Mathematical Biosciences and Engineering

MBE, 17(5): 5288–5303.
DOI: 10.3934/mbe.2020286
Received: 06 May 2020
Accepted: 22 July 2020
Published: 10 August 2020

http://www.aimspress.com/journal/MBE

Research article

Challenges of the digital age for privacy and personal data protection

Radi P. Romansky [1,*] and Irina S. Noninska [2]

[1] Department of Informatics, Technical University of Sofia, Sofia 1000, Bulgaria
[2] Department of Computer Systems, Technical University of Sofia, Sofia 1000, Bulgaria

* **Correspondence:** Email: rrom@tu-sofia.bg; Tel: +359-2-965-3295; Fax: +359-2-962-4577.

Abstract: Digital age can be described as a collection of different technological solutions as virtual environments, digital services, intelligent applications, machine learning, knowledge-based systems, etc., determining the specific characteristics of contemporary world globalization, e-communications, information sharing, virtualization, etc. However, there is an opportunity the technologies of the digital age to violate some basic principles of the information security and privacy by unregulated access to information and personal data, stored in different nodes of the global network. The goal of the article is to determine some special features of information and personal data protection and to summarise the main challenges of the digital age for the user's security and privacy. A brief presentation of the fundamental legislation in the fields of privacy and personal data protection is made in the introduction, followed by a review of related work on the topic. Components of information security for counteracting threats and attacks and basic principles in the organization of personal data protection are discussed. A summary of the basic challenges of the digital age is made by systematizing the negatives for user's privacy of the contemporary technologies as social computing, cloud services, Internet of Things, Big Data and Big Data Analytics and separate requirements to secure privacy of the participants based on General Data Protection Regulation principles are formulated.

Keywords: technologies of the digital age; information security; privacy; data protection; e-Privacy; challenges for the privacy

1. Introduction

Privacy is a fundamental human right with international significance and it is recognized in the different international and regional documents [1]. Privacy is the ability of an individual or group of individuals to protect the private life and private environment, including the information about

themselves. Several questions could be asked, for example: “What is a private life? What are the boarders of this domain?”. The concrete answers of these questions could be formulated on the base of the national culture and specific individual’s characteristics, but there are common themes which could be discussed for determining the general boarders of the domain “private life”. In general, the domain of privacy partially overlaps confidentiality of personal information and their protection (access, using, dissemination, transfer, etc.). In this reason, each person has the right for protection his/her personal data [2].

The right to privacy forms the common foundation of the freedom of conscience, the right to be secure in one’s person, the right to refuse self-incrimination. The current digital age extends the definition of privacy as a "*privacy in the digital environment (e-privacy)*” [3] and suggests that the "*right to privacy should be seen as an independent right that deserves legal protection in itself*." In this respect, the follow working definition for a "right to privacy“ can be proposed: “*The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity”.* The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing the using of those parts we choose to disclose. The first paradigm related to the privacy has been defined in year 1890 (USA) by the jurists Samuel D. Warren & Louis Brandeis in the article “The Right to Privacy” as a “*right to be let alone*”, which has been included in the American precedent legislation. The new European regulation GDPR [4] changed the vision of privacy by updating it to the digital age and introduced the paradigm “*right to be forgotten / to be erased*”.

Personal Data Protection (PDP) determines the relations between the persons and the society, presented by government institutions, companies, public and private organizations and other subjects which process personal data and this is connected directly with the privacy of these persons. In this reason, the PDP could be regarded as a part of the privacy. The Privacy Act, § 552a (1974) establishes a code of rules for the governments in case of collection, storing, using, and dissemination of information about individuals and supporting records with these data [5]. The growth of the Information Technologies (IT) role in the society and the widespread use of computers and information processing in the public sphere in the last 3 decades of the 20th century imposea developing a strong policy for the PDP, starting with the first laws in different countries during 1970s (Land of Hesse in Germany, Sweden, USA, Germany, France, etc.). The next stage was the adoption of documents that form the basic European legal framework as Convention No. 108 (1981), Directive 95/46/CE for PDP (1995), Directive 97/66/CE for PDF in Telecommunications (1997), Directive 2002/58/CE for PDP in e-communications (2002), Directive 2006/24/CE on the retention of traffic data in the provision of publicly available electronic communications services (2006). This process led to the adoption of General Data Protection Regulation (GDPR) in 2016, which came into force on 28 May 2018 [4,6].

The purpose of this article is to present some main challenges of the contemporary digital technologies (cloud [7,8] and online social networks based on deep neural network [9], Internet of Things and Big Data [10]) for the basic principles of the privacy and PDP. These technologies have good position in the digital age but could cause problems for realization of the principles of “CIA” triad (Confidentiality, Integrity & Availability) and the requirements of the European regulation GDPR [4]. In this reason, a brief discussion of the information security and data protection principles is made in the second section and a summary of the challenges and possible risks for the personal data protection and privacy is presented in the next sections.

2. Related work in the field of information security and privacy

Information Security can be defined briefly as the state of protection of the information resources with different types of data which are stored, processed or transmitted by using computer systems and networks. It must protect the data from different internal and/or external actions that could cause disturbance of system functions, including unauthenticated and unauthorized access. This protection must be realized by using special means and tools (software and hardware) on the base of strong security policy. The information security is an important part of the security in general, which is determined in [11] as "*all about protecting critical and valuable assets*" and the article marks the different parts but not limited as "*... computer security, internet security, communication security, network security, supplication security, data security, and information security*". An important aspect of information security is the development and implementation of adequate policy, but [12] determines that there is no consensus on what an information security policy (ISP) means or how it must be developed. In this reason, the article reviews basic principles of an ISP and study its different definitions and functions based on proposed methodology. The goal is to give a "*better understanding of the current state of ISP development methods and their research as well as their differences and issues*". As a reason for this, the article states that "*a classic definition of ISP goals might be to protect the confidentiality, integrity, and availability (assurance for the service) of information but this view has been criticized for its strong focus on technical security*". In the context of ISP development the architecture is also discussed, which provides that the general policy should be developed at the first (highest) level and then to be created next levels as strategic-level policy, operational-level policy, technical-level policy, etc. and the ISP policy must be integrated with the business strategy.

Another discussion in the field of information security related to the using of cloud technologies in educational institutions, which is made in [8]. The authors determine the protection of the virtual environments as an important security task "*because when multiple virtual machines are located on the same computer, you cannot put a hardware protection device, such as a firewall between them*". Some recommendations for secure use of cloud technologies are proposed in this article. Cloud computing is entering different area of the contemporary world, and this bring some new challenges in the field of information security. This fact is an object of discussion in [7] where is proposed "*a risk assessment approach for assessing the potential damage from the attack on the implementation of components of confidential data and justify the need for the inclusion of private clouds with a high degree of protection in a hybrid cloud computing environment*". The authors determine the proposed approach as a suitable means for estimation of cloud environments which permits to choose the best cloud configuration between different variants and to "*choose more appropriate way according to security requirements arises*".

A problem for information security is discussed in [9] in the context of artificial intelligent and particularly deep learning using in computer vision. The article confirms popularity of Online Social Networks (OSN) for sharing different types of information, but notes that "*attacker exploits fake accounts to distribute misleading information such as malware, virus, or malicious URLs*". In this respect, a deep neural network algorithm named DeeProfile is proposed to deal with fake account issues which is realized by using dynamic CNN (Convolutional Neural Network). The using of deep learning technology for cyber security intrusion detection is extended by survey in [13]. A review of intrusion detection systems based on deep learning approaches is made, 35 well-known cyber datasets are described and their classification is provided. Seven deep learning models are analyzed for studying

the performance in two categories of classification (binary and multiclass).

It is known that the main reasons for the information security disturbance are threats (a potentially possible accident that may have an undesirable effect on the supported system and information resources) and attacks (unauthorized access to a system and corresponding information resources to detect system's vulnerability to common threats). Prevention against them is the subject of research in various publications. For example a threat model and a framework for the secure reuse of software is proposed in [14]. This framework outlines the procedures to follow in order to avoid threats in a simple way and creates opportunity to minimize the risk of introducing security vulnerabilities through third party software components. Article [15] deals with the advanced Transport Management Systems which use virtual and cloud computing for processes automation. The article states that "*it is necessary also to take account of the probable risks, because using cloud technologies could create prerequisites for physical and cybersecurity issues*". In this respect, a method for assessing the probability of cyberattacks in such systems is proposed and simulation experiments are carried out to obtain results for qualitative and quantitative risk assessments determining.

Some challenges caused by application of Internet of Things (IoT) technologies and Big Data Analytics (BDA) in safety critical domains (nuclear power plants, energy grids, health systems, etc.) are discussed in [10]. Concepts of safety and cyber safety considering security and cybersecurity components are object of analysing and some methodological and practical issues are proposed. As an addition some tools in the context of safety and security assessments and assurance are discussed in the article too. Another point of view is presented in [16] proposing Secure and Efficient data perturbation Algorithm utilizing Local differential privacy (SEAL), which "*provides a good balance between privacy and utility with high efficiency and scalability*" in the field of big data and cyber-physical systems.

Privacy is one of the fundamental human rights with great importance, which is recognized in different regional and international documents. This term is associated with necessity and obligation to keep the private life of the individuals secret. It must guarantee confidentiality of personal information by protecting data during inside and outside access, using, dissemination and transfer. These requirements define two important rights – "right to privacy" and "right to data protection". The current digital age extend the privacy definition as a "privacy in the digital environment" or "e-privacy", which is discussed in the General Data Protection Regulation – GDPR [4] and it is created a possibility to define a new data model which is proposed in [17], "*where all constraints and parts of processes are described as metadata and supporting registers of certain events*". Four groups of metadata are determined in this article – metadata for data discovery (a way of recognizing personal data); metadata for data availability; metadata for data use; metadata for data administration and control. The formulated conclusion is that this model "*gives a structured approach to introducing regulatory or ethical data processing restrictions*" and a structured Data Governance Model defining a legal framework is constructed. This will allow stricter organization of personal data processing in all organizations, including the components of e-governance.

In general, e-governance includes many components with e-access and e-servicing and one of them that uses and processes personal data is e-learning. A summary of principles of secure access and privacy in e-learning environment which uses cloud infrastructure and services is presented in [18]. New important challenges in privacy and personal data protection which reflect on the principles of user's security in the cyberspace are discussed. The need for strong security procedures based on authentication, authorization and data protection to protect all information resources and user's profiles

is determined in the article where a functional architecture of combined e-learning environment with two main sub-systems (front office and back office) is proposed. The main procedures for processes organization in this combined environment should provide the required level of security (protection) of the maintained registers with personal data and all information resources. The basic rules are presented by the CIA triad (Confidentiality, Integrity, Availability), which is a model for guiding policies for information security within different organizations and personally for determining procedures for personal data collecting, storing, processing and transfer. Classic CIA triad "*as a basis for carrying out IT risk assessments*" is presented in [19] and ideas how to find the balance between these tree points are proposed.

3. Organization of structures for information security and data protection

3.1. Information security

The European Commission proposes the definition "*Information security is the protection of networks and information systems against human error, natural disasters, technical malfunctions or malicious attacks"*, which includes all Information and Communication Technologies (ICT) and IT-services in the digital age. It is clear that the poor information security might compromise the system and could cause additional damages and costs. There are terms with specific differences in the field of security of information resources: ✓ Information Security is protection of the information in all possible forms (electronic, printed or other); ✓ Computer Security covers the functioning of computer systems and networks and the information processed by them; ✓ Information Protection includes risk management practices related to the use, processing, storage and transmission of information, including systems and processes for that purpose, with the primary aim of preventing data loss in critical situations. Two groups of components of the information security can be determined:

1. Organizational components: ✓ Physical security for protection of physical data resources and systems (hardware, software, networks, etc.) and it includes procedures for access control, limited copying of data to other devices, separated segments of the internal network, and preventive actions against fire, flood, terrorist attacks, etc.; ✓ Security of processes – it is determined as critical for the business processes and must guarantee continuity of the business without interruption due to accidents, natural disasters or human errors.

2. IT components: ✓ Application security (protection against threats, theft, modification, or deletion of the applications); ✓ Mobile security (means and tools for protection of different portable devises and their corresponding network connections); ✓ Network security (set of technologies, policies and practices for protection of the network infrastructure and all connected devises, including the endpoints protection); ✓ Internet security (protection of software applications, web browsers and virtual private networks to counteract attempts for data transfer by malicious software, phishing attacks, and denial of service attacks – DDoS).

The strictures for information security must counteract possible threats and attacks. Some of the reasons for possible threats are: ✓ strong increasing in the volume of processed and stored information; ✓ massive use of computer networks and their integration; ✓ expanding the number of users who have access to the system and information resources; ✓ uniting different information funds into a common database and allowing multiple access to it. On the other hand, the "success" of the attacks depend on the level of effectiveness of the information security system. The undesirable features of such an attack

are: ✓ significant remoteness of the offender from the attack object; ✓ the attack can target both a particular computer and a network connection; ✓ the ability to attack network infrastructure and protocols; ✓ attacks to the telecommunication services. Some important information security breaches are summarized in Table 1.

Table 1. Breaches for the information security.

Channels for information leakage	✓ Direct theft of a disk medium; ✓ Copying information from a medium; ✓ Unauthorized connection to an information system or communication channel; ✓ Unauthorized access to information by special means; ✓ Electromagnetic wave interception from an apparatus.
Major violations	✓ Audition without disturbing the operation of the system; ✓ Changing the settings and the state of the system; ✓ Disguise of one logical object as another, possessing greater powers; ✓ Blocking at logical objects; ✓ Re-addressing messages; ✓ Modification of messages and others.
Information security breaches	✓ Attacks on financial systems; ✓ Discretization of the activities of corporations; ✓ Disclosure of corporate secrets; ✓ Sabotage of production processes; ✓ Breach of intellectual property rights; ✓ Illegal disclosure of personal data.

As mentioned above, cloud computing as a technology of the digital age brings new challenges in the field of information security and it is important to organize reliable control of the information risk management processes. In this regard, a qualitative information security risk assessment method with the following basic steps is proposed in [7]: 1. Risk identification ➔ (1.1. Identification of information security risks and influence on assets; 1.2. Identification of assessment object vulnerabilities, provision principles, processes, procedures and security environment). 2. Risk analysis ➔ **(**2.1. Influence level estimation of malicious use; 2.2. Frequency estimation of malicious use). 3. Risk assessment ➔ **(**3.1. Risk level definition for each list of frequency and influence; 3.2. Risk assessment and comparison with criteria of risk acceptance; 3.3. Risk categorization for processing into lists of risks; 3.4. Internal relations definition between risk lists; 3.5. Identification of conflicts between risk lists; 3.6. Appointment of priority list and risks; 3.7. Solution of found conflicts). 4. Risk processing ➔ **(**4.1. Identification of alternative decisions for security provision and their grouping into lists; 4.2. Effect identification and targets of alternative systems of information security; 4.3. Estimation and search of optimal ISS or decision list for security ensuring).

3.2. Personal data protection (PDP)

Personal Data Protection (PDP) deals with the relations between persons and the society, presented by different subjects and authorities as government, state, institutions, public and private organization, companies, etc. The processing of personal data must be based on strong rules for data

protection, keeping privacy of the Data subject. In this reason, all institutions, that process personal data (personally, Data controller) must develop and apply a clear and prompt Data Protection Policy as a part of the Information Security Policy and the Security Policy in general. An organizational structure for Data Protection Policy is proposed in Figure 1.

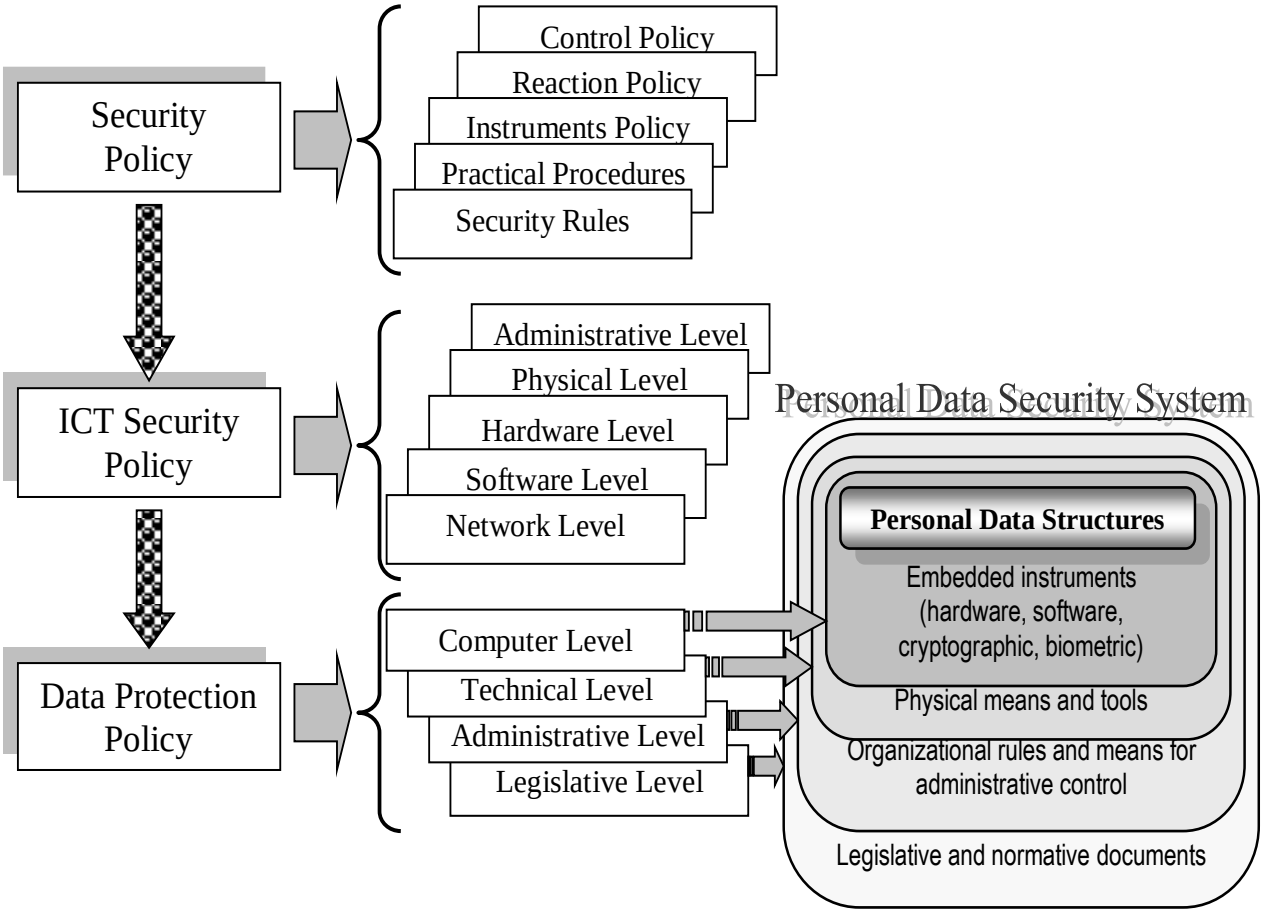

Figure 1. Development of the Data Protection Policy in the digital age.

On the other hand, there are different types of processed information: ✓ Public information which is freely accessed and used, and can be transmitted without limitation; ✓ Official information which is owned of an institution (organization) and it can be stored, processed and transmitted in the frame of the institutional computer systems and via the internal networks (a special permission must be done for transmitting to third party on the public networks); ✓ Confidential information must be processed and stored in the secured institutional computers and transmitted by the external (private) network without connection to the global network (the transmission must be made after encryption approved by the organization). The place of personal data in this classification (in reason data type) could be in the last two categories and all proposed measures in the Data Protection Policy must be used. The computer level includes the most secure means (hardware, software, cryptographic) against attempts of external attacks for unauthorized access to data. The technical level relates to physical tools for protection and means of preventing access by external persons, network separation, separating all servers in a special room, isolation some of servers from the internet, backup the power for servers, etc. The next two levels – administrative and legislative, determine the developing and application of

organizational rules and means for administrative control as an extension of the physical means and application of laws and normative documents for data protection.

A summary of methods and means used for information and data protection and relation between them when a Personal Data Security System (PDSS) is organized is proposed in Figure 2. The presented methods are:

- *Blocking* – prevents unauthorized user's access to the rooms where the data are stored;
- *Access Management* – provides secure use of all information resources and using all system resources by verifying the access rights, preliminary defined for each user;
- *Encryption* – provides using of cryptographic algorithms to encrypt data making them incomprehensible to an illegitimate user;
- *Identification* – identification of staff and individual components of the system that are registered as legitimate users and for which access right have been defined;
- *Control* – methods, which protect data from unauthorized activities of legitimate users;
- *Sanctions* – the protection program describes the internal rules for processing and using the information, and the responsibility of the consumers according to the legal norms and laws.

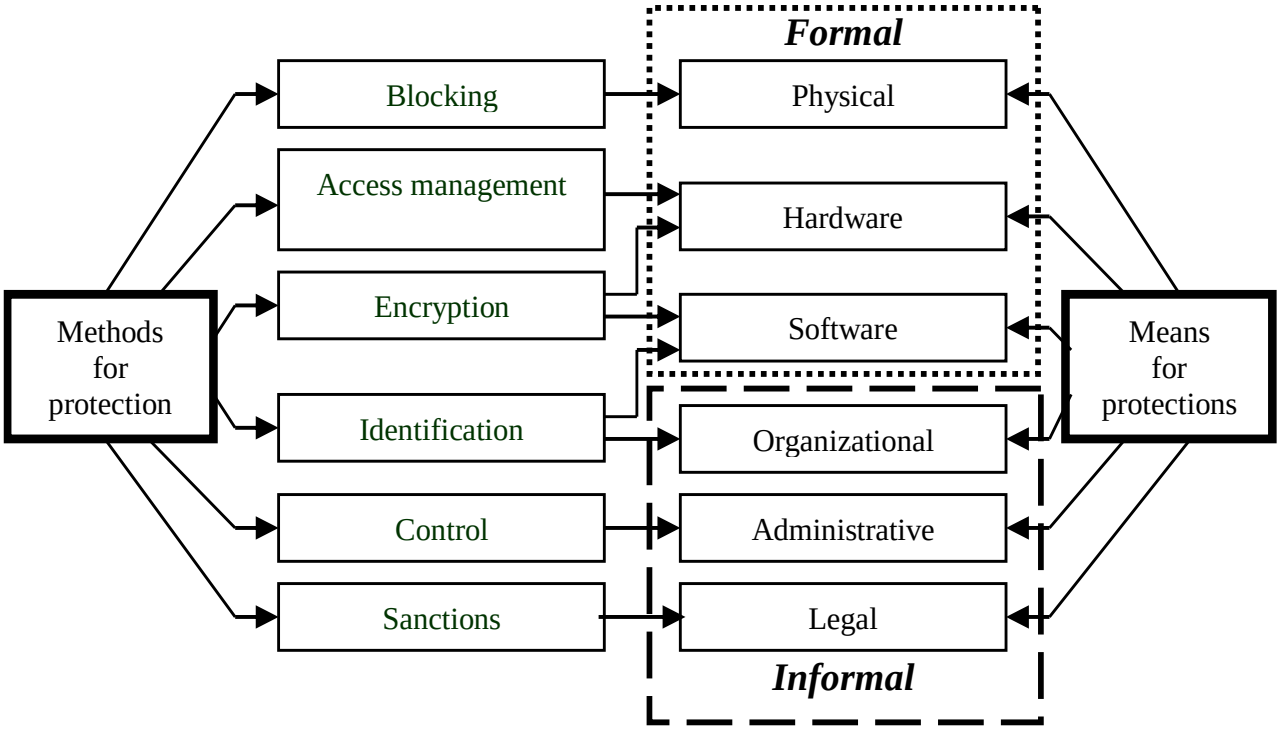

Figure 2. Methods and means for PDSS organization.

4. Challenges of the digital age for privacy and data protection

Information Security and Data Protection are dynamic fields that are constantly challenged and influenced by advances in digital age technologies and innovation in business practices. The ICT development reflects to the rules for data protection organization and changes the understanding for the definition of personal data, management of cross-border data transfer, user's privacy in the digital age, rights of the users and obligations of the data controllers. A survey among Internet users shows that 74% of EU citizens believe that the discovery of personal data is an increasingly integral part of

the digital world. On the other hand only 26% of social computing users and 18% of online shoppers believe that they have full access to their personal data. Many questions can be set about how and where are stored our personal data, who can assess them, who is responsible for the data protection, what policy is applied to store personal data and to keep their confidentiality, what is guarantee of correct transfer of the data between different nodes via the global network. Various examples in the internet can be given. For example in "Privacy Notes" published in the site of a company is indicated that the collected categories of personal data are "*name, gender, birthday or age, homepage, profile photo, time zone, mail address, country, interests, and comments and content you have posted/shared*". Many of these categories are not related to the specific area of the company. These challenges will be discussed in the next sub-sections.

4.1. Social computing (SoC) challenges

It is known that this technology permits to organize a dialog between individual computer users through the Internet by using different environments united under the term Social Networking Sites – SNS (Social Media, Social Networks, Social Bookmarking, Social Aggregators, Blogs & Microblogs, Wikis, Multiplayer games, etc.). Practically the SoC is a useful instrument for connection between users and information sharing, but there is a possible risk to personal data protection because it might happen the information is shared to an unauthorized person. In some cases this can cause negative financial and psychological consequences to the owner of these data. A brief summary of the SoC negatives for user's privacy is presented below.

1. In many cases, web sites play the role of an "open door" – during the preliminary registration or at the first visit with just one "click" users can accept the Privacy Policy without reading the text. The result is full acceptance of all conditions without the user being really aware of them. In this case she/he is not aware of exactly what will happen to her/his personal data in the created user's profile.

2. In other cases, the user's personal data are stored after one visit only and automatically transferred to the center without the owner's knowledge and consent. Indicative is the fact that only 54% of social network users think that they are informed about the conditions for collecting personal data and their next use when they join a social networking site or register for an online service.

3. In some cases, a media may not provide information about the Privacy Policy or require too much personal information when user makes registration which exceeds the defined goal of the media (the GDPR principle of limited personal data is violated).

4. Another problem is the location of stored personal data somewhere in the global network. It may be possible to maintain multiple copies when looking for an acceptable position. This is contrary to the GDPR principle for minimizing stored and processed personal data. An example in this direction is the conclusion of the National Consumer Agency in Germany for violation of legislation on data protection by Facebook with the disseminated information that the advertisements are fully free of charges. The stated reason is that social network receives significant amounts by collecting personal data and their storage in various location in the global network.

5. The above problem causes another negative to do the GDPR requirement "right to be forgotten / erased" in case of refusal of further use. The user cannot be sure that all copies of personal data are indeed deleted in different nodes of the network. There is an example with a law student from Austria who requested all the information that a social networking site (SNS) had stored for him regarding the user's profile. He receive as a response 1224 pages of information including his photos, messages and

publications from years ago, some of which he considered erased. Apparently, the site has collected much more personal information than the user has imagined, as well as storing unnecessary information and one that has been deleted.

4.2. Cloud computing (CC) challenges

CC is a distributed environment based on connected virtual computers with dynamic communications between them, which provides cloud services to the clients (users). The basic cloud services, defined by NIST (National Institute of Standards and Technology) are Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These services could be provided by different types of cloud – public, community, private, and hybrid, including using the technology of the Mobile Cloud Computing (MCC) – uniting the 3 parts: mobile device, mobile internet and cloud computing. The Thales report for 2020 [20] determines that 83% of the organizations use 11 or more SaaS providers and 48% of the corporative data in the cloud are sensitive but only 57% of them are protected by encryption. For comparison, the assessment of data encryption using in the digital space for 2019 is 36%.

Cloud computing does not violate principles of data protection, but can be a risk for cross-border data transfers. Practically, there are not specific regional legislations for personal data protection when using cloud services, however, to support GDPR e-privacy requirements, a document representing guidelines for correct cloud computing services using was developed and published [21]. The CISCO determines that 59% of companies confirm their readiness for the GDPR and other 29% will be ready in early 2020 [22]. The opportunities and benefits of the cloud provoke identification of possible negatives that could be risk to user's privacy and persona data protection, summarized in the Table 2.

Table 2. Possible risks for privacy when using cloud computing.

Subject	Comments
Multi-tenancy	A group of users share services and use the components of the cloud infrastructure which could be risk for the CIA triad: • Confidentiality, because a large number of users can access the stored data by mobile devices and applications; • Integrity, because it is possible some of the cloud users to make attempts for modification of data without permission; • Availability, because the providing access to services, data and tools anywhere, anytime could be a problem for resources.
Data location	The customer does not know where the data are stored.
Regulatory compliance	It is not clear whether the cloud computing provider is determined as a "data controller" of "data processor" and whether he is a subject of external audits and security certification.
Privacy	There is no information what capacity of system restoring is provided
Right to be forgotten	The data usually migrate among different nodes in the cloud and it is difficult to prove if the data are erased in the all places where they have been stored.

4.3. Internet of things (IoT) challenges

The term is used to describe a set of objects and devices that are connected to the Internet in order to send and receive data obtained by using sensors for monitoring of selected parameters and to capture and analyze values obtained to control of processes on different spaces as home, city, health, etc. It is possible that connected devices may disturb the privacy and security and could undermine consumer confidence. In this connection two main aspects of IoT for the privacy and data protection could be defined:

a) Confidentiality – it could be disturbed because each physical or logical object or thing could receive a unique identification code and could freely communicate through the Internet or via the other networks. All data sent from the end points are not the target for the strong confidentiality, but the analysis of these data which are usually received by many points could consist of sensitive information for a person. On the other hand, the increase in the number of sensors leads to the accumulation of data, which increases the risks to security and privacy. For example, when hacking smart sensors, accessing the collected data can lead to learning about certain habits, health and religion data, and more.

b) Security of IoT – a set of different computers and internet devices are configured by using traditional passwords that are not protected, and the things could be object of different attacks. The attacks target components with low-level of "cyber-hygiene" and look for their vulnerability to hacking and tampering. Another problem with IoT security is identity verification - usually a traditional approach is used which hardly provides the necessary level of access control. It is also possible to use devices that have factory default passwords that cannot be changed.

Statistical studies show that IoT devices are susceptible to cyberattacks. For example, 56% of risk professionals report not keeping and inventory of IoT devices and 64% report not keeping an inventory of IoT applications [23]. Other 76% believe that the cyberattacks are likely to be executed through IoT. Other statistics presented in [23] related to the privacy show that 74% of global consumers worry about losing individual rights and only 45% of respondents require the third parties that have access to their sensitive and confidential information to implement measures to ensure reliable data security and protection.

4.4. Big data (BD) and Big data analytics (BDA) challenges

The term "big data" relates to a set of collected and stored information in very large volume received from different sources in different places for further processing for any purpose. This information could exist in different forms. The main idea is "the more data will be better", but it creates negatives for the privacy and is against the GDPR principle of minimizing personal data in processing. BD are collected from various sources for further analysis (BDA) to form conclusions, select solutions, or investigate trends in object behaviour, including for persons. In this sense, BD itself are not a problem for the privacy, but BDA can lead to negative situations for individuals – incorrect conclusions about private life or behaviour of certain people personals, inaccurate trends, etc. The existence of possible negative problems for privacy in BD is discussed in [24] stating that "*big data storage, processing, sharing and management crucial procedures*" which are subject of serious attacks and lead to the violation of privacy. Certain features of the BD/BDA can lead to unwanted negative consequences for privacy and can be defined as follows:

- The processed BD could be collected for different purposes and this violate the important principle of data correctness "Defining the goal". What is the guarantee that the collected data are correct, precise and full (GDPR requirement)?
- The very large scale of the collected data violates another GDPR principle of data correctness – "data minimization";
- Incorrect interpretation of the collected "big data" for a person is possible, which can cause troubles for the relationship of the person in the organization, and in his/her family. The incorrect conclusions can cause some ethical deviations or discrimination (incorrect conclusions for race, status, sexual orientation, etc.);
- Using BDA in business marketing research can lead to incorrect conclusions and may compromise reputation of individuals, for example when recruiting employees;
- The GDPR requirements for anonymization and pseudonymization of personal data cannot be realized by BDA;
- The accuracy of the BDA cannot be full guaranteed, because it is not clear what methods and tools (algorithms, software, applications, etc.) are used for the analysis and this will violate the GDPR requirement for data processing transparency.

5. Requirements for negative impacts limitation

The digital age offers various technological possibilities for solving problems in people's everyday life but, as presented in the previous section, it also creates disadvantages and negative consequences for individuals who are users of e-services. Certain requirements and opportunities can be proposed for limitation of the negative impacts of the digital technologies under user's privacy and data protection.

Social Computing (SoC) is widespread and has many supporters. This significantly limits the ability to regulate activities generally to ensure targeted and reliable protection of consumer privacy. In this respect, it is difficult to determine some general requirements for PDP in social computing, but some recommendations can be made to users. The main principle must be that each user of a social media is owner / holder of his or her personal data and as such has the corresponding responsibilities. The problem is that the GDPR-requirements for legitimate and fair personal data processing could hardly be addressed to the social networks users, but one of the viewpoints accepts each participant in social activities as a data controller of his/her personal data. GDPR has defined relevant obligations to data controllers and in assuming this role, users should be responsible for providing personal data. Another requirement deals with the information uploaded in the social sites – it must be sufficient and relevant to the defined purpose. Finally, the important requirement is that the personal data must be collected and processed based on the consent of the data subject and on the base of the principle of limitation and minimum volume of data. An example of incorrect data processing is the recognition of about 35% of employers that they use personal data from social sites to solve their problems – user preferences, search for suitable employees, etc.

Cloud Computing (CC). The main concerns of cloud service users are the following: ✓ is there a vulnerability to attacks beyond the user's internal protection; ✓ are there adequate data security practices in the cloud; ✓ whether personal privacy regulations are being followed in the cloud. GDPR has introduced fundamental requirements for the digital space and in particular for digital (cloud) service providers, such as:

- Requirement to give explicit and full consent to the collection and use of personal data;
- Users to have easy access to their own personal data and be able to control them;
- An obligation of network service providers is to inform consumers clearly and transparently how the data provided will be used;
- Providing portability rights for personal data (easier transfer from one provider to another).

The main requirement for the cloud computing (CC) is to organize a complex system of information security with special functionality for personal data protection. This system must meet the requirements for common security (external and internal security) and architectural security (problems with virtual machines, data and storages, web applications and API-interface, access regulation and control). To perform these tasks, the system must be organized as a set of components that support the following functions and requirements:

- Requirement for general security management (management of the security processes based on the normative and legal acts, security and PDP policies, procedures and instructions);
- Protection of the perimeter (control and management of the access, security guards and signaling);
- Security of the environment (fire alarm, surveillance of the resources, power backup, condition for functionality, connections, etc.),
- Requirement for serious network protection (against external DDoS attacks and viruses, data loss protection, web-traffic filtering, protection of communication channels, etc.);
- System security, requirement for IT-infrastructure security and protection of the virtualized environment.

Internet of Things (IoT) collects many of the requirements for CC, but it must be clear that the IoT is not only devises, sensors, and network connections and IoT security is not only devices' and network security. The IoT information security integrates elements of the security of devices, network connections, interfaces, software, mobile applications, USB ports, cloud, etc. In this sense, the IoT security and data protection system should implement all requirements of the specified elements in order to provide adequate security. The following basic requirements for IoT security can be defined:

- Connectivity between things must be realized after their identification;
- Interoperability between all connected sub-system must be ensured;
- Specific means and tools must be used to provide correct and precise functionality of all network components and apps for automatic processing the data of things;
- System for information security for IoT must be designed based on the requirements of adopted policies for IT Security and Data Protection, because every "thing" deals with data which can be treated for confidentiality, authenticity and integrity of data (see the "CIA" triad), including personal data too;
- Privacy protection must be important issue of the IoT security, because the monitored and collected data are related to the human life and can consist sensitive data.

Big Data Analytics (BDA) is used to discover the causes of events, to study trends and to form forecasts, which are complex and time-consuming tasks. To solve these problems, large amounts of data are collected from various sources. The diversity of data sources makes it possible to accumulate tools that breach security and privacy. Some basic requirements can be defined as follows:

- Unification of collected data by type and purpose;
- Clear definition of the purpose of the data collection and analysis should only be performed on data corresponding to the purpose for which they were collected;
- BDA should only be performed on lawfully collected data in accordance with GDPR

requirements (avoid data such as court records, personal home records, etc.);

• Adequate decisions must be taken in advance for relevance of the Big Data technology with the GDPR requirement of "data minimization" by taking measures and approaches to anonymize or pseudonymize the accumulated data. The goal is to make impossible to identify a particular person on the base of results obtained by BD processing using powerful analyzes, and to avoid the possibility that the results of the BDA may lead to a breach of the confidentiality of participants.

• BD analysis and decision-making should be based on open and publicly available rules and algorithms, thus ensuring the GDPR requirement for processing transparency

6. Conclusion

The purpose of this paper is to make an analysis of relations between the contemporary technologies of the digital age and the principles of the information security, privacy and personal data protection. In order to clarify the current problems in the field, a review of actual publications has been made in the section “Related work”. Organizational and structural components, as well as possible problems and risk situations in the digital age are discussed in both directions – information security and data protection. On this basis, dependencies between security policies are identified and the place of Data Protection Policy is determined in the discussed hierarchical structure. Classification of appropriate methods and means to ensure reliable data protection is proposed and the relations between the participating components are explained. The goal of the last two sections of the article is to systematize main risk problems of the digital age for user’s privacy, in particular on contemporary technologies, and to propose some requirements to limit their negative impact on users of e-services in the global network.

Conflict of interest

The authors declare that they have no conflicts of interest to this work and they have no commercial or associative interest that represents a conflict of interest in connection with the submitted article.

References

1. E. J. Bloustein, N. J. Pallone, *Individual and Group Privacy*, Routledge, New York, 2017.
2. M. Oostveen, U. Irion, The golden age of personal data: How to regulate an enabling fundamental right?, in *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (eds. M. Bakhoum, B. Conde Gallego, M. O. Mackenrodt, G. Surblytė-Namavičienė), Springer, (2018), 7–26. Available from: https://link.springer.com/chapter/10.1007/978-3-662-57646-5_2.
3. R. Romansky, A survey of digital world opportunities and challenges for user’s privacy, *Int. J. Inform. Technol. Secur.,* **9** (2017), 97–112.
4. *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)*, European Commission, 2016. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

5. J. J. Hanus, H. G. Relyea, A policy assessment of the privacy act of 1974, *Am. Univ. Law Rev.*, **25** (1976), 555.
6. M. Shabani, P. Borry, Rules for processing genetic data for research purposes in view of the new EU general data protection regulation, *Eur. J. Human Genet.*, **26** (2018), 149–156.
7. A. V. Tsaregorodtsev, O. Ja. Kravets, O. N. Choporov, A. N. Zelenina, Information security risk estimation for cloud infrastructure, *Int. J. Inform. Technol. Secur.*, **10** (2018), 67–76.
8. O. Yu. Zaslavskaya, l. A. Zaslavskiy, V. E. Bolnokin, O. Ja. Kravets, Features of ensuring information security when using cloud technologies in educational institutions, *Int. J. Inform. Technol. Secur.*, **10** (2018), 93–102.
9. P. Wandra, H. Jie, DeepProfile: Finding fake profile in online social network using dynamic CNN, *J. Inform. Secur. Appl.,* **52** (2020), article 102465. Available from: https://www.sciencedirect.com/science/article/abs/pii/S2214212619303801.
10. V. Kharchenko, Big Data and Internet of Things for safety critical applications: Challenges, methodology and industry cases, *Int. J. Inform. Technol. Secur.*, **10** (2018), 3–16.
11. I. Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. Al-Qudah, A. Al-Omari, Introduction to information security, in *Practical Information Security* (eds. I. Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. Al-Qudah, A. Al-Omari), Springer, (2018), 1–16. Available from: https://www.springer.com/gp/book/9783319721187.
12. H. Paanen, M. Lapke, M. Siponen, State of the art in information security policy development. *Comp. Secur.*, **88** (2020), article 101608. Available from: https://www.sciencedirect.com/science/article/pii/S0167404818313002.
13. M. A. Ferrag, H. Janicke, Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study, *J. Inform. Secur. Appl.*, **50** (2020), article 102418. Available from: https://www.sciencedirect.com/science/article/pii/S2214212619305046.
14. A. R. Mahlous, SSR: A framework for a secure software reuse, *Int. J. Inform. Technol. Secur.*, **10** (2018), 87–98.
15. Y. A. Ivanova, Assessment of the probability of cyberattacks on Transport Management Systems, *Int. J. Inform. Technol. Secur.*, **10** (2018), 99–106.
16. M. A. P. Chamikara, P. Bertok, D. Liu, S. Camtepe, I. Khalil, An efficient and scalable privacy preserving algorithm for big data and data streams. *Comp. & Security*, Special issue "Security and Privacy in Smart Cyber-physical Systems" (2019), article 101570. Available from: https://www.sciencedirect.com/journal/computers-and-security/special-issue/109XHWZ5JSX.
17. Tz. Tzolov, Data model in the context of the general data protection regulation, *Int. J. Inform. Technol. Secur.*, **9** (2017), 113–122.
18. R. Romansky, I. Noninska, Principles of secure access and privacy in combined e-learnng environment: Architecture, formalization and modelling, in *Multidisciplinary Perspectives on Human Capital and Information Technology Professionals* (eds. V. Ahuja, S. Rathore), IGI Global Publ., USA (2018), 152–178.
19. M. Aminzade, Confidentiality, integrity and availability—finding a balanced IT framework, *Netw. Secur.*, **50** (2018), 9–11. *Ava*ilable from: https://www.sciencedirect.com/science/article/pii/S1353485818300436.
20. Thales, *2020 Data Threat Report – Global Edition. Survey and Analysis from IDC*, 2020. Available from: https://cpl.thalesgroup.com/data-threat-report.

21. *Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies*, European Data Protection Supervisor, 2018. Available from: https://edps.europa.eu/data-protection/our-ork/publications/guidelines/guidelines-use-cloud-computing-services-european_en.
22. *Maximizing the value of your data privacy investments – data privacy benchmark study*, CISCO Cybersecurity Series, 2019. Available from: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf.
23. Casey Crane, 20 surprising IoT statistics you don't already know, *Security Boulevard*, 5 Sep 2019. Available from: https://securityboulevard.com/2019/09/20-surprising-iot-statistics-you-dont-already-know/.
24. A. Azmoodeh, A. Dehghantanha. Big data and privacy: Challenges and opportunities, in *Handbook of Big Data Privacy* (ed. K-K. R. Choo, A. Dehghantanha), Springer-Cham, Switzerland, (2020), 1–6.

AIMS Press