standards and the EU legal framework are defined, the main documents being Directive 2000/31/EC for e-commerce (legal aspects of information society services, in particular e-commerce in the internal market), ePrivacy Directive 2002/58/EC (on the processing of personal data and the protection of privacy in the electronic communications sector), Directive 2006/24/EC on the protection of traffic data in the provision of publicly available electronic communications services or public communications networks, Directive 2009/136/EC on universal service for consumers' rights relating to electronic communications networks and services (last two revised Directive 2002/58/EC). Of course, reference should also be made to the main document General Data Protection Regulation (GDPR)

[1] https://www.justice.gov/opcl/privacy-act-1974

- Regulation 2016/679 of the European Parliament and of the Council of Europe, adopted on 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, in force since May 2018

4. PRIVACY IN THE DIGITAL AGE

In today's digital world, global communications are widely used for remote access to information resources, websites, virtual spaces, discussion and social forums and more. In this way, any user of network communications can freely "cross national borders" and access remote sites in the network space (Figure 1).

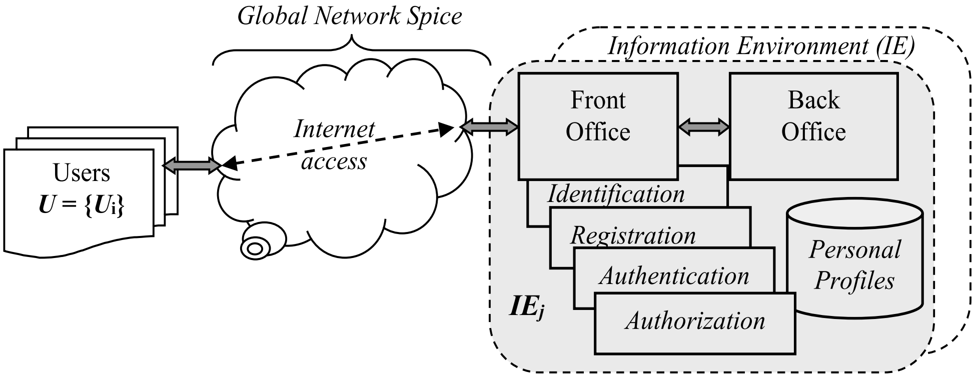

Figure 1. Remote access to distributed information resources in the digital age

Each remote user $U_i \in U = \{U_1, U_2, ..., U_N\}$, $U \neq \varnothing$ can access a selected information environment $IE_j \in IE = \{IE_1, ..., IE_M\}$, $IE \neq \varnothing$ via Global Network Spice by using the communication opportunity. It is assumed that each IE_j environment contains its own technological components for the organization of information services, divided into two basic subsystems – Front Office (input portal for the organization of input-output communications and preliminary regulation of access) and Back Office (basic administrative environment from technical-technological means for basic regulation of the access to the resources and their adequate protection from illegal access and destruction).

The main resource in the second subsystem is the maintained personal profiles with personal data for employees and registered users, and the general management must comply with a specified PDP-policy, which is part of a common security policy and in particular an information security policy. (Figure 2).

The main part of the problems of information security in the network world can be related to the violation of digital privacy (e-privacy), because different environments in the global network require prior registration of users by providing categories of personal data that are not directly related to the specified purpose. The result of the survey of EU citizens is that 74% of them believe that the disclosure of personal data is an existing problem in today's digital world, while another 84% said that the global network requires too much personal data that does not meet of the set goal. At the same time, 72% of network users fear that they do not have full control over their data. It is known that some users agree to the privacy policy maintained by the relevant network space without being aware of it. In certain cases, information about this policy is not provided or personal information is required during registration without the person having an idea of how it will be processed. In most cases, users have no choice but to provide the requested personal data if they wish to access the selected network space.

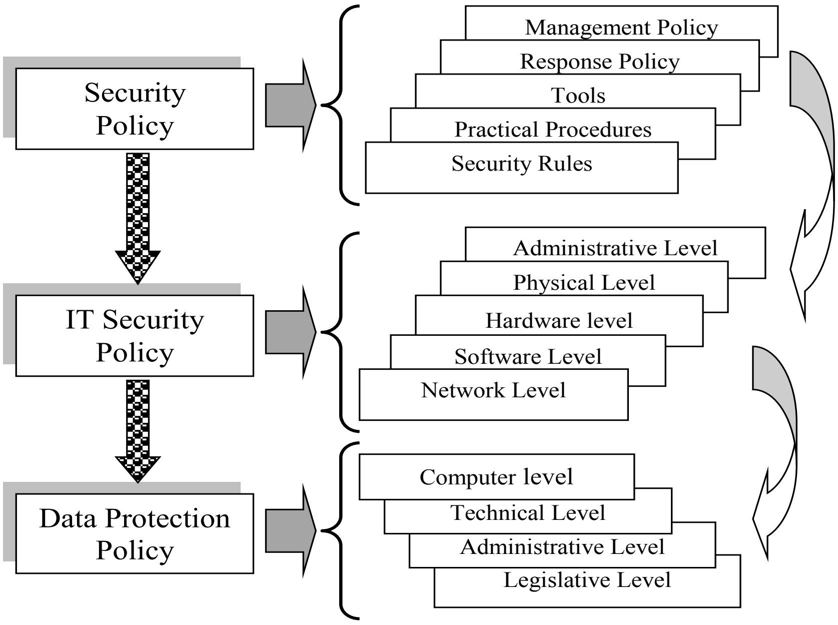

Figure 2. Hierarchy and responsibilities of the policies

All of the above raises the important questions:

✓ How and where the personal data is provided stored?

✓ Who has access to them and what regulations are valid for them?

✓ Who is responsible for the protection of user data and the procedures for their processing, including modification and deletion?

✓ Do the policies required by the GDPR, such as ‘privacy by design’ and ‘privacy by default’, apply?

✓ What is the guarantee for correct transfer of personal data between different nodes in the global network and does it comply with the requirement to maintain an adequate level of protection?

The answer to the questions can be given after an adequate Information Resources Security System has been established, which must provide the necessary security and protection of the personal data in the supported accounts. In principle, this is a set of technical, technological and organizational means that must comply with the provisions of the GDPR regulation: ✓ ensuring the necessary level of protection of personal data stored in automated or non-automated registers; ✓ counteraction of external and internal influences on the security of the data in the maintained personal profiles (accidental or intentional interventions for destruction, loss or modification of data; unauthorized access; virus programs, etc.); ✓ overcoming unqualified actions by the staff and their consequences; ✓ provision of adequate countermeasures for losses in case of damages, accidents and natural disasters;

All this requires that measures be envisaged at each of the successive levels of the data protection policy in Figure 2.

5. POSSIBLE PRIVACY ISSUES IN THE DIGITAL WORLD

User's privacy and PDP in global network is well discussed in various forums and by institutions on European and World level. A key element of the digital space is the maintenance of websites, as an important requirement is that the information published in it must be correct, reliable and that the necessary protection measures are taken when communicating with users and collecting their personal data. This is the responsibility of the site owner, who must ensure that the published information is brought into line with the requirements of the new regulation. The reason for this is that this information is publicly available and in certain cases may lead to a risk for the owners of this personal data (phone, address, photos, CV, financial documents, etc.) with undesirable financial and psychological consequences, as well as consequences for reputation.

The published information on the network, incl. in social networks, data centers in the cloud, as well as in the construction of heterogeneous environments for distance and e-learning [19], must comply with the requirements for lawful and correct processing of personal data, the information must be sufficient and relevant to the goal, to have clear consent of the person who is the owner for his personal data. One of the mandatory requirements of the GDPR is "the right to be forgotten / erased", which sets out the right of the data subject to request incorrect data to be corrected, removed or blocked, as well as to require the removal of links to personal data when the information is inaccurate, inadequate, inappropriate or excessive for the purposes of data processing.

5.1. Privacy in Internet and Mobile Communications

The basic requirements for Internet service providers for different types of network communications are clearly defined in various data protection documents. One summary is the following:

✓ ensuring confidential communication by prohibiting the listening, eavesdropping or storage of messages without the consent of the data subject;

✓ ensuring the security of the services through appropriate measures introduced by the e-mail providers;

✓ notifications of data breaches when the provider identifies security issues leading to loss or theft of personal data;

✓ traffic and location data must be deleted or anonymous when no longer required for communication purposes or other legal situations;

✓ prior consent before sending unsolicited commercial messages (known as "spam"), which includes SMS text messages and other electronic messages;

✓ requirement of prior consent for inclusion of public directories (telephone number, e-mail / postal address) in a public directory;

The "cookie" (a small text file with user information stored on the website for better performance by preserving user preferences) is widespread on the Internet. Under the new rules, the user must be informed about the use of cookies and ask for his consent, giving the option to deactivate or not to accept cookies on their own device. It is also his right to know how the information from the cookies will be used.

Another area is social communications, united in the common direction of Social Computing (SoC), which are a tool for relationships with friends, family and colleagues. It should be borne in mind that the provision of personal information, photos and comments can be seen by a wider range of people than previously thought, and this leads to a possible risk to privacy [6, 20]. In some cases, presets on sites that work by default allow one-click to accept user terms without actually knowing what they allow in their accounts. Even when visiting the site once, the user's personal data is saved and automatically sent to the central office.

5.2. Privacy in Cloud Computing and Internet of Things

Cloud Computing (CC) is a technology of a distributed environment of connected and virtual computers for the provision of computer resources and services on a contractual basis between a customer and a provider. It is based on multiple hiring, which together with maintaining copies of data in different nodes of the network creates possible risks to the confidentiality of information. This sets the basic requirement for ensuring reliable information security by ensuring access only to authorized persons. The principle of multiple hiring can lead to a breach of the integrity of the information and create a risk of breach of integrity (intentional or unintentional) and the availability of supported data, including personal data (deletion, modification, theft). On the other hand, the so-called residual data (not deleted data in network nodes) is a clear violation of "right to be forgotten / erased".

The business uses a single-sign-on (SSO) approach to integrating production directories, with most direct communication systems also integrating authentication with existing production systems, which creates a risk to the information maintained on access. Another applied approach is "share link", which is convenient for sharing data with various business partners, but it is not secure because it creates conditions for a breach in system security and data leakage to an unauthorized domain. All of this requires ensuring the confidentiality of the software to ensure that each application or process will process and maintain the information in a secure and reliable manner.

There are similar risks with the Internet of Things (IoT), based on the presence of many objects and devices that are connected to the Internet and can send and receive data. For this purpose, the devices and objects have sensors for measuring parameters and monitoring their values in order to control processes at the level of home, city, health status of persons, etc. In this reason, IoT (via connected devices) creates potential opportunities for violation of the user's privacy, because the relatively independent communication of devices with the Internet violates the confidentiality of collected data, and the security in IoT is a problem because often configuring devices happens with "weak" or standard passwords

Studies define the significance of possible risks to IoT security in the following order: (1) Insecure web interface; (2) Inadequate authentication and authorization (3)

Insecure network services; (4) Lack of transfer encryption; (5) Problems with privacy; (6) Insecure cloud interface; (7) Insecure mobile interface; (8) Unreliable security system configuration; (9) Unreliable software / firmware; (10) Poor physical security.

5.3. Privacy in Big Data and Big Data Analytics

Big Data (BD) is information collected and stored in very large volumes, obtained from various sources, for further processing and analysis. The principle "the more data is the better" generates a problem for privacy due to the huge amount of information, the diversity of sources, the different forms of existence and the possible lowering of the supervision of this data. The principle of BD technology makes the principle of "data minimization" meaningless, as well as the requirement to predetermine the purpose of their collection, the basic requirements of the GDPR. There is also the possibility that the data collected is outside the jurisdiction of data protection, as well as the possibility that the accumulated data sets contain means causing breaches in information security.

Big Data Analytics (BDA) is a method of BD analysis to reveal the causes of events, study trends and form forecasts. This is a time consuming task, but can cause privacy issues as well as run counter to the basic requirements of the GDPR. It is possible, for example, in big data analysis to make decisions using specific (not publicly available) algorithmic and software tools, which will violate the requirement for transparency of processing, as well as the results themselves to lead to breaches of privacy and anonymity. A summary of possible privacy issues is provided below.

1. Although legal requirements exist, consideration has already been given to possible risks of breaching the confidentiality of data when using the BDA. Violated confidentiality can cause inconvenience to certain individuals, including job loss or adverse family consequences in marketing research.

2. The GDPR has introduced strict requirements for anonymization and pseudonymization of personal data used, but with the collection of huge data sets and the use of powerful analyzes, this may become impossible. Also, inappropriate pseudonymization of data can lead to easy disclosure of real people. These problems require the implementation of effective anonymization and pseudonymization policies and procedures to counteract the risks of privacy breaches.

3. Another group of problems is the possibility of discrimination and unethical actions in interpreting BDA results, for example when selecting job candidates, speculating on human health, denial of service due to incorrect conclusions about race, property status, sexual orientation or other.

4. There is no guarantee that the BD analysis performed and the results obtained by them are completely correct and accurate. Data files may contain inaccurate or atypical data, use incorrect data models, refer to atypical individuals, or apply incorrect algorithms. Obviously, in such a situation, the results will lead to wrong decisions and even false accusations.

5. The collection of data from multiple sources and their storage in different places in the network space allows BD to "exist forever", especially if organizations prefer not to delete data already accumulated – a violation of the right to be forgotten.

6. The problem of searching and e-discovering various documents and data should also not be ignored, because the growing volumes of data make it difficult to identify,

and the search process requires time and resources. This would also make it difficult to determine the level of uniqueness and control of copyright (for example in the patent business) due to the need to visit a huge number of data warehouses.

6. CONCLUSION

The article is an attempt to summarize the features of the new digital age, based on modern technologies and new approaches to communication between people. The high efficiency of the digitalization of the society cannot be denied, not only with the application of the technologies discussed above, but also in the field of e-government, e-learning, as well as with the offer of many e-services (e-banking, e-business , e-voting, etc.). However, it is also necessary to analyze the possible problems that could lead to undesirable consequences for participants in the digital world, so that the latter can be aware of them and take the necessary precautions to protect their privacy and identity. This is the main reason for proposing this material, which is a summary of research conducted by the author in the field of personal data protection and privacy, security policies and technologies for organizing systems to manage access to information resources, including arrays (profiles) with personal data.

REFERENCES

[1] Ordenov, S. Polishchuk, O., Skyba, I., Shorina, T. Clarification of problems in modern society in the processes of informatization and globalization, *E3S Web of Conferences*, Vol. 164, article 11037, May 2020, 15 p. DOI: https://doi.org/10.1051/e3sconf/202016411037

[2] Romansky, R., I. Noninska. Challenges of the Digital Age for Privacy and Personal Data Protection. *Mathematical Biosciences and Engineering*, ISSN 1551-0018, Vol. 17, No. 5, August 2020, pp.5288-5303. DOI: 10.3934/mbe.2020286

[3] Soldatova N. F., Rebrikova N. V., Zakharenko I. K. Informatization of Society: The Development of Key Digital Competencies of Personnel. In: Ashmarina S. I., Mantulenko V. V. (eds) *Digital Economy and the New Labor Market: Jobs, Competences and Innovative HR Technologies*. IPM 2020. Lecture Notes in Networks and Systems, Vol. 161, 2021, pp 496-505, Springer, Cham. https://doi.org/10.1007/978-3-030-60926-9_63

[4] Reddy, P. Sharma, B., Chaudhary, K. Digital Literacy: A Review of Literature, *International Journal of Technoethics*, Vol. 11, No. 2, 2020, 30 p. DOI: 10.4018/IJT.20200701.oa1

[5] Romansky, R. Informatization of the Sciety in the Digital Age. *Biomedical Journal of Scientific & Technical Research*, ISSN 2574-1241, Vol, 33, No.3, 2021, pp.25902-25910. DOI: 10.26717/BJSTR.2021.33.005418

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

[7] Romansky, R., I. Noninska. Architecture of Combined e-Learning Environment and Investigation of Secure Access and Privacy Protection. *International Journal of Human Capital and Information Technology Professionals (IJHCITP)*, ISSN: 1947-3478, Vol. 7, No 3, 2016, pp. 89-106. DOI: 10.4018/IJHCITP.2016070107

[8] Goncharov, V. N. Informatization of Society: Social and Economic Aspect of Development. *Proceedings of the VIII International Scientific Conference on Informatization of society: socio-economic, socio-cultural and international aspects*, 15-16 January 2018, ISBN 978-80-7526-263-9, pp. 8-11.

[9] Vasilenko, L. A. Public Policy in Digital Society. *XXIII International Conference on Culture, Personality, Society in the Conditions of Digitalization: Methodology and Experience of Empirical Research Conference*, Vol. 2020, KnE Social Sciences, 2020, pp. 585–593. DOI: 10.18502/kss.v5i2.8404

[10] Kravets, O.Ja., Atlasov, I.V., Aksenov, I.A., Molchan, A.S., Frantsisko, O.Yu., Rahman, P.A. Increasing efficiency of routing in transient modes of computer network operation, *International Journal on Information Technologies and Security*, vol. 13, No. 2, 2021, pp. 3-14.

[11] Cheryshov, A.B., Choporov, O.N. Preobrazhenskiy, A.P., Kravets, O.Ja. The development of optimization model and algorithm for support of resources management in organizational system *International Journal on Information Technologies and Security*, Vol. 12, No. 2, 2020, pp. 25-36.

[12] Baraković, S., Baraković Husić, J., van Hoof, J., Krejcar, O., Maresova, P., Akhtar, Z., Melero, F.J. Quality of life framework for personalised ageing: A systematic review of ICT solutions. *International Journal of Environmental Research and Public Health,* Vol. 17, No. 8, 2020, art. 2940. DOI: https://doi.org/10.3390/ijerph17082940

[13] Tsonkov, N. Economic security and regional policy. *International Journal on Information Technologies and Security*, Vol. 13, No. 1, 2021, pp. 101-109.

[14] Ninov, M., Atanasov, Pl. Content analysis as a way of identifying hybrid threats in the media content. *International Journal on Information Technologies and Security*, Vol. 11, No. 3, 2019, pp. 101-108.

[15] Dey, B.L., Yen, D., Samuel, L. Digital consumer culture and digital acculturation. *International Journal of Information Managemen*t, Vol. 51, April 2020, article 102057. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.102057

[16] Krokosz, T., Rykowski, J. New approach to IoT authorization based on single-point login and location-specific-rights. *International Journal on Information Technologies and Security*, Vol. 12, No. 1, 2020, pp. 99-114.

[17] O'Neill, O. Trust and Accountability in a Digital Age. *Philosophy*, Vol. 95, No. 1, Jan 2020, pp. 3-17. DOI: https://doi.org/10.1017/S0031819119000457

[18] Rengel, Al. *Privacy in the 21st Century*, Series: Studies in Intercultural Human Rights, vol. 5, eISBN: 978-90-04-19219-5, October 2013, 268 pp.

[19] Romansky, R., I. Noninska. Technological Organization of the Access Management to Information Resources in a Combined e-Learning Environment. *International Journal on Information Technologies and Security,* ISSN 1313-8251, Vol. 11, No. 4, 2019, pp. 51-62.

[20] Romansky, R. Social Computing and Privacy. *Biomedical Journal of Scientific & Technical Research*, ISSN 2574-1241, Vol. 33, No.5, vol.33, 2021, pp.26156-26162. DOI: 10.26717/BJSTR.2021.33.005455

Information about the author:

Radi Romansky is a full professor at Technical University of Sofia, Department of Electronics and Electro-energetics, Ph.D. in Computer Engineering and D.Sc. in Informatics and Computer Science; Full member of European Network of Excellence on High Performance and Embedded Architectures and Compilation (HiPEAC). He has over 215 scientific publications and over 25 books. Areas of scientific interests: ICT, informatics, computer architectures, computer modelling, privacy and data protection, etc.

Manuscript received on 05 October 2021