„Krytyka Prawa", tom 16, nr 2/2024, s. 209–222, ISSN 2080-1084, e-ISSN 2450-7938, © 2024 Authors.

ADRIÁN VAŠKO[1], JAROSLAV KLÁTIK[2]

Cybercrime in Slovakia in the Context of European Union Legislation[3]

Submitted: 7.12.2023. Accepted: 16.04.2024

Abstract

A negative phenomenon in the form of cybercrime has become a society-wide problem addressed not only by national legislators, but also by the structures of the member states of the EU integration group, the member states of the international organization of European states of the Council of Europe, as well as the member states of the almost global United Nations. The authors decided work on this paper as in the event of cybercrime it is an extremely serious and actual topic both at the national and European and international level, which must be adequately addressed.

Keywords: cybercrime, internet crime, European Union, non-cash means of payment.

1 Assoc. prof. Adrián Vaško, PhD. – Matej Bel University in Banska Bystrica (Slovakia); e-mail: adrian.vasko@umb.sk; ORCID: 0000-0002-2113-7909.

2 Prof. Jaroslav Klátik, PhD – Matej Bel University in Banska Bystrica (Slovakia); e-mail: jaroslav.klatik@umb.sk; ORCID: 0000-0002-6918-1511.

3 The research in this article has not been supported financially by any institution.

 DOI: 10.7206/kp.2080-1084.686

„Krytyka Prawa", tom 16, nr 2/2024, s. 209–222, ISSN 2080-1084, e-ISSN 2450-7938, © 2024 Authors.

ADRIAN VAŠKO, JAROSLAV KLÁTIK

Cyberprzestępczość na Słowacji w kontekście prawodawstwa Unii Europejskiej[4]

Streszczenie

Negatywne zjawisko w postaci cyberprzestępczości stało się problemem ogólnospołecznym, którym zajmują się nie tylko ustawodawcy krajowi, ale także struktury państw członkowskich grupy integracyjnej UE, państwa członkowskie międzynarodowej organizacji Rady Europy, a także państwa członkowskie globalnej Organizacji Narodów Zjednoczonych. Autorzy postanowili pracować nad tym artykułem, gdyż w przypadku cyberprzestępczości jest to niezwykle poważny i aktualny temat zarówno na poziomie krajowym, jak i europejskim i międzynarodowym.

Słowa kluczowe: cyberprzestępczość, przestępczość internetowa, Unia Europejska, bezgotówkowy sposób płatności.

[4] Badania wykorzystane w artykule nie zostały sfinansowane przez żadną instytucję.

Introduction

We are at the end of the second decade of the 21st century, and strong cultural, economic, and commercial globalization, constant modernization of technologies, increasing availability and accelerating the transfer of information can be undoubtedly considered as the main denominators of the current era. Smartphones, electronic payment terminals, tablets, and personal computers (PCs) have become a regular part of our lives, we spend a lot of time browsing on social networks, and we make full use of information technology in everyday life. However, this communication, working, and payment instrument, as well as an instrument for other purposes has also become a means of harming another person or persons. Therefore, it was natural that the legislators reflected this fact by regulating serious unlawful acts by defining individual crimes. A negative phenomenon in the form of cybercrime has become a society-wide problem addressed not only by national legislators, but also by the structures of the member states of the EU integration group, the member states of the international organization of European states of the Council of Europe, as well as the member states of the almost global United Nations.

Primary Aspects of Cybercrime and Its International Dimension

The term *cybercrime* is a terminological term for a group of crimes directed against computers as well as a group of crimes committed using a PC. In general, according to the author, these crimes can be defined as crimes against the integrity, availability, or secrecy of PC systems.[5] These are also crimes in which information or telecommunications technologies are used. These are the entire spectrum of crimes in which not only PCs, the internet, but also other new technologies are used. The main synonym for computer crime is *cybercrime* derived from the English language.[6] The term *computer crime* or *cybercrime* is used to refer to three basic groups of crimes. The first group consists of crimes targeting PCs, the second group consists of crimes in which the PC is used as a means to commit such crimes, and the last third group

[5] J. Požár, *Selected Trends in Cybercrime*, Prague 2015, p. 337.

[6] P. Kováč, *Criminal Law Aspects of Cybercrime*, Bratislava 2011, p. 33.

 DOI: 10.7206/kp.2080-1084.686

consists of crimes in which the PC is used as a certain secondary or occasional means to commit crimes.[7] The embedding of the second concept from the field of cybercrime, namely the concept of internet crime, is a narrower concept to the concept of cybercrime, referring to crime where the internet connection itself can be both a tool and an objective or location for committing a crime. The cybercrime may be divided into crimes targeting PC networks or devices and crimes enabled through computer networks or devices.[8] Another primary concept that will be in the centre of our attention in our paper is the concept of information and communication technologies. Pursuant to provisions of Article 2(1) of Act No. 95/2019 Coll. on Information Technologies in Public Administration and on Amendments and Supplements to Certain Acts, the legislator understands the concept of information technology as a means or procedure the task of which is to process data or information in an electronic form. In the provision given, the legislator includes the information system itself, infrastructure, information activities as well as electronic services. The concept of information and communication technologies includes both the concept of information technologies, i.e. the hardware and software equipment of computers, phones, scanners, cameras, and other devices enabling electronic access, electronic search, insertion, organization, presentation of information and the concept of communication technologies representing a set of communication equipment the information can be transferred through and at the same time devices this information can be made available through.[9] The fourth selected primary term in the field of cybercrime in the form of an information system can be enshrined through the provision of Article 5l of the Act No. 18/2018 Coll. on the Protection of Personal Data and on Amendments to Certain Acts, according to which the information system is any organized set of personal data of a centralized or decentralized nature made available according to predetermined criteria. Another selected term in the field of cybercrime – the critical infrastructure can be defined through the provision of Article 2(a–c) of the Act No. 45/2011 Coll. on critical infrastructure, in which the legislator deals with critical infrastructure as a system divided into sectors and elements. Based on these concepts, the authors state that information security is a broader concept compared to the concept of cybersecurity, even though these concepts could be seen as synonyms. Another term from the primary concept of cybercrime is *cyberspace*. Following the substantial difference above between cybersecurity and information security, anchoring the concept of cyberspace will help to further emphasize the very terminological boundaries

7 S. Musil, *Cybercrime*, Prague 2000, p. 6.

8 P. Lošonczi, M. Mesároš, *Basis for Child Safety in the Internet Environment*, Ostrowiec 2016, p. 167.

9 Z. Horváthova, *The Use of Information and Communication Technologies in Education*, České Budějovice 2005, p. 84.

of information security which is not limited to information technologies and computer networks.[10]

Specific Features of Cybercrime and Division of Methods

Cybercrime is characterized by a high variability of the ways the relevant illegal acts can be committed.[11] Global reach from home can be considered as one of the specific features of cybercrime. From the point of view of computer crimes using an internet or any other network, the international character is also characteristic, with legal consequences in the form of challenges in the jurisdiction and in the area of cross-border cooperation.[12] Another specific feature of cybercrimes is the possibility of their decentralization, their frequent anonymity, the possibility of remote interaction, the possibility of manipulating devices and data through low costs, latency, sophistication, as well as the possibility of automating the criminal process, easy multiplication of the harmful effect of originally small dimensions, the possibility of aggregating profits through theft of insignificant decimal amounts from transactions, extensive access to information, innovation, and limited protection options.[13] Furthermore, cybercrime is characterized by the use of state-of-the-art specialized tools and computer technology. Last but not least, it is the lack of evidence, difficult quantification, and frequent exclusion or absence of witnesses. The first way how the cybercrime can be committed is through such unlawful conduct directed to the computer. The second way is an unlawful act committed using a PC and, finally, the last way is an unlawful act in which we can state that the computer was a secondary means or an occasional one.[14] An first example how a computer crime can be committed is a computer offence – an unlawful conduct by which a computer crime is directed at a PC as a subject, e.g. the offence of unauthorized access to a computer system under the provisions of Article 247 of the Criminal Code, the offence of unauthorized interference with a computer system under the provisions of Article 247a of the Criminal Code, as well as unlawful actions directed against a computer expressed also within the offence of unauthorized interference with computer data under the provisions of Article 247b as well as the offence of unauthorized interception of computer data under the provisions of Article 247c of the Criminal

10 K. Hennyeyová, G. Gerhátová, *Security Aspects of Information Processing*, Nitra 2016, p. 77.

11 J. Kolouch, *CyberCrime*, Prague 2016, p. 182.

12 J. Pande, *Introduction to Cyber Security*, Haldwani 2017, p. 10.

13 E.J. Koops, *The Internet and Its Opportunities for Cybercrime*, Nijmegen 2010.

14 M. Brvnišťan, *Cybercrime and Prevention Options*, [in:] *Current Challenges of Cybercrime Prevention*, Bratislava 2018, pp. 26–37.

 DOI: 10.7206/kp.2080-1084.686

Code. The first category of how the cybercrime can be committed is the crime of unjust enrichment under the provisions of Article 226, the essence of which also deals with enrichment to the detriment of someone else's property or another through interference with the technical or software equipment of a computer. We are aware of the fact that in terms of criminal law, the first group represents the largest group within the issue of its specific features, anchored in comparison with the other two groups through a larger number of criminal law provisions. The second group of committing unlawful acts, when the computer is a tool for committing cybercrime, may include, for instance, the offence of unauthorized production and use of a means of payment, electronic money, or other payment card pursuant to Article 219(2) of the Criminal Code.

Typology of the Perpetrator and the Victim of Cybercrime

The most common profile of cybercrime perpetrators can be described as men around 15 to 35 years of age, who have a lot of practical experience as well as professional theoretical knowledge in the field of computer technology. Another specific feature is that they frequently have no entry in the criminal records until committing the cybercrime. These people tend to be very intelligent and it is very difficult to detect their activities in some cases, as evidenced by the estimated rate of undetected cybercrime at about 90%. The perpetrator almost always commits cybercrime remotely.[15] According to the authors Hadzhidim and Payne (2019) presented in the international study "The Profile of International Cyber Offender in the U.S." based on the analysis of press releases of the United States Department of Justice, the sample consisted of 225 foreign cyber criminals who together committed 414 crimes from 2009 to 2017, the minimum age of the perpetrator was 19 and the maximum was 72, of which 94% were men and only 6% were women. The perpetrators mostly came from China – 26.7%, Romania – 11.6%, Russia – 7.1%, Estonia – 5.3%, Canada – 4%, Mexico – 4%, etc.[16] The most common types of cybercrime committed by the perpetrators included fraud, hacking, counterfeiting, identity theft, unauthorized access, and others. It is typical for victims of cybercrime that they often do not even know that they were the subject of an attack by the perpetrator. An example of such an attack includes a theft of personal data and passwords. Other characteristic features of a victim of cybercrime include frequent lack of legal awareness of the criminality of the offender's conduct, on the basis of which,

[15] M. Brvnišťan, op. cit., p. 28.

[16] L.I. Hadzhidimová, B. Payne, *The Profile of International Cyber Offender in the U.S.*, Boston 2019, pp. 45–46.

for instance, they do not pay attention to it, as mentioned above. Furthermore, public administration organizations are increasingly becoming victims of cybercrime, as information of a highly confidential nature is also accessed in their databases after extensive digitization.[17] According to Ngo and Paternoster, the low level of self-control of the victim as well as risky computer activities via the internet can be understood as some of the basic causes of susceptibility to becoming a victim of cybercrime. The authors further report that, based on a study conducted through data collected by the University of South Florida Sarasota-Manatee, people with low levels of self-control are over 180% more likely to become victims of online harassment. Subsequently, the results of the study also imply that employed persons have about 70% less chance of becoming a victim of online defamation. After all, people with risky online behaviour are 55% more likely to become a victim of personal data lure.[18]

Regulation of Cybercrime at the Level of the Council of Europe

The authors decided to address the issue of cybercrime as a European crime first at the level of the primary legislation of the Council of Europe and then cybercrime as a European crime at the level of the primary legislation of the European Union. The primary international law of the Council of Europe in the field of cybercrime is represented by the Convention on Cybercrime of the Council of Europe. Despite the fact that the Convention on Cybercrime was opened for signature in Budapest since 2001, it was approved by the Slovak Republic only in 2007, with effect for Slovakia from 1 May 2008. Due to the fact that the Convention on Cybercrime enshrines extensive legal aspects of cybercrime in the European area, the authors decided, in view of the limited space defined for this contribution, to draw attention to the issue of the General Principles of International Cooperation on Legal Aid. According to Article 25(1) of the Convention, the first general principle regarding legal aid is represented by the mere provision of mutual assistance between the parties within the purpose of an investigation or criminal proceedings related either to the issue of computer systems and data, or to the issue of the cumulation of evidence about a crime through an electronic form. The principle of the necessity to adopt a set of necessary legislative and other measures can be found in Article 25(2) of the Convention. The principle of sending a request for legal aid by

17 M. Brvnišťan, op. cit., p. 55.

18 F.T. Ngo, R. Paternoster, *Cybercrime Victimization: An Examination of Individual and Situational Level Factors*, "International Journal of Cyber Criminology" 2011, 5(1), pp. 782–783.

 DOI: 10.7206/kp.2080-1084.686

means of fast communication means is expressed in Article 25(3) of the Convention. Subsequently, within the provisions of Article 25(4) and (5) of the Convention, the parties discuss the principle of the conditions of legal assistance derived from the legal assistance contracts from the requested party, as well as the principle of making legal assistance conditional on the existence of mutual criminality fulfilled despite the fact that the law of the requested party classifies, identifies, and characterizes unlawful conduct otherwise than the requesting party. Finally, according to the provisions of Article 26(1) and (2) of the Convention, the parties discuss the principle of providing spontaneous helpful information during the investigation as well as the principle of making the use of this information conditional, for example, on maintaining the confidentiality of this information or other conditions. All obligations imposed by the Convention under criminal law are properly transposed and implemented into the national law of the Slovak Republic. The unlawful conduct in the form of falsification of computer data can be found in Article 7 of the Convention, under which the Parties should take legislative and any other measures to make the intentional and unauthorized entry, modification, deletion of computer data, or the prevention of access to computer data a criminal offence. Last but not least, the provision also states that individual parties may make the criminality of such unlawful acts subject to the condition of fraudulent and dishonest intent. The enactment of unlawful conduct in the form of intentional and unauthorized entry, modification, deletion or prevention of access to computer data can be found in the Slovak legal law incorporated within several provisions, namely in Article 247a of the Criminal Code regarding unauthorized interference with the computer system, in Article 247b of the Criminal Code regarding unauthorized interference with computer data, in Article 247c regarding the interception of computer data and in Article 259 regarding the misrepresentation of economic and commercial records. Unlawful conduct in the form of computer fraud, is expressed within the provisions of Article 8(a and b) of the European Council Convention on Cybercrime, in which the parties discuss the obligation of each party to adopt adequate legislative or other measures that would implement unlawful conduct in the form of intentional property damage to another person by inserting, altering, deleting computer data or preventing access to computer data as well as interference with the computer system itself in the national law as a criminal offence. A characteristic feature of computer fraud should be a fraudulent or dishonest intention to obtain financial benefits. The Slovak legal system does not recognize the concept of computer fraud. However, the enactment of the above-mentioned forms of unlawful cybercrime proceedings, which the Convention of the European Council on Cybercrime refers to as computer fraud, is enacted by the Slovak legislator similarly to the counterfeiting of computer data under the

provisions of Article 247a, Article 247b, Article 247c, and Article 259 of the Criminal Code. The main difference between the classification of unlawful acts under the counterfeiting of computer data pursuant to the Article 7 of the Convention above and to the identification of computer fraud pursuant to Article 8 of the Convention consists in causing material damage, while the methods of proceedings are similar, in addition to the unlawful interference with the computer system in the event of computer fraud can be found in the Slovak legal regulation of unlawful conducts in the event of computer fraud expressed by the Convention, as the qualified merits of the same paragraph provisions as in the case of unlawful acts of falsification of computer data expressed by the Convention. When the issue of Regulation of cybercrime within the European Union is discussed, it is referred the second level of its solution in the European area. From the set of a large number of institutions, organizations and agencies, the authors decided to enshrine the primary role of the European Commission, the European Council, the European Union Agency for Network and Information Security ENISA and the primary role of the European Cybercrime Centre EC3 in the first subchapter in the field of cybercrime. The answer to the question of the role of the European Commission against cybercrime is given by the authors Mogherini and Kunasek, according to whom the European Union fulfils its role in the field of cybersecurity by focusing on three basic objectives, which are the proactive promotion of important cybersecurity topics in individual European Union policies, improving capabilities and cooperation in the field of cybersecurity so as to achieve its full development evenly within each Member State, and last but not least, striving for the Union to be one of the most advanced global players in terms of technological, administrative, personnel and information readiness.[19] In addition to the above tasks, it is clear that the European Commission, as the supreme executive institution of the European Union, fulfils its role in the cybersecurity by proposing European Union legislative acts towards the European Parliament and the Council of the European Union, as well as by providing assistance to individual member states in the process of implementing relevant European legislation, as well as by managing and allocating funds, it proactively supports innovative solutions for the protection of cyberspace. Last but not least, the European Commission, with its supervisory powers, together with the European Court of Justice ensures compliance with European legislation and represents and represents views on the Union's issues outside, together with the European External Action Service.

[19] F. Mogherini, F. Kunasek, *Handbook on Cybersecurity The Common Security and Defence Policy of the European Union*, Vienna 2018, p. 74.

 DOI: 10.7206/kp.2080-1084.686

Comparison of the Slovak legislation on Cybercrimes with the Directive (EU) 2019/713 of the European Parliament and of the Council on Combating Fraud and Counterfeiting of Non-cash Means of Payment

At the beginning of this comparative subchapter, the authors state that the Slovak Criminal Code does not recognize the term non-cash means of payment. In the event of the provisions of Article 3(a and b) of the Directive on combating fraud with non-cash means of payment and counterfeiting and altering thereof, expressing the cybercrime of fraudulent use of non-cash means of payment, there is no consistent provision in the Slovak criminal law. However, the content of the facts of the fraudulent use of non-cash means of payment could be subsumed under the provision of Article 219(1, 3, and 4) of the Criminal Code including the crime of unauthorized production and use of a means of payment, electronic money or other payment card, while the Slovak criminal law deals with the criminality of the unauthorized acquisition of a means of payment, electronic money and a payment card and telephone cards for the purpose of using it as a genuine and therefore, there is no longer a need for its fraudulent use, which is included in Article 3 (a and b) of the Directive. As for the obligation to transpose the sanction for the crime of fraudulent use of non-cash means of payment in the form of at least the upper limit of the penalty of imprisonment for two years expressed in Article 9(2) of the Directive, it is similarly provided in the Slovak criminal legislation in the provision of Article 219(1) of the Criminal Code. When comparing the provisions of Articles 4 and 5 of the Directive concerning the obligation of the member states of the European Union to adopt adequate legislative measures to ensure that the set of offences related to the fraudulent use of both tangible and intangible non-cash payment instruments is implemented in national law as a criminal offence, it can be found in the Slovak criminal law, as mentioned above in Article 3, the possibility of subsuming the facts from the provisions under Article 219 of the Criminal Code. However, as in the eventuality of Article 3, there is an incomplete interpretation of non-cash payment instruments, the term of which, although not recognized by the Criminal Code, but in relation to which the Slovak legislator refers to in the above-mentioned provision of Article 219(1) as the means of payment, electronic money and payment and telephone card, or any other thing capable of performing such function. This implies that although the Slovak criminal law does not distinguish between tangible and intangible non-cash means of payment, as it does not even recognize the concept of a non-cash means of payment as such, however, it does recognize the concept of payment means under which all their divisions can be included. Therefore, theft, fraudulent counterfeiting, alteration, imitation, illegal possession, illegal appropriation, imitation, and illegal acquisition or unlawful circulation of a tangible non-cash means of payment, as well as unlawful acquisition,

fraudulent imitation, alteration and counterfeiting as well as unlawful acquisition, possession, and unlawful circulation of an intangible non-cash means of payment, can also be included under the relevant provision of Article 219 of the Criminal Code. Considering the provisions of Article 5(a)134, it is necessary to pay special attention to the reference of the European legislator to Articles 3 and 6 of the Directive on attacks against information systems. Because the provision expresses the obligation to transpose the unlawful acquisition of an intangible non-cash payment instrument into national law as a criminal offence at least in those cases in which it was necessary to simultaneously commit unlawful access to information systems, unlawful interference with the system, unlawful interference with data and unlawful interception of data, the Slovak criminal law transposed through the provisions of Article 247, Article 247a, Article 247b, and Article 247c of the Criminal Code, but it is not referred to through the provision of Article 219 of the Criminal Code, which could limit the set of crimes of unlawful acquisition of intangible non-cash payment instruments in the event of a distinction between tangible and intangible non-cash payment instruments. The issue of punishing offenders for committing crimes related to the fraudulent use of both tangible and intangible non-cash means of payment is enshrined in the provisions of Article 9(2 and 3) of the Directive, while in paragraph 2, the European legislator sets the minimum upper limit of the penalty of imprisonment for two years and in paragraph 3 for three years. Therefore, if the terminology relating to non-cash means of payment were modified in the provision of Article 219 of the Criminal Code, which can be subsumed under the current means of payment, the penalty obligation could also be considered as completely transposed.

Conclusion

The authors of the paper are aware of the fact that the issue of preventing not only cybercrime but also crime as a whole is one of the most important topics for ensuring the proper functioning of society and at the same time one of the most effective ways to reduce the incidence of crime in the long term, while the main actors of crime prevention can include not only the state but also governmental organizations, non-governmental organizations, such as civic associations and foundations, business entities in the form of companies and sole traders as well as churches and educational institutions. Prevention of cybercrime can be divided into several groups, for instance, information prevention; the second group consists of technological

 DOI: 10.7206/kp.2080-1084.686

prevention, as well as psychological and legal prevention.[20] In addition to the division of cybercrime prevention in question, it is also possible to discuss about the standard division of prevention into primary, secondary, and tertiary, which range from education, through education of vulnerable groups, to work with victims. Finally, in the event that prevention fails, repression occurs. The current cybersecurity system at the national level in Slovakia is based on 'The Concept of Cybersecurity of the Slovak Republic', the document of the Action Plan for the Implementation of the Concept of Cybersecurity of the Slovak Republic as well as the wording of Act No. 69/2018 Coll. on Cybersecurity and on changes and amendments to certain laws. Pursuant to the provisions of Article 15(2) of the Cybersecurity Act, the governmental CSIRT cybersecurity unit provides preventive services in the field of prevention of cybersecurity incidents to public administration through training, creating security awareness, further monitoring and recording of security incidents, as well as through cooperation with other CSIRTs and with the cybersecurity system and through receiving and sending early warnings. Rather than mentioning the main aspects of the *UN Manual on the Prevention and Control of Computer-related Crime*, we consider it necessary to note that the UN's intensive efforts to call on member states to deal with attacks and abuse of information technology more effectively can be traced back to 1990, four years before the UN General Assembly published the *Manual* in 1994. It is well known that the issue of the *Manual* was preceded by the adoption of Resolution 45/121 on the prevention of crime and the treatment of offenders in 1990, which we will deal with in the following subchapter.[21] The issue of the *UN Manual for the Prevention and Control of Computer-related Crime*, which we dealt with in the previous seventh subchapter, was preceded by the adoption of Resolution 45/121 on the prevention of crime and the treatment of offenders, which was adopted at the eighth UN Congress on the Prevention of Crime and the Treatment of Offenders. The Resolution also discussed the fact that crime prevention and criminal proceedings cannot be considered only in the context of the public system, social and cultural values, and social development, but also in the context of constant economic development, while it is also necessary to consider the threats of increasing crime, which undermines economic and political stability.

[20] P. Madriaza et al., *6th International Report on Crime Prevention and Community Safety: Preventing Cybercrime*. Montreal 2018, p. 42.

[21] B. Sanou, *Establishment of Harmonized Policies for the ICT Market in the ACP Countries*, Geneva 2013, p. 15.

Bibliography

Literature

Brvnišťan M., *Cybercrime and Prevention Options*, [in:] *Current Challenges of Cybercrime Prevention*, Bratislava 2018, pp. 26–37.

Hadzhidimová L.I., Payne B., *The Profile of International Cyber Offender in the U.S.*, "International Journal of Cybersecurity Intelligence & Cybercrime" 2019, 2(1), pp. 40–55.

Hennyeyová K., Gerhátová G., *Security Aspects of Information Processing*, *International Scientific Days 2016*, Nitra 2016, pp. 77–84.

Horváthová Z., *Use of Information and Communication Technologies in Education*, [in:] Jandová R. et al., *Teacher Training and Current Changes in Primary Education*, České Budějovice 2005.

Kolouch J., *CyberCrime*, Prague 2016.

Lošonczi P., Mesároš M., *Basis for Child Safety in the Internet Environment*. "Acta Scientifica Academiae Ostroviensis" 2016, 7(1), pp. 163–173.

Madriaza P., et al. *6th International Report on Crime Prevention and Community Safety: Preventing Cybercrime*, Montreal 2018.

Mogherini F., Kunasek F., *Handbook on Cybersecurity: The Common Security and Defence Policy of the European Union*, Vienna 2018.

Musil S., *Computer Crime*, Prague 2000.

Ngo F.T., Paternoster R., *Cybercrime Victimization: An Examination of Individual and Situational Level Factors*, "International Journal of Cyber Criminology" 2011, 5(1), pp. 773–793.

Pande J., *Introduction to Cyber Security*, Haldwani 2017.

Porta D.D., Keating M., *Approaches and Methodologies in the Social Sciences*, Cambridge 2008.

Požár J., *Selected Trends in Cybercrime*, "Acta Informatica Pragensia" 2015, 4(3), pp. 336–348.

Sanou B., *Establishment of Harmonized Policies for the ICT Market in the ACP Countries*, Geneva 2013.

Legal Acts

Council of Europe Convention on Cybercrime.

Cybersecurity Concept of the Slovak Republic for 2015–2020.

Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the Agency of the European Union for Cybersecurity) and on cybersecurity certification of information and communication technologies and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

 DOI: 10.7206/kp.2080-1084.686

Directive (EU) 2019/713 of the European Parliament and of the Council on combating fraud, counterfeiting and counterfeiting of non-cash means of payment.
The Act No. 45/2011 Coll. on Critical Infrastructure.
The Act No. 69/2018 Coll. on Cyber Security and on changes and amendments to certain laws.
The Act No. 95/2019 Coll. on Information Technologies in Public Administration and on changes and amendments to certain laws.
The Act No. 300/2005 Coll. Criminal Code.