KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 11, No. 2 (2021), p. 60 – 73

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

Selected aspects of cyber security from the point of view of recent legislation

Vybrané aspekty kybernetickej bezpečnosti z pohľadu súčasnej legislatívy

Martin CHOVANEC[1]

[1]*University of Security Management in Kosice*

The manuscript was received on 07. 10. 2021 and was accepted after revision for publication on 02. 12. 2021

Abstract:

Cyber security issues can be considered as one of the most recent issues. The truth is that in today's modern society, which is known as information and technology society, in a globalized world and an integrated Europe, information is becoming more fundamental than ever before. At the same time, information and technology progress is aimed at majority of knowledge, phenomena, facts, information in the broadest sense being expressed in virtual environment, in virtual reality. Against this background, it is necessary that not only transnational clusters and their standardization, but also individual states react to these new elements through their legislation.

Keywords: *information security, protection of information, security threats, available legislation*

Abstrakt:

Problém kybernetickej bezpečnosti možno považovať za jeden z najnovších problémov. Pravdou je, že v dnešnej modernej spoločnosti, ktorá je známa ako informačná a technologická spoločnosť, v globalizovanom svete a integrovanej Európe sa informácie stávajú zásadnejšími než kedykoľvek predtým. Súčasne informačný a technologický pokrok smeruje k tomu, aby väčšina poznatkov, javov, faktov, informácií v najširšom zmysle slova bola vyjadrená vo virtuálnom prostredí, vo virtuálnej realite. Na tomto pozadí je potrebné, aby na tieto nové prvky svojou legislatívou reagovali nielen nadnárodné klastre a ich štandardizácia, ale aj jednotlivé štáty.

Kľúčové slová: *informačná bezpečnosť, ochrana informácií, bezpečnostné hrozby, dostupná legislatíva*

Introduction

Information security, its content, goals and possibilities of its provision through the legislation of individual states, are constantly current issue. This is mainly because the information is of a non-quantifiable value, which is naturally the reason for the need for its comprehensive protection, including legal protection. Moreover, today's society can reasonably be reffered at the beginning of the 21st century as information, technological, or cybernetic society, which reflects a certain degree of development.

The information protection infringements are usually in the nature of attacks by individuals, but often also by specific groups, groupings or directly by the state. Also, for that reason, it is the essential role of the state to protect the rights and legally protected interests of individuals and groups, the existence of which is presumed by the law of its territory, through an effective and efficient system of protection of information and related data against attacks that threaten them, aim at unauthorized handling of information, to unauthorized use of information and directly to its misuse for one's own purposes. Naturally, in order to ensure the necessary level of information protection, the state should use all available means to ensure information security and at the same time to protect the national cyberspace. These areas should naturally be legislative, thus legally enshrined and envisaged in terms of their nature, possibilities and conditions of use, as well as mechanisms of control and technical support as well.

The importance of the legislative solution and the framework of information security in the conditions of the Slovak Republic can thus be perceived as very current, in some way also a new, modern topic. The aim of the presented processing is to critically evaluate the legislative framework and legislative regulation of information security in the conditions of the Slovak Republic and to propose options for making the protection of personal data of individuals more effective (natural and legal persons) in the context of information security. For these purposes, we will use mainly general-scientific methods, such as analysis and synthesis, analytical-legal, historical-legal, analytical-historical methods and part of the comparative methods.

1. Information security and its legislative framework in the Slovak Republic

Security has the nature of a multidisciplinary concept. In addition to the police (police science) and security (security sciences) divisions, it also deals with legal, sociological and philosophical divisions. It is not only a natural and priority interest of individuals, but also a very important interest of society, the state as such, and, eventually, the interest of the transnational community in general.

The term *"safety"* is derived from the Latin *securitas*, which expresses a state of general certainty, security, a state in which the protection of individuals is guaranteed, in which individuals are not exposed to danger. It is stated that it is "*the state of a social, natural, technical, technological or other system which, in specific internal and external conditions, enables to meet specified functions and their development in the interests of man and society."* [2] In addition the sense of security itself in the form of the existence of protection against danger, it is also a certain feeling in which there is

no threat, fear, and conversely, there is a certainty of safety, a certainty of the necessary protection [3].

In the available resources, we will meet with the division into *hard safety* and *soft safety*. While hard security constitutes military dimension of international security (war, armed violence between states, armed interventions of the international community, military-professional issues, arms control and disarmament issues, etc.), soft security constitutes its non-military dimension (the opposite of international security without military violence, use of military means to resolve disputes) [4].

Security threats have the character of events, phenomena or processes, which generally have a long-term effect and have the ability to negatively affect social entities, damage them, cause damage and their destabilization. On their own, states are negatively affected mainly in the economic and political levels, affecting large number of people and their fundamental values such as human life, health and property [5]. Naturally, security threats can be both external and internal in terms of the perpetrators of threat (in the case of external, this perpetrator operates outside the state, in the case of internal threats comes directly from the state environment).

The Copenhagen School distinguishes between several types of security sectors, usually the military, political, economic, social, environmental and information sector and human sector (human and information security). While *human security* aims to protect the rights of individuals, *information security* focuses mainly on the protection of personal data of individuals, society. Its importance can be seen in recent years, when the protection of personal data of individuals has come to the forefront As a consequence of informatization of society, which is directly linked to data transfer, their varied use, brokering and at the same time and at the same time the possibility of endangering the security of this data from the point of view of individuals as well as from the point of view of states as such and their components.

Information security refers to an overall term for a relatively comprehensive approach to information protection. In view of their importance, extent and nature, it is natural that necessary information and data must be protected from negative impacts, such as loss, leak, but also illegal using, handling, stealing, damaging, corruption or implementation of illegal changes. In principle, these are any illegal, unlawful or directly unauthorized interference with the integrity or confidentiality of information which may have a negative impact on the operation and functioning of the entities. According to the ISO/ EEC27001 set standards *information security* includes the protection of information against the whole spectrum of various threats, and its nature should be:

- ensuring the continuity of processes,
- minimizing of losses, minimizing of the application of threats,
- maximizing return on investments.

In today's modern information and technology society, the misuse of information and its possible leakage are very common problems that can have both external and internal perpetrators. From the point of view of this protection, aspects of computer and cyber security are important, as well as the possibilities of the handling and treatment of personal data as provided by current legislation, as well as the possibilities of handling of classified information. In terms of legislation, it is possible to mention:

a.) Act No. 68/2018 Z. z. Coll. on Cyber Security (with effect from 1 April 2018); and accordingly adjusted, the Security Strategy from 2017 and the National Cyber Security Strategy for the period 2015 – 2020,
b.) Act No. 18/2018 Coll. on Personal Data Protection with effect from 25 May 2018 (hereinafter "Act on PDP "),
c.) Act No. 214/2014 Coll. on the Protection of Classified Information and on Amendment of certain Acts (hereinafter „Act on CI "),
d.) Act No. 272/2016 Coll. on Trust Services for Electronic Transactions in the Internal Market and on Amendment and Supplementing of certain Acts with effect from 18 October 2016 (repealed Act No. 215/2002 Coll. on the Electronic Signature; hereinafter „Act on TS").

2. Legislative framework of cyber security in the Slovak Republic

In the result of the development of personal data protection, information security has come to the foreground in recent years. We have been facing the Information Space of national nature, including the international nature, is endangered and also directly undermined by individuals and groups of various natures, which leads to destabilization, paralysis of the proper running and functioning of states and their individual areas. That is also why an adequate, appropriate and effective security policy is extremely important, which finds expression at the legislative level, and thus in particular legislation.

The basic security document in the conditions of the Slovak Republic can be considered the *Security Strategy*, which was adopted in 2017 and replaced the document of the same name from 2005. This original document was valid for 12 years,

during which the nature of information threats and level of development of society in this area have changed significantly, so naturally the document has been requested to be updated for a long time. The content of the draft Strategy (2017) mentions information security, but the truth is that it is a document that has not gone through the legislative procedure in the National Council of the Slovak Republic. It is therefore only a draft act, in the content of which information security is mentioned, but only relatively marginally. For example, cyber threats are not defined in the content. In addition, until 2018, there was an absence of specific legislation that would address cyber security issues at this level, although it is desirable that the legislation go beyond the national strategy. It is thus possible to speak of the absence of the current national security strategy, as well as, the absence of the cyber security act, and this legal situation (absence of the law) lasted until 2018. By its adoption, the Slovak Republic fulfilled its obligation in relation to the EU when the Slovak Republic transposed the Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (so-called NIS Directive).

Specifically, this happened through Act No. 68/2018 Coll. on Cyber Security, which aims to support, increase the security of those networks and information systems on which the functioning of social, economic and security interests of the Slovak Republic is built.

The term of cyber security is encountered in several places in not approved yet Security Strategy *"Security is not only the domain of the physical world: information and communication technologies have enabled unprecedented civilizational progress, but have also created new vulnerabilities. Cyber-attacks have become a daily part of life, they are more complex, sophisticated and dynamic, used by state and non-state players and increasingly used in conventional and hybrid fight. The consequences of a cyber-attack can reach a level comparable to the consequences of conventional attacks and can significantly jeopardize the functioning of the state and the security of the citizen. The Slovak Republic and its NATO allies have therefore recognized cyberspace as a special operational domain in which the state operates in accordance with the principles of international law. The outer space is becoming an increasingly important part of the security environment"* (Point 28 of the 2017 Security Strategy Draft).

In terms of the goal, the Security Strategy aims to create cyber security, thus an open, protected and secure cyberspace. In addition, according to the wording of the text, the Slovak Republic should create an institutional (legal) framework for cyber security.

An important step towards the support of cyber security in the conditions of the Slovak Republic was the adoption of *Act No. 69/2018 Coll. on Cyber Security*, which entered into force on 1 April 2018. It is this legislation that is intended to create uniform legislative conditions in the conditions of the Slovak Republic to ensure the necessary protection of cyberspace from possible potential threats. As stated in Article 2 of this Act, it is a matter of creating minimum requirements for cyber security.

In its content, the act regulates Article 1:

a.) the organization, competence and responsibilities of public authorities in the area of cyber security,

b.) a national cyber security strategy,

c.) a unified cyber security information system,

d.) the organization and scope of units for handling cyber security incidents (CSIRT unit) and their accreditation,

e.) the status and obligations of the basic service provider and the digital service provider,

f.) security measures,

g.) cyber security system,

h.) control over compliance with this Act and audit.

The content gradually defines the individual security measures aimed at achieving cyber security and which are essentially in the nature of specific tasks, processes and technological security as at the level of personnel, technical, and also organizational level. In parallel to this, the Act also defines the *National Cyber Security Strategy* (this was approved by the Government of the Slovak Republic on 17 May 2015 in the form of Resolution No. 328/2015). A new institutional framework for ensuring cyber security is formulated as the goal of the concept for the period 2015-2020.

The act defines security measures, which are tasks, processes, roles and technologies in the organizational, personnel and technical areas, the aim of which is to ensure cyber security during the life cycle of networks and information systems. The Act also defines the National Cyber Security Strategy, which was approved on 17 June 2015 by the Government of the Slovak Republic, specifically by Resolution no. 328/2015. The aim of the concept of cyber security of the Slovak Republic for the years 2015-2020 is to propose a new institutional framework for the management of cyber security in the Slovak Republic. The strategy is a response to the Directive of the European Parliament and of the Council on measures to ensure a high common level of security of network and information systems in the Union and to determine national competent authority for the security of network and information systems.

According to the provision of Article 3 (g) to (i) it is possible to define as cyber security and as risks and threats. *Cyber security* is a state in which networks and information systems are capable of withstanding on a certain degree of reliability, any action that jeopardizes the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed or related services provided or accessible through those networks and information systems. The *risk* is then considered to be a certain level of cyber threat, which is characterized by a certain probability of the occurrence of an undesirable event. A *threat* is considered to be a reasonably identifiable circumstance, an event directed against networks or information systems, which is capable of adversely affecting cyber security.

2. Information security and personal data protection

With effect from 25 May 2018, the Personal Data Protection Act has become current act, which is a transposition of Regulation of the European Parliament and of the Council No. 2016/679. In its third part, is incorporated Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of crimes, or the enforcement of penalties and on the free movement of such data and repealing Council Decision 2008/977/SVV. This is an amendment that replaced the original Act No. 122/2013 Coll. on the protection of personal data and at the same time, which brought several changes in the area of personal data protection as the nature and basis of information security. The truth is that this legal statement, which reflects the content of the Regulation in our terms and conditions, creates a uniform framework for the protection of personal data everywhere, thus in all EU Member States. The original rules of personal data protection have been replaced by new rules which cover a wide range of areas in which personal data are used, captured and processed. It is true that, mainly from the point of view of the subjects obliged to protect personal data, it introduced a number of obligations in the processing and protection of personal data, which was associated mainly with administrative and organizational complexity.

In provision of Article 1 of the Act on PDP defines the subject of the legal regulation, thus that the provisions of this act regulate:

a.) protection of the rights of natural person against unlawful processing of their personal data,

b.) rights, obligations and responsibilities in the processing of personal data of natural persons,

c.) the position, competence and organization of the Office for Personal Data Protection of the Slovak Republic.

The central term of legal regulation can be considered the definition of personal data, therefore what all has such a nature. *Personal data means data relating to an identified natural person or an identifiable natural person which can be identified directly or indirectly, in particular by a generally applicable identifier, another identifier such as name, surname, identification number, location data or an online identifier, or on the basis of one or more characteristics or characters that make up its physical identity, physiological identity, genetic identity, mental identity, mental identity, economic identity, cultural identity or social identity* (Article 2 of the Act on PDP).

In addition to the positive definition of the scope of the of the Act on PDP provision of Article 3 of the Act on PDP also defines the negative scope and thus the provisions of the act do not apply to personal data processing by a natural person in his domestic or personal activities, to personal data processing by SIS or Military Intelligence or by the National Security Office for conducting security clearances for judicial competence.

The Act on PDP linked the possibilities of processing personal data to a number of principles, which are expressed in the Act on PDP and for a precisely defined purpose (Article 7) for the time that is absolutely necessary (Article 8). The processing of personal data must be lawful; thus, it must be based on one of the legal reasons (Article 13), with the conditions for granting consent to the processing are also legally regulated (Article 14). As a result of the uniform regulation of personal data protection, the conditions under which consent to the processing of personal data can be granted, have generally been tightened up and clarified. The legislator distinguishes between the processing of traditional personal data and specific categories of data (such as personal data *revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade union membership, genetic data, biometric data, health data or data concerning the sexual life or sexual orientation of a natural person*), or they reserve their processing only for certain cases (Article 16 (1) and (2) of the Act on PDP).

In the event that personal data are provided, the data operator is obliged to provide the statutory range of information to the person concerned or data subject (contact details of the data operator, responsible person, if specified, purpose of processing, data retained period, etc. pursuant to Article 19). Also, the data subject has the right to obtain a confirmation from the data operator if his personal data are processed (purpose of processing, nature, scope, etc.). For the data subject whose personal data are being processed, the possibility shall be provided for incorrect data to be corrected without delay. It even provides for the possibility to request the addition of incomplete personal data and the right to delete personal data (Article 23 of the Act on PDP).

If the conditions set out in Article 44 of the Act on PDP are met, the data operator or intermediary is obliged to appoint *a responsible person*, who may also be their employee, or may perform tasks for them on the basis of a contract. They are also

obliged to ensure that the protection of personal data (and the tasks stated in provision of Article 46 of the Act on PDP) is performed by the responsible person properly and in a timely manner.

The legislator also formulated in detail the obligation of the data operator and his representative to keep records of processing activities to precisely defined extent. Also, each of them is obliged to keep these records in electronic form.

Inter alia, there is stated requirement for the data operator and the intermediary to take such measures (organizational, technical nature) to ensure the security of the processed data with regard to their nature, scope, processing time, purpose of processing, etc. The data operator is obliged to report breaches of personal data protection within a specified period of time within 72 hours after he became aware of this breach in relation to the Office for Personal Data Protection. Pursuant to the new regulation, he is also obliged to immediately notify the data subject of this breach, if it may be associated with a high risk to the rights of a natural person (Article 41 of Act on PDP).

3. Information security and trust services

Act No. 272/2016 Coll. on Trust Services for Electronic Transactions in the Internal Market and on Amendment and Supplementing of certain Act with effect from 18 October 2016 introduces new institutes into the application practice of personal data protection. That is a legal regulation that replaced the original Act No. 215/2002 Coll. on electronic signatures, and at the same time to ensure compliance of national law in Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (the so-called e-IDAS Regulation). Its content aims to support and strengthen the expectations perception and trust in the implementation of electronic transactions in the internal market by creating a uniform basis and framework for electronic transactions between individuals, individuals and businesses, and public administrations. Also, the uniform rules for electronic transactions are established, new trusted services are defined, as well as the conditions for the recognition of means for the purpose of electronic identification of persons. The subject of the Act regulates the following areas (Article 1):

a.) conditions for granting of trust services,

b.) obligations established for providers of these services,

c.) the competence of the National Security Office in the area of providing trust services and

d.) sanctions imposed for breach of obligations under the above regulation or this Act.

4. Information security and protection of classified information

State as such should primarily be the guarantor of the protection of personal data as well as cyberspace, while for these purposes it should create both sufficient legislative (legal) instruments in the form of sufficient legislation and a sufficient

institutional framework. It is the State that has the character of the main guarantor for the protection of personal data and information that is transferred between object of cyber security [6]. On the one hand, the state creates a legal framework for the protection of personal data and for the protection of information, but on the other hand it must also create a legal framework according to which it will be able to obtain information and data in a confidential manner for specifically defined purposes. These activities are therefore carried out in a confidential manner, using specially designed techniques, and are carried out by the specific security authorities in whose responsibilities they are entrusted. These are mainly such authorities as the Slovak Information Service (SIS, under the provisions of Act No. 46/1993 Coll. on the Slovak Information Service as amended), Military Intelligence (under the provisions of Act No. 198 / 1994 Coll. on Military Intelligence as amended) or the Police Force of the Slovak Republic (under the provisions of Act No. 171/1993 Coll. on the Police Force as amended). Such activities, where the state, through its bodies or authorities, obtains information in a confidential manner for the purposes of protection of public order, security, prevention of crime, crime, etc., it is necessary to distinguish from cases where certain information is considered to be so important from the point of view of the running and functioning of the state that it grants them a higher degree of protection.

In the regard to the state, it is necessary to protect important information. This protection is implemented through the confidentiality regime of certain types of information which, in the case of loss, destruction, damage, unlawful use, disclosure or espionage, thus due to a number of risks, could lead to breach of security, stability and running of the state. The system of measures aimed at the protection of such information is regulated by Act No. 215/2014 Coll. on the Protection of Classified Information as amended. Generally, a classified information within the meaning of Article 2 of the Act on CI is considered to be *information or an object determined by the originator of a classified information, which in view of the interest of Slovak Republic must be protected from disclosure, misuse, damage, unlawful reproduction, destruction, loss or disposal (hereinafter „unlawful handling") and which may be incurred only in areas established by the Government of the Slovak Republic by its regulation*.

According to the meaning, the information is divided into 4 levels of protection (classification level "Top Secret", "Secret", "Confidential" and "Restricted"). In relation to them, requirements are set for the level of security clearance (I. and II. Level) and requirements for its fulfillment (Article 15 et seq. of the Act of CI). Two groups, or two systems of measures, are responsible for the protection of these levels of classified information. [7]:

a.) measures relating to persons working with classified information and persons themselves participating in the system of their protection (ensuring the technical, administrative, personnel aspects of measures aimed at protection; these persons are required to comply with the legal conditions depending on the level of confidentiality of the information they work with),

b.) measures of a technical nature, which may include object security, administrative security, security of technical means used for the transmission and storage of information).

The provisions of the Act of CI precisely define the conditions under which specific persons may become informed with classified information at various levels and regimes of protection, under which they may work with, reproduce, disseminate and use it. Significant are the penalties for breach of these obligations, which may consist in restricting or abolishing the ability to become informed with a particular degree of classified information, in the possibility of evaluating this procedure as an administrative offence or in the possibility of assessing the infringement as a criminal offence.

On the other hand, the provision of Article 4 of the Act on CI defines what facts can never have status of classified information, thus those that can never be subject to this regime of protection. Also, the provisions of this act do not apply to the protection of legally protected secrets which regulate certain special regulations (trade secrets under Commercial Code, tax secrets under provisions of the Tax Code, banking secrets under provisions of the Banking Act).

It is also relevant that act establishes the competence of the National Security Office (under the Act "Office"), including ensuring documents for the decision of the Judicial Council of the Slovak Republic on the fulfillment of requirements, assumptions for judicial competence as guarantees for the proper undertake of the function.

The act takes the use of a qualified electronic signature forward, as well as a qualified electronic seal, which entities are obliged to use in contact with public authorities. On the one hand, there is established a certain form of protection of personal data and verification of the specific identity of entities, on the other hand, the nature of such documents is strengthened in the eyes and system of activities of public administration bodies. The qualified electronic signature and certificate for electronic signature are issued by a qualified provider of trust services. It is a provider to whom the Office has granted qualified status. Also, a qualified electronic seal and certificate for it are issued by a qualified trust service provider who is granted qualified status. The provisions of the act regulate the position and activities, obligations and authorizations and possibilities of control of qualified providers, as well as the status and competence of the National Security Office as a regulatory body in this area.

5. Protection of personal data as a part of information security - recommendations for application practice

Despite the fact that the primary task of states as such is to create within their legislation conditions aimed at the protection of personal data as a basis for information security in society, besides the legislative framework, it is application practice which shows the quality of legislation and reflects its implementation into application practice. It can be said that in the conditions of the Slovak Republic, important European documents (directly binding regulations and directives) have been transposed, which aim to create a uniform standard in the area of personal data protection and information security in EU countries. There is thus an appropriate legislative framework and legislative basis to cover various aspects of information security, including quality options of personal data protection. A number of obligations have been put in place for controllers and processors of personal data, the possibility of using a qualified electronic signature and a qualified electronic seal, as well as the rules and concepts of cyber

security and the protection of classified information. In specific cases, however, it is also important how individuals – natural persons, legal entities as business entities approach to the protection of personal data, and how they behave responsibly in relation to their data (personal, work) and how they approach work matters and managed areas (public administration). Also, in view of this, it is possible to recommend several proposals for application practice in the area of personal data protection as a partial part of information security (based on the problems of application practice):

a.) *From the point of view of controllers and processors of personal data communication with the Office for Personal Data Protection is important* - the Office regularly issues methodological guidelines for the application of legislation in the area of personal data protection; the truth is that this methodological level has been incompatible with the new legal regulation of the Act of PDP for a relatively long time; therefore, in case of clarity and problematic application aspects, a consultation activity with the Office on accessible telephone lines can be recommended

b.) *The original legislation in the area of personal data protection has changed significantly, so the measures aimed at ensuring their protection are no longer sufficient* - it is necessary to align the original information data with the requirements of new legislation (e.g. information boards on monitoring the territory of the municipality, the responsible person, etc. have become insufficient and it is necessary to adapt them so that this information and possible usability of information is based on the legal basis; this is the case of almost all municipalities that inform about monitoring of their territory in the regime of the original law)

c.) *Verification of the functionality of the qualified electronic signature and the qualified electronic seal* by means of communication with the authorities with which the information is exchanged; in some cases, there are problems with the identification of the subject, with the correct assignment to the subject, with the non-delivery of files that are provided in this way (e.g. in relation to the Financial Administration); Naturally, it is also the protection of access data, which aims to protect qualified signatures and seals, or their use by authorized persons

d.) *A specific problem is the use of so-called car cameras*, the use of which also captures and records the personal data of road users, but paradoxically, although it is a good institute aimed at preventing crime in transport and is helpful in dealing with insurance claims, has no legal regulation in our legislation; at the level of legislation, it is necessary to recommend the formulation of appropriate legislation of the regimes for the use of these instruments

e.) *Completion of the necessary training* aimed at getting acquainted with the issue of personal data protection for the purpose of processing and adapting existing security documents to the conditions and requirements of new legislation (possibilities of using professional assistance and advice) before the real state which is result of control; this applies to all entities processing personal data of any nature; in the case of negative control findings in the area of personal data protection, the Office for Personal Data Protection has an obligation to call upon the audited entity to eliminate deficiencies in this area, so that time to align internal legislation is formed, but in such a short time it is not sometimes achieve absolute compliance and eliminate all problematic aspects; therefore, it can only be recommended that the procedures and steps towards harmonization be carried out in advance

f.) *Consistently study the conditions, scope, time and other possibilities of personal data processing in the contractual conditions*, within the framework of electronic communication, where personal data is exchanged (many shops located on the web); active interest in the nature, scope and possibilities of protection of personal data provided in electronic and physical communication (including the possibility of their further communication); in this case it is also about activities concerning both individuals and business entities (smaller or larger natural persons or legal persons)

g.) *Protection of personal and business information and data* provided by security systems (computer, camera, technical measures, etc.); protection against loss, stealing, creation of access codes and passwords in order to determine who and how had the opportunity to obtain specific data (internal legislation prohibiting the misuse of access data and passwords)

h.) In the case of natural persons, the protection of personal documents, personal data, non-disclosure to third parties, personal disposition of documents, non-communication of personal data on request to untrusted subjects, non-sending, non-disclosure of private photos, non-opening of e-mails from unknown senders.

Conclusion

Information security issues are important and current in connection with the level of development of a modern information and technology society. Modern technologies have the ability to capture, record and store personal data of specific entities or subjects, users, and so for a long time in the future. Despite the fact that we use them every day, paradoxically, we are few times aware of this aspect. It is an aspect that in today's society there is a collection of many personal data, even in situations where we expect little information, or when we would not assume it.

Legislation of information security is primarily issue of a correct and comprehensive approach by states to the protection of their interests and the interests of the individuals who represent it. Information security requirements are mainly the task of states, which should incorporate into their national legislation a number of European and international instruments to be conducive in this area, but also to formulate specific conditions and possibilities for the collection, processing and use of personal data.

In the conditions of the Slovak Republic several European instruments aimed at the protection of personal data have been incorporated into its legal system. Not only these, but also several legal regulations contained in the legal order of the Slovak Republic set a relatively high standard of personal data protection as the essence of information security in society. However, the truth is that some tools were not incorporated in time, or could have been incorporated earlier and some related issues were not quite properly resolved. An example of this is that although a new act on personal data protection entered into force on 25 May 2018, in its methodological guidelines the Office for Personal Data Protection has consistently referred for a long time to the original wording of the act and its provisions. Several aspects of monitoring public spaces have not been resolved, both in the interconnection of public and private interests, as well as, in the use of certain tools (such as car cameras). Finally, it is precisely application practice that points to the quality of legislation and

its application in practice (its challenges). In this context, in the seminar papier is outlined the legislative framework of information security in the Slovak Republic with an emphasis on personal data protection which is also evaluated, thus seminar paper fulfilled the goal stated in its introduction. At the same time, however, the seminar paper formulated several recommendations for individuals, legal and natural persons as business entities, as well as for state authorities in order to improve the protection of personal data in practice.

References:

[2] ŠIMÁK, L. a kol. *Terminologický slovník krízového riadenia*. Žilina: 2006. s. 5

[3] ŠKVRNDA, F., PAWERA, R., WEISS, P. 2008. *Medzinárodná bezpečnosť*. Bratislava: Vydavateľstvo Ekonóm, 2008, s. 18

[4] MEDELSKÝ, J. *Kybernetická bezpečnosť.* In Zborník príspevkov z medzinárodnej vedeckej konferencie „Ochrana informácií prostriedkami verejného práva". Bratislava: PEVŠ, 2018, s. 215 a nasl

[5] ŠKVRNDA, F., PAWERA, R., WEISS, P. 2008. *Medzinárodná bezpečnosť*. Bratislava: Vydavateľstvo Ekonóm, 2008. s. 29 – 30

[6] MEDELSKÝ, J. *Kybernetická bezpečnosť.* In Zborník príspevkov z medzinárodnej vedeckej konferencie „Ochrana informácií prostriedkami verejného práva". Bratislava: PEVŠ, 2018, s. 215 a nasl.

[7] POLÁK, P., BRVNIŠŤAN, M. *Ochrana utajovaných skutočností.* In Zborník príspevkov z medzinárodnej vedeckej konferencie „Ochrana informácií prostriedkami verejného práva". Bratislava: PEVŠ, 2018, s. 21 a nasl.

Books and Journals:

[1] MEDELSKÝ, J. *Kybernetická bezpečnosť.* In Zborník príspevkov z medzinárodnej vedeckej konferencie „Ochrana informácií prostriedkami verejného práva". Bratislava: PEVŠ, 2018.

[2] MEDELSKÝ, J. *Medzinárodná bezpečnosť.* Bratislava: Akadémia PZ, 2017. s. 290. ISBN 978-80-8054-730-1.

[3] POLÁK, P., BRVNIŠŤAN, M. *Ochrana utajovaných skutočností.* In Zborník príspevkov z medzinárodnej vedeckej konferencie „Ochrana informácií prostriedkami verejného práva". Bratislava: PEVŠ, 2018.

[4] ŠIMÁK, L. a kol. *Terminologický slovník krízového riadenia*. Žilina: 2006. ISBN 80-88829-75-5.

[5] ŠKVRNDA, F., PAWERA, R., WEISS, P. *Medzinárodná bezpečnosť*. Bratislava: Vydavateľstvo Ekonóm, 2008. s. 134, ISBN 978-80-225-257-524-8.

Legislation:

[6] Zákon č. 18/2018 Z. z. o ochrane osobných údajov.

[7] Dôvodová správa k zákonu č. 68/2018 Z. z. o kybernetickej bezpečnosť.

[8] Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
[9] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti.
[10] Zákon o ochrane utajovaných skutočností č. 214/2004 Z. z. a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
[11] Bezpečnostná stratégia Slovenskej republiky z roku 2005. In. http://www.vlada.gov.sk/zakladne-dokumenty-riesiace-bezpecnost-slovenskej-republiky/.
[12] Koncepcia kybernetickej bezpečnosti Slovenskej republiky 2015 – 2020. NBÚ SR. In. http://www.nbusr.sk/kyberneticka-bezpecnost/strategicke-dokumenty/index.html.

Autors:

[1]**Martin Chovanec** – External doctoral student, University of Security Management in Kosice, Kostova 1, 040 01 Kosice, Slovakia, martin.chovanec@vsbm.sk