A SURVEY OF INFORMATIZATION AND PRIVACY IN THE DIGITAL AGE AND BASIC PRINCIPLES OF THE NEW REGULATION

Radi Romansky

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

Abstract: The paper deals with some features of the network technologies in the contemporary digital word and possible problems for privacy and personal data protection of users. The first part of the article discusses the historical aspects of the Information Society creation (informatization as a process in the society) and of the first steps of the privacy in the world. On this base the new regulation for data protection is summarized and some important possible problems for user's privacy are determined.

Key words: digital age, informatization, privacy, data protection.

1. INTRODUCTION

Our society is in the digital age and this puts requirements for the social life of all humanities in the world. The globalization proposes good opportunities, but it could create different problems for the persons [1]. For example, all contemporary information and network technologies for information distribution and sharing, for remote access to different data (including personal data), etc., determine a fully integrated digital world. This permits to increase the international communication and to obtain new and new forms for collaboration and information exchange [2]. It is good, but each person should know the positive opportunities of the digital world and what sides could have a negative effect.

The informatization of the society is a fact for many years, but the 21st century proposes new technologies for social communications [3, 4], cloud computing [5, 6], Internet of Things (IoT) [7, 8], Big Data Analysis [9, 10]. Each of these technologies has own development in the years and creates new opportunities for collaboration, remote storing data, smart application, processing very large data. Does this create problems for the privacy? This is the question that needs to find the right answer. Some problems in this aspect are discussed in [11, 12]. The basic goal in the digital age is to stop the unauthorized access to all information resources, including personal data of the users. In this reason authors of [6] indicate that the encryption mechanisms "*are not fair enough to stop the unauthorized access to genuine user data*" and propose using two techniques together – user behaviour profiling and decoy technology. On the other hand, a new

European regulation is applicable since May 2018 and some guidelines for using the new technologies as cloud services [13], IoT, etc., have been published. The problems of the access to information resources in the digital space are discussed in [14] too with determining some important challenges for security and user's privacy.

The main goal of this article is to make a survey in two aspects – the continuous informatization of the society and the resulting tasks for personal data protection and privacy. In this reason the initial steps for the contemporary digital world creation and the historical aspects of privacy are discussed as a basis for the transition to the modern understanding of the privacy and personal data protection. The next section discusses the informatization of the society, section 3 deals with the history of the privacy legislation as an introduction to the new European regulation GDPR discussed in the section 4, and finally section presents some important challenges and possible problems of the new technologies for user's privacy and data protection.

2. INFORMATIZATION OF THE SOCIETY

Informatization is a fundamental term for building the Information Society related to the role of the term "Industrialization" for the Industrial Society. UNESCO determines this term as "*development and application of methods and tools for collecting, processing, storing and dissemination of information that permits forming new knowledge and their using for management of the processes in the society*". In this reason the informatization of the society is a social-economical and science-technical process for changing the social information environment, based on creation of optimal conditions for realization of the information necessities by keeping the rights of citizens and organizations. An informatization of the worldview is discussed in [15]. Informatization has the following special features:

- Using information resources and the information culture of citizens;
- Creating different possibilities for using knowledge of human activity;
- The information is basic resource for all activities in the society;
- Using contemporary Information & Communication Technologies (ICT);
- Developing common information space.

What is the history of the term? It has been introduced independently by two authors – by Marc Porat (1977) and by S. Nora & A. Minc (1978) for presenting the important role of the information for creating the new digital age. Acad. A. E. Ershov discusses the concept of informatization of national education in a publication (1979) "School Informatics" (http://ershov.iis.nsk.su/en/node/805749) and determines the term as *"a complex of measures secured full using of correct and true knowledge in all social activities"*. In 1994 G. Wang determines the "informatization" as a process of using information and Information Technologies (IT) to force the economic, political, social and cultural status of the society and to growth the speed, quantity, and popularity of information production and distribution.

In the beginning of the 21st century the discussion of the informatization continues. For example, Everett Rogers (2000) defines informatization as the process through which new communication technologies are used as a means for furthering development as a nation becomes more and more an Information Society. Kim (2004) propose to

measure the informatization in a country using a composite measure made up of the following variables: Education, Research, Agricultural Sector and Intellectual Property. In addition, he determines the Information and Communication Technologies (ICT) and information as important characteristics of the digitalization in the countries.

Two basic approaches could be determined for the informatization:

Technical approach – developing basic technical & technological means and tools for the manufacturing and management by using contemporary ICT for increasing work performance.

Sociological approach – uniting all human activity of persons in the society (knowledge, information, economics, social life, etc.) and determining complex of factors – technical, economic, social, political, cultural, etc.

In the end of the 20th century/beginning of the 21st century the term "informatization" is related to the application of the contemporary tools for information processing, ICT and WWW (World Wide Web) in the development of the society. The goal is to build a developed global communication infrastructure and increasing the effectiveness of using determined information resources based on system computerization of the society. In this reason the information could be regarded as a product of the intellectual activity of the society. All these specific parts of the digital age create with the 21st century the real Information Society with the follow basic features:

Essence – a society in which information is a major product, and the aim is to ensure the prosperity of the economic, social and cultural spheres, with the realization of processes and interactions in society and the economy being realized through the global network and the contemporary ICT.

Objective – effective implementation of modern ICTs to improve the social, economic and cultural status of society through the rapid and effective exchange of data between different organizations, administrative structures and businesses, as well as providing citizens with various e-services and remote access capabilities and use of information resources.

Main task of the IS – by combining different components to provide conditions for efficient and modern management by creating information environments, systems and platforms for remote access to information resources and their use.

Components – the main activities are e-servicing, e-society, e-policy, e-democracy, e-governance / e-government, e-health, e-learning, e-business / e-commerce, e-banking, etc.

New technologies of the 21st century – GRID technology, social communications, cloud computing and its extension to mobile cloud computing, Internet of Things (IoT) with the phases wireless sensor networks, machine to machine (M2M) and cyber physical systems (CPS), Fog machine learning, Big Data and Analysis.

In [16] the author regards the information increasing in the digital age and discusses different sentences and approaches for development of the society, including information revolutions based on social media and blogs, extensions of shared information, remote access to different information resources in the cloud and processing collected big data. All these aspects of the digital age raise the question of the protection of privacy and personal data in the network environment [11, 12].

3. PRIVACY AND DATA PROTECTION – HISTORICAL ASPECTS

Privacy is a fundamental human right with international significance. It is recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional documents. It includes freedom of association and freedom of speech, ability of individuals to keep their personal data and all information about themselves. The basic definition of the term "private life" depends on the national culture and individual's characteristics, but common themes could be determined, for example the confidentiality of personal information and their protection (access, using, dissemination, transfer, etc.). In this reason, each person has the right for protection their personal data. The main paradigm is precisely defined by " **right to privacy**" which is our right to keep domain around us including our body, home, property, thoughts, feelings, secrets and identity. Only we could allow entry in our personal space and this is very important for the digital age and the new technologies. A brief summary of the historical aspects of privacy protection is presented below.

It can be accepted that the privacy has historical roots in Aristotle's philosophical discussion for distinction between public and private spheres. Next important period is XII-XVII centuries in Britain started by Assize of Clarendon (year 1166, which he has suggested the way for the "*abolition of trial by combat and trial by ordeal".* Next phases are *Magna Carta* (year 1215), *"Justice of the Peace Act"* (year 1361) with rules against peeping toms), *"An Agreement of the People"* (year 1647 – for liberty of conscience in matters of religion, freedom from conscription, against discrimination on grounds of tenure, estate, charter, degree, birth or place). Other documents in XII century are *Habeas Corpus Act* (year 1679) and *English Bill of Rights* (year 1689). 85 years later was launched the *Parliamentary Register* reported the details of parliamentary debates which had previously been restricted (victory of the free press and public information).

The 18th century was marked by two significant actions: ✓ James Madison, president of USA, proposed in 1789 "*The Bill of Rights*" determining "*right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*", but did not specifically mention a right to privacy; ✓ a declaration for the rights of the person and citizens was accepted in France in 1789.

Different countries made reforms in the field of privacy during the 19th century. Britain accepted two documents – "*Reform Act*" (1832) for increasing the electorate in England and Wales and "*Slavery Ablution Act*" (1833) which abolished slavery throughout the British Empire. A prohibition for publishing facts from the private life of the humans and provision of strong measures for the infringers was made in France (1858). Norway (1889) included in the criminal code a prohibition for publishing an information for personal or family acts. But the most important act was made in USA in 1890 by the jurists Samuel D. Warren & Louis Brandeis. Their published article "*The Right to Privacy*" determines the paradigm "***right to be let alone***" as a definition of the privacy – each person must choose a reason and a manner for processing the information about personal life. After this publication the disturbance of the privacy has been included in the American precedent legislation.

The activity of Europe in the area of privacy began after the Second World War – Universal Declaration of Human Rights (1948); European Convention on Human Rights (1950); The Wolfenden Report (1957); International Convention on the Elimination of All Forms of Racial Discrimination – CERD (1965); Sex Discrimination Act (1975); International Covenant on Economic, Social and Cultural Rights – ICESCR (1976); UN Convention on the Rights of Child (1985); Disability Discrimination Act (1995); Human Rights Act (1998, in force since October 2000); Recommendation No. R(99)of the Council of Europe for the protection of privacy on the Internet (1999).

Some important documents are accepted in the first decade of 21st century – OECD[1] Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002); Universal Periodic Review (2006) – UN's new review system for security regulation of human rights records of all Member States; OECD Guidelines on Cross-Border Privacy Law Enforcement (2006); UN Convention on the Rights of Persons with Disabilities (2008); The Equality Act (2010) – it brought together over 116 separate pieces of legislation into one single Act.

Personal Data Protection (PDP), as a part of privacy, determines the relations between the person and the society, presented by government institutions, companies, public and private organization and other subjects which process personal data, and this is direct connected with the privacy of these persons. The growth of the IT and increasing the using of computers and information processing in the public sphere in the 1960s and 1970s imposes developing a strong policy for the Data Protection Right and concrete rules for regulation of collecting, storing and processing personal data.

In the early 1970s, countries began adopting broad laws intended to protect individual privacy. Throughout the world, there is a general movement towards the adoption of comprehensive privacy laws that set a framework for protection. Most of these laws are based on the models introduced by the Organization for Economic Cooperation and Development and the Council of Europe. As a result, the first lows and documents are established in Land of Hesse in Germany (1970) – the first law in Europe, followed by national laws in Sweden (1973), USA (1974), Germany (1977) and France (1978). The Privacy Act, § 552a (1974)[2] establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

During 1979 in 7 countries (Austria, Denmark, France, FR Germany, Luxemburg, Norway and Sweden) were adopted general laws for data protection. Spain, Portugal and Austria included PDP as a human right in the Constitutions. In 1980 principles for data protection at trans-border flows were developed.

The first significant document of the Council of Europe is *Convention 108/1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data,*

[1] Organisation for Economic Co-operation and Development

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

ETS No. 108 (1981, Strasbourg) [3], followed by documents Guidelines governing the Protection of Privacy and Trans-border Data Flows of Personal Data (1981, Paris), 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 (24 Oct 1995, EU Parliament and Council)[4], Directive 97/66/EC in the Telecommunications (15 Dec 1997, EU Parliament and Council)[5].

Some documents accepted in the first decade of the 21st century which provide the basis for developing the new regulation of data protection, are listed below:

✓ Directive for e-commerce (Directive 2000/31/CE) – includes some legal aspects of information services, in particular about e-commerce in the internal market[6];

✓ ePrivacy Directive (Directive 2002/58/CE) for PDP and privacy protection in the sphere of e-communications (2002) which defines most clear requirements and limitations for the using of Internet-space for commercial purpose and advertisements by e-mail (spam) [7].

✓ Directive 2006/24/CE on the retention of traffic data in the provision of publicly available electronic communications services or of public communications networks.

✓ Directive 2009/136/CE on universal service for consumers' rights relating to electronic communications networks and services and amending Directive 2002/58 / EC.

4. ORGANIZATIONAL ASPECTS OF DATA PROTECTION AND PRINCIPLES OF THE NEW REGULATION

The ***Data Protection Policy*** must be regarded in the context of IT Security Policy as a part of Security Policy – fig. 1 [14]. The first standard for Security Policy titled "Department of Defence Trusted Computer System Evaluation Criteria (TCSEC)" was accepted in 1985 (USA). TCSEC describes the security policy as a collection of security rules, standards, procedures, instruments and practical instructions for regulation of the management, protection and dissemination of the information. This document gives rules for control of access to the information resources.

Security Policy should be regarded as set of means and methodologies for preventing incidents, detecting attacks and restoring the system after successful attack. It includes rules, procedures and tools used on hierarchical layers (network, software, hardware, physical and administrative).

Data Protection Policy should be discussed in the frame of *IT Security Policy* and harmonization of data protection with information security rules from the security core (computer layer) to the external layers (administrative and legislative) is needed. The computer layer presents embedded instruments for protection of personal data structures (hardware, software, cryptographic, biometric). The physical layer consists of technical instruments, means and tools for unauthorized access blocking, separation of LAN

[3] http://www.coe.fr/eng/legaltxt/108e.htm
[4] http://www.odpr.org/restofit/Legislation/Directive/Directive_Contents.html
[5] http://www2.echo.lu/legal/en/dataprot/protection.html
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000L0031
[7] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058

segments, recognition of legitimate users, etc. The next two layers unite organizational rules, instructions and procedures for administrative control and legislative and normative documents [1].

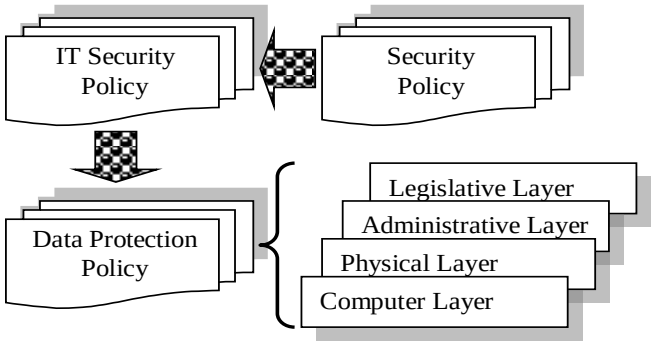


Fig. 1. Place of the Data Protection Policy

European understanding for "personal data" is the information that permits to identify a person directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. The main *organizational procedures* in the field of PDP are presented in fig. 2 as a formalized description by using discrete technique of the Data Flow Diagram (DFD).

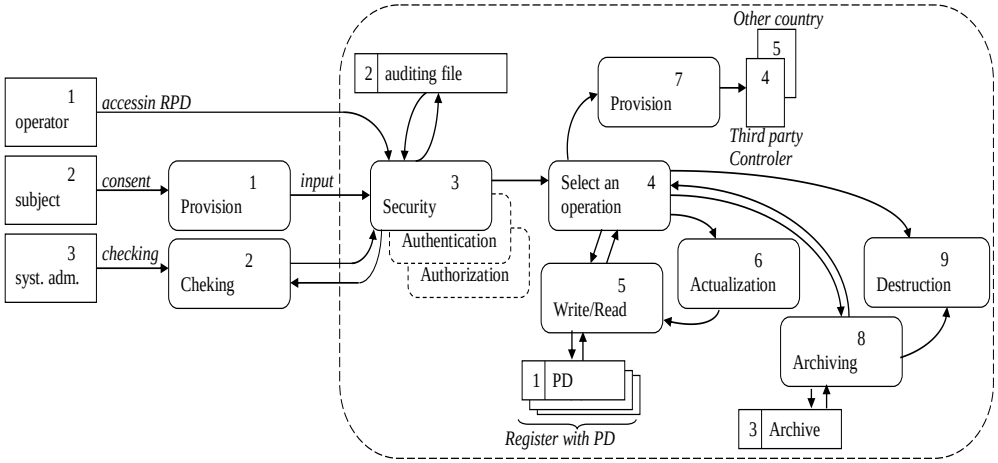


Fig. 2. Formal description of the PDP procedures by using DF-diagram

✓ *Processing of personal data* – this is any operation or set of operations with personal data (using automatic or not-automatic means). The operations are: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, actualization, changing, transfer, using, dissemination, erasing, etc.

✓ *Provision of personal data* – acts of total or partial transfer of a database from one data controller to another, or to a third party on the territory of the country or outside.

✓ *Consent of the data subject* – any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing their personal data.

The main participants in data protection procedures are listed below.

✓ "Data subject" (the owner of personal data) – natural person which is owner of his/her personal data and has rights based on the principles of the right of privacy;

✓ "Data controller" – that determines the purpose and the means of the processing of personal data and it is responsible for all procedures with personal data. It must process personal data based on legal basis.

✓ "Data processor" – which make the real processing of personal data on behalf of the controller and this is a natural or legal person, public authority, agency or other body.

✓ "Data receiver / recipient" – a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

✓ "Third Party" – this is each natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data. The receiving of personal data should be on the base of lawful reason only.

The new European regulation, known as GDPR [17], was adopted on 27 April 2016 after 4 years work on the principles and came into force on 25 May 2018. There is no requirement for formal transposition into national law because it has European validity. The right of privacy and PDP is not absolute right, but it must be regarded with connection to other rights and with their function in the society. The main important factors for GDPR creation are the following:

- Exponential growing of the trans-border flows of personal data;
- High growing transfer and collection of personal data;
- The technologies change the economic and social life and propose new means and tool for information security (stronger frame of data protection);
- Very high sensitivity of the individuals to the personal data.

What are the main changes in the new regulation?

◆ *Expansion of the scope* of the EU legislation on data protection over the foreign companies processing personal data of EU citizens.

◆ Provide *privacy by design* and *privacy by default* for automated protection.

◆ Implementation of *the accountability principle* for personal data processing operations to verify compliance with the requirements of the Regulation

◆ *More rights of the citizens* with possibility for control of own personal data in the digital word and implementation of the paradigm "***right to be forgotten / to be erased***".

◆ *Extension of the definition* of personal data with new "digital" data as IP-address, global location, online identifier, etc. Implementation of new legal rules and definition in the field of cloud computing.

◆ Reduction of the administrative burdens by *removing the registration* as a duty to process personal data.

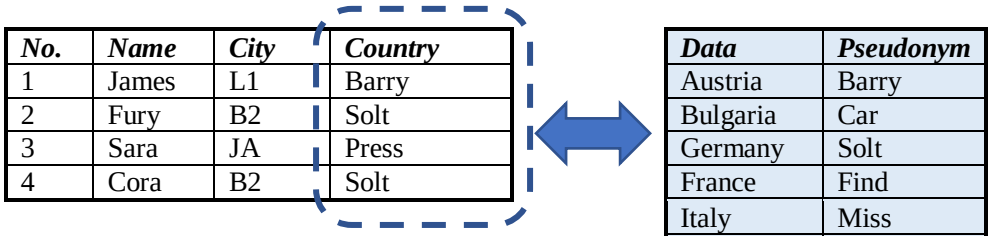
◆ *New mechanisms for data transmission*, complementing traditional practices.

◆ *Support the digital marketing* on a European and global scale.

◆ Establishment of a *European Committee of Data Protection.*

- New requirements on *consent of a child* at providing services in the Internet.
- Implementation of *codes of conduct* and *certification of an organization*.
- *Increased sanctions* for violations.

Practically, GDPR defines the personal data as any information related to a person who can be identified directly or indirectly with specific factors for personal, physical, digital, physiological, genetic, mental, economic, cultural or social identity. In this reason, GDPR introduces the procedure "***pseudonymization***" for processing personal data in such manner that the person cannot be identified. This needs an additional information which must be stored separately and specific technical and organizational measures to ensure only authorized access must be considered – fig. 3.



No.	***Name***	***City***	***Country***
1	James	L1	Barry
2	Fury	B2	Solt
3	Sara	JA	Press
4	Cora	B2	Solt

Data	***Pseudonym***
Austria	Barry
Bulgaria	Car
Germany	Solt
France	Find
Italy	Miss
Spain	Press

Register of personal data with pseudonymised data

Key information whit authorized access

Fig. 3. An example for pseudonymisation of personal data

Another procedure used for supporting personal information is "***anonymization***" – the information in the register with personal data cannot permit identification of the persons (fig. 4). This process is irreversible, and the anonymized data is not subject to GDPR. (applied to media, marketing studies, statistical or research purposes).

No.	***Sex***	***City***	***Country***
1	Male	Sofia	Bulgaria
2	Female	Varna	Bulgaria
3	Female	Arta	Greece
4	Male	Plovdiv	Bulgaria

Fig. 4. Anonymized information in a register with personal data

GDPR changes the paradigm "***right to be let alone***" (see section 3) and introduces a new paradigm "***right to be forgotten / right to be erased***" to guarantee that the period of data storing in the digital environments (sites, social media, cloud, etc.) is limited to the required minimum. The data controller must erase personal data immediately after the goal of collection and processing is realized or transfer to other data controller if this is a legal requirement.

Other new items introduced by GDPR are the Data Protection Officer (DPO) – person which is responsible for all PDP-procedures, creating and supporting "audit registers" for all activities carried out by personal data, terms "privacy by design" and

"privacy by defaults". Privacy by design requires introducing appropriate technical and organizational measures at the phase of initial system development to provide reliable and effective data protection. Privacy by default requires to use appropriate technical and organizational measures, including providing reliable protection during the automated processing of personal data. This principle applies to the personal data already collected, their processing, access and storage and keeping period (the purpose is to ensure that by default will be processed only personal data that are required for each specific processing purpose). Data model and implementation of the regulation based on ISO standards are discussed in [18] and [19].

And finally, GDPR extends the requirements for implementation of appropriate technical and organizational measures to ensure adequate protection and security of personal data in the registers with personal data from any form of illegal activity, especially in the case of electronic transmission, for example: pseudonymization, encryption, confidentiality, integrity, availability and sustainability of processing systems, rules for the prompt recovery of "damaged" data when necessary and access to them, regular checks, assessment and evaluation of the effectiveness and efficiency of technical and organizational measures, rule for regulative access to data (authentication, authorization), backup important data, etc. On the other hand, the regulation extends the data subject rights based on the increasing obligations of data controllers – right to be informed, right for access to the own data, right to be forgotten, right for requests, right to be notified, etc.

5. CONCLUSION

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

The main issue for the information security in the network world could be determined as a violation of digital privacy (e-privacy), because different network environments request preliminary registration of the user and providing some personal data which are not related to the defined goal. 74% of the EU citizens believe that the disclosure of personal data is a growing part of the contemporary digital world.

The new situation in the digital world changes the traditional understanding of the privacy as "the right to be alone" and introduces the new vision – "the right to be forgotten". In this reason, giving different information resources and distributed information services by Internet requires creation of knowledge in the society for principles, methods and technological means and tools for adequate data processing.

Many users agree with the privacy policy maintained by the relevant network space without getting to know it. In some cases, information about this policy is not provided or registration requires personal information without the person having any idea how it will be processed. Users have no choice but to provide the requested personal data if they wish to access the selected network space. The new regulation GDPR must correct these practices in the digital world and to assist to find the right answers to the questions:

✓ How and where are stored our personal data, who has access to them, and what regulations are valid for them?

✓ Who should protect user data, processes and solutions from change and destruction?

✓ What policies apply to storing personal data and confidentiality when processing in digital environments?

✓ What is the guarantee of correct transfer of personal data between different nodes in the global network?

To answer these questions the challenges of the digital age for personal data and digital privacy of users and the possible violations of their integrity and correctness should be determined. This will permit to define rules for effective and successful work in the global network. This will be a goal of a future investigation and publication of the author.

ACKNOWLEDGMENTS

This research has been made with support of project DH-07/10 funded by Bulgarian Ministry of Education and Science.

REFERENCES

[1] Romansky, R., I. Noninska. Globalization and Digital Privacy. *Electrotechnika & Electronica (E+E)*, ISSN: 0861-4717, Bulgaria, **11/12** (vol.50), 2015, pp. 36-41

[2] Thussu, D. K., *International Communication: Continuity and Changes* (3rd ed.), Bloomsbury Academic, ISBN: 978-1-7809-3265-1, 2019 (370 p.).

[3] Kim, J., M. Hastag. Social Network Analysis: Characteristics of Online Social Networks after a Disaster. *International Journal on Information Managements*, **1** (vol. 38), Feb 2018, pp. 86-96; https://doi.org/10.1016/j.ijinfomgt.2017.08.003

[4] Sunstein, C. R. *#Republic: Divided Democracy in the age of Social Media*. ISBN 978-0-691-18090-8, Princeton University Press, 2018 (316 p.).

[5] Samreen, S. N., N. Kharti-Valmik, S. M. Salve, P. N. Khan. Introduction to Cloud Computing. *International Research Journal of Engineering and Technology*, **2** (vol. 5), 2018, pp. 785-788 (https://irjet.net/archives/V5/i2/IRJET-V5I2174.pdf).

[6] Kulkarni, T. R., V. Waghmare, D. Chaudrhary, P. Kulkarni. Security Implementation in Cloud Computing Using User Behavior Profiling and Decoy Technology. *World Journal of Technology, Engineering and Research*, **1** (vol. 3), 2018, pp. 108-113.

[7] Lin, Jie et al., A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, **5** (vol. 4), Oct 2017, pp. 1125-1145, DOI: 10.1109/JIOT.2017.2683200.

[8] Ray, P. P. A Survey on Internet of Things Architectures. *Journal of King Saud University – Computer and Information Science*, **3** (vol. 30), July 2018, pp.291-319.

[9] Oussous, A. et al. Big Data Technologies: A Survey. *Journal of King Saud University – Computer and Information Science*, **4** (vol. 30), Oct 2018, pp. 431-448 (https://doi.org/10.1016/j.jksuci.2017.06.001)

[10] Mikalef, P., I. O. Pappas, J. Krogstie, M. Giannakos. Big Data Analystics Capabilities: a Systematic Literature Review and Research Agenda. *Information Systems and e-Business Management*, **3** (vol. 16), Aug 2018, pp.547-578 (https://link.springer.com/article/10.1007/s10257-017-0362-y).

[11] Romansky, R. Opportunities of the Digital Space and Challenges for Privacy and Individual's Security. *Proceedings of the 31st International conference on Information Technologies (InfoTech-2017)*, ISSN 1314-1023, Bulgaria, 20-21 Sep. 2017, pp. 169-178.

[12] Romansky, R. A Survey of Digital World Opportunities and Challenges for User's Privacy. *International Journal on Information Technologies and Security*, ISSN 1313-8251, Bulgaria, **4** (vol. 9), December 2017, pp. 97-112.

[13] *Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies*, 16 March 2018, European Data Protection Supervisor, (https://edps.europa.eu/data-protection/our-ork/publications/guidelines/guidelines-use-cloud-computing-services-european_en)

[14] Romansky, R., I. Noninska. Access to Information Resources in Digital Spaces – Challenges for Security and Privacy. *Communication & Cognition*, ISSN 0378-0880, Belgium, **1-2** (vol. 50), August 2017, pp. 11-26.

[15] De Mul, J. The Informatization of the worldview, Information, *Communication and Society*, **1** (vol. 2), 1999, pp. 69-94 (https://doi.org/10.1080/136911899359763)

[16] Webster, Fr. Theories of the Information Society, 4th ed. eISBN: 9781317964940, Taylor & Francis, March 2014, 416 p.

[17] Regulation (EU) 2916/679 of the European Parliament and the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protect Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[18] Tzolov, Tz. Data Model in the Context of the General Data Protection Regulation. *International Journal on Information Technologies and Security*, ISSN 1313-8251, **4** (vol. 9), Dec. 2017, pp. 113-122 (http://ijits-bg.com).

[19] Tzolov, Tz. A Model for Implementation GDPR Based on ISO Standards. *Proc. of the 32nd Int'l Conf. on Information Technologies*, 20-21 Sep 2018, ISSN 1314-1023, pp.189-194 (http://infotech-bg.com).

Information about author:

Radi Romansky is a full professor at Technical University of Sofia, Department of Informatics, Ph.D. in Computer Engineering and D.Sc. in Informatics and Computer Science; Vice Rector of Technical University of Sofia; Full member of European Network of Excellence on High Performance and Embedded Architectures and Compilation (HiPEAC). He has been a member of Bulgarian Commission for Personal Data Protection (2002-2007). Areas of scientific interests: ICT, informatics, computer architectures, computer modelling, data protection, etc.

Manuscript received on 8 January 2019