Balkan Araştırma Enstitüsü Dergisi / Journal of Balkan Research Institute
Cilt/Volume 11, Sayı/Number 1, Temmuz/July 2022, ss. 269-296.

Geliş - Received: 15.02.2022 Kabul - Accepted: 15.03.2022

DOI: 10.30903/Balkan.1134224

ARAŞTIRMA MAKALESİ – RESEARCH ARTICLE

THE INFORMATION SOCIETY AND INFORMATION SECURITY IN THE REPUBLIC OF SERBIA

Vida VILIĆ[*] - Mehmet Emin ERENDOR[**]

ABSTRACT

Cybercrime or the computer-related crime is the most widespread form of transnational crime, which is in its social and economic characteristics significantly different from traditional and organized crime. Cyberspace offers countless opportunities for economic development, social interaction, and political cooperation, but also provides tools for illegal surveillance, personal data collection, influencing democratic processes, committing crimes, and exchanging numerous ways and methods of warfare. This paper provides an overview of legal documents in the Republic of Serbia related to information security, data security, and deviant behavior in cyberspace, with special emphasis on the analysis of the Strategy for Information Society Development and Information Security in the Republic of Serbia for 2021-2026. Using the criminological approach, this paper focuses on legislation concerning existing criminal offenses related to cybercrime and various forms of other criminal activities, but also on the international cooperation that Serbia achieves in the field of information and cyber security.

Keywords: Information Society, Information Security, Cyberspace, Cybercrime, International Cooperation.

[*] Ph.D., Assistant Director for Legal Affairs Clinic of Dentistry Niš, Niš, Serbia, ORCID: orcid.org/0000-0003-1413-4037, E-mail: vila979@gmail.com

[**] Assoc. Prof. Dr., International Relations Department, Kyrgyz Turkish Manas University, Manas, Kyrgyzstan, E-mail: mehmet.erendor@manas.edu.kg; International Relations Department, Adana Alparslan Türkeş Science and Technology University, Adana, ORCID: orcid.org/0000-0002-8467-0743, E-mail: merendor@atu.edu.tr

VİDA VILIĆ - MEHMET EMİN ERENDOR

SIRBİSTAN CUMHURİYETİ'NDE BİLGİ TOPLUMU VE BİLGİ GÜVENLİĞİ

ÖZ

Siber suç veya bilgisayarla ilgili suç, sosyal ve ekonomik özellikleri bakımından geleneksel ve organize suçlardan önemli ölçüde farklı olan, sınıraşan suçun en yaygın biçimidir. Siber uzay, ekonomik kalkınma, sosyal etkileşim ve siyasi işbirliği için sayısız fırsat sunar, ancak aynı zamanda yasadışı gözetim, kişisel veri toplama, demokratik süreçleri etkileme, suç işleme ve çeşitli savaş yöntemleri ve yöntemlerinin değiş tokuş edilmesi için araçlar sağlar. Bu makale, 2021-2026 için Sırbistan Cumhuriyeti'nde Bilgi Toplumu Geliştirme ve Bilgi Güvenliği Stratejisinin analizine özel vurgu yaparak, siber uzayda bilgi güvenliği, veri güvenliği ve sapkın davranışlarla ilgili Sırbistan Cumhuriyeti'ndeki yasal belgelere genel bir bakış sunmaktadır. Kriminolojik yaklaşımı kullanan bu çalışma, siber suçlar ve çeşitli diğer suç faaliyetleriyle ilgili mevcut cezai suçlarla ilgili mevzuata ve aynı zamanda Sırbistan'ın bilgi ve siber güvenlik alanında gerçekleştirdiği uluslararası işbirliğine odaklanmaktadır.

Anahtar Kelimeler: Bilgi Toplumu, Bilgi Güvenliği, Siber Uzay, Siber Suç, Uluslararası İşbirliği.

Introduction

Cyberspace offers countless opportunities for economic development, social interaction, and political cooperation, but also provides tools for illegal surveillance, personal data collection, influencing democratic processes, committing crimes, and exchanging numerous ways and methods of warfare. The events that have taken place in the last few decades have revealed how positive cyberspace is for the international community and how vulnerable it is. After the developments since the early 2000's, states and international organizations started to show more tendencies towards cyber security. The cyberattacks that took place in Estonia in 2007 have an important position that can be considered as a milestone within the framework of the international community's creation of cyber security policies and its more inclination towards this new security field.[1] States such as the United

[1] Madeline Carr, "Public-private partnerships in national cyber-security strategies", *International Affairs*, Volume 92, Number 1, 2016, p. 43-62; Andrew M. Colarik, Lech Janczewski, "Establishing Cyber Warfare Doctrine", *Journal of Strategic Security*, Volume 5,

States and the United Kingdom, as well as organizations such as the UN, NATO, and the European Union, have begun to develop new policies on cyber security.

Information security is a crucial part of cybersecurity, which refers exclusively to the processes and tools designed and deployed for data security, and protection of personal and professional information from modification, disruption, destruction, and inspection. The intention is to protect sensitive information from unauthorized activities through information security and especially from possible theft of private information, data tampering, and data deletion.

States that are members of the European Union have tried to strengthen their cyberinfrastructures within the framework of organizational legislation. The widespread use of information technology worldwide and in Serbia, in particular, is prone to further intensive development. Being a transnational problem, cybercrime or computer-related crime has its social and economic characteristics, which significantly differ from traditional and organized crime.

Although Serbia, located in the Balkan geography, is not a member of the European Union, it reviews its policies within the framework of the Union's legislation and acts as if it will be a member of the Union in the future. Bukvić and Petrović stated that the European Union accepted the Lisbon Strategy in 2000, which sets the development goals for the construction of digital society and the development of information and communication technologies infrastructure and connections, and that the Republic of Serbia also participated in these strategic goals.[2] Although the Republic of Serbia acts within the framework of European Union norms, it has also tried to develop policies within the framework of its realities. These; Strategy for Information Society Development in the Republic of Serbia until 2020, the Strategy for the Development of Broadband Networks and Services in the Republic of Serbia until 2016, the Strategy for the Development of Information Technologies from 2017 to 2020, and Information Society Development and Information Security Strategy 2021-2026.

Number 1, 2012, p. 31; Joe Burton, "NATO's cyber defence: strategic challenges and institutional adaptation", *Defence Studies*, Volume 15, Number 4, 2015, p. 297-319.

[2] Rajo Bukvić, Dragan Petrović, "Manufacturing and Information Society in Serbia: Current Status and Prospects", *11th International Conference Economics and Management-Based on New Technologies*, 20-23 June 2021, Vrnjačka Banja Serbia, p. 2.

In this study, the question of how effective the policies implemented by the Republic of Serbia within the framework of cyber security will be discussed. The importance of this paper is reflected in the explanation of the possibilities that the new legal framework provides, in the field of information security, through the analytical presentation of relevant documents. Considering that the Republic of Serbia is currently at a relatively early stage of development of its comprehensive national framework governing cybersecurity, it is necessary to point out the existing legal framework, especially through the prism of relevant legal documents and through the importance of the recently adopted Strategy for Information Society Development and Information Security in the Republic of Serbia for 2021-2026.[3]

1. Literature Review

The developments that have emerged in the digitalized world have naturally become a part of the academy and the subject of research. In particular, the approaches of states towards emerging security areas have started to form an important part of the research subjects. Today, states are more concerned with security problems arising from digital environments, because every development in digital environments affects all areas of the state level in different ways and studies on this can vary according to the area. In this context, the policies developed by the Republic of Serbia have been evaluated by different authors by considering different fields.

Bukvić and Petrović conducted a study on the economic and social measurement of the impact of information and communication technologies in the process of building an information society and how this level of development is met by the society.[4] Along with the official sources and figures used, the authors claimed that the Republic of Serbia could not build an adequate information society and the country still did not reach a satisfactory level.[5]

Čekerevac, Prigoda, Bogavac, and Čekerevac discuss the use of information and communication technology (ICT) in public administration as

[3] Bukvić, Petrović, *ibid.*, p. 2.
[4] Bukvić, Petrović, *ibid.*, p. 2.
[5] Bukvić, Petrović, *ibid.*, p. 2.

part of e-government, as well as the usage of ICT during the last three decades.[6] The authors stated that The EU has identified ICTs as a major factor in the impact on economic growth and innovation and has included the Digital Agenda for Europe among the seven leading projects of the Europe 2020 economic strategy, as well as the e-Europe project and the Lisbon Strategy. The article also discusses the growth of electronic administration through two valid strategies: the Republic of Serbia's Public Administration Reform Strategy and the Republic of Serbia's Strategy for the Development of Electronic Administration from 2015 to 2018.[7]

Vuletic, Saranovic, and Marcek discussed a study of the lack of a Computer Emergency Response Team in the Republic of Serbia in their article.[8] The article discusses the essential role of a sovereign government in the defense against cyber threats, as well as the importance of a national CERT as a key operational component of a national cyber security strategy. On behalf of one or more stakeholders, CERT typically focuses on responding to ICT-related security issues. This article focuses on the advantages of having a National CERT, which should provide incident response services to a designated constituency. The article has also highlighted the importance of CERTs in terms of protecting national critical infrastructure and implementing information security standards in government bodies.[9]

Kljajić, Pavićević, Obradović, and Obradović analyze information and communication technologies in terms of the business sector.[10] The article has highlighted the usage of cloud services for business companies in the Republic of Serbia. This article is important in terms of one of the strategic documents which discussed the Strategy for the Development of the Information Society in the Republic of Serbia through 2020. The authors argue that Serbia is in the process of developing ICT, which has harmed its

[6] Zoran Čekerevac, Ludmila Prigoda, Milanka Bogavac, Petar Čekerevac, "Digital administration in the Republic of Serbia", *Biblioteka*, p. 1, https://cekerevac.eu/biblioteka/K67.pdf, (08.03.2022).
[7] Čekerevac, Prigoda, Bogavac, Čekerevac, *ibid.*, p. 7.
[8] Dejan Vuletic, Jovanka Saranovic, Jan Marcek, "Lack of Computer Emergency Response Team in The Republic of Serbia - A Securıty Challenge", *Međunarodni Naučnı Skup International Scientific Conference*, 3-4 March 2015, Belgrade, p. 183-188.
[9] Vuletic, Saranovic, Marcek, *ibid*., p. 183-188.
[10] Marko Pavićević, Maja Obradović, Ana Obradović, "Information and Communication Technologies: Use by Companies in the Republic of Serbia", *International Scientific Conference on Information Technology and Data Related Research*, Sinteza, 2021, p. 214, https://portal.sinteza.singidunum.ac.rs/Media/files/2021/214-219.pdf, (10.03.2022).

worldwide competitiveness, particularly during pandemics produced by the COVID-19 virus, according to the global development agenda designated Serbia and Agenda2030.[11]

One of the other articles was written about critical infrastructure in the telecommunications sector in the Republic of Serbia by Gospić, Murić, and Bogojević. The authors stress the fundamentals, definitions, and standards of critical infrastructure, with a focus on the telecommunications industry, and spark a discussion on the regulatory needs of critical telecommunications network infrastructure - CTI in Serbia.[12] This article focuses on Critical Infrastructure (CI), a key infrastructure, and countries that focus on building national broadband infrastructure, stimulating demand by adopting online services and applications, and expanding connectivity to provide universal access. Describes the number of broadband policies and plans for, and this infrastructure. This paper also discusses the impact of telecommunications sector system failures and the standardization framework for critical infrastructure. The authors present the situation in this region and Serbia with respect to CTI mentioned in the general regulation on CI. In Serbia, the National Strategy for the Information Society in Serbia in 2020 deals with the protection of critical infrastructure related to information security, ICT-based attacks, and protection methods.[13]

2. Research Method

Qualitative research methods were used in this article. Data were collected and classified using document scanning methods by scanning the source and archive. During the preparation phase, primary sources on the subject were handled as a priority. In particular, the laws, statutes and regulations, and other practices adopted by the country were examined. Apart from this, secondary sources related to the country's studies in this field were scanned. For this, books, articles, theses, newspaper news, internet resources, and databases were used.

Data analysis was carried out in three stages, and in the first stage of this, a literature review and preliminary readings were made about what was

[11] Pavićević, Obradović, Obradović, *ibid.*, p. 214.
[12] Nataša Gospić, Goran Murić, Dragan Bogojevic, "Managing Critical Infrastructure for Sustainable Development in the Telecommunications Sector in the Republic of Serbia", *E-society Journal: Research and Applications*, Volume 3, Number 2, 2012, p. 51-59.
[13] Gospić, Murić, Bogojevic, *ibid.*, p. 57-58.

in the literature and the subject discussed, and an opinion was tried to be reached. Afterward, the data were reduced, summarized, and classified. In the second stage, the classified data were processed into a meaningful whole and an inference was made. Here, it has been tried to establish links between the historical processes and developments regarding the information society and information security in the country. In the last stage, the data were explained and interpreted in light of the findings obtained since the beginning of the research.

3. Cybercrime and information security in Serbian legislation

Computer (cyber, high-tech) crime is a worldwide phenomenon, which continuously monitors the development of information and communication technologies.[14] In Europe, the fight against cybercrime began during the '90s and it was primarily based on relevant international documents. Since then, many countries have changed, modernized, and coordinated their national criminal legislation, according to the documents that have been adopted at the international level.[15]

On April 7, 2005, in Helsinki, as a member of the State Union of Serbia and Montenegro (at the time), the Republic of Serbia signed and ratified the Council of Europe Convention on Cybercrime No. 185 of 2001 and the Additional Protocol to the Convention on Cybercrime concerning the criminalization of racist and xenophobic acts perpetrated through computer systems, and the National Assembly of the Republic of Serbia ratified both documents in 2009.[16] These documents represent the first international

[14] Vida Vilić, "Legal framework for fighting cybercrime and criminal activities on social networks: the example of former Yugoslavia", *Contemporary Issues in International Relations: Problems of the International Community*, (ed.) Dr. Mehmet Emin Erendor, Mehmet Fatih Oztarsu, Cambridge Scholars Publishing, Newcastle 2020, p. 90-130.
[15] Vilić, *ibid.*, p. 93.
[16] Irina Rizmal, Vladimir Radunović, Đorđe Krivokapić, "Guide through Information Security in the Republic of Serbia", *OSCE*, 2020, p. 25-26, https://www.osce.org/files/f/documents/2/7/272171.pdf, (06.02.2022). Also for more information: Službeni Glasnik RS, *Zakon o Potvrđivanju Konvencije o Visokotehnološkom Kriminalu*, 19 March 2009, http://atina.org.rs/sites/default/files/ZAKON%20o%20potvrdjivanju%20Konvencije%20o%20visokotehnoloskom%20kriminalu.pdf, (04.02.2022); Službeni Glasnik RS, *Zakon O Potvrđivanju Dodatnog Protokola Uz Konvenciju O Visokotehnološkom Kriminalu Koji Se Odnosi Na Inkriminaciju Dela Rasističke I Ksenofobične Prirode Izvršenih Preko Računarskih Sistema*, 19 March 2009, http://ravnopravnost.gov.rs/wp-

documents regulating the substantive, procedural, organizational, and international framework for criminal offenses committed via the Internet and computer networks.

The most important legal documents enacted in the Republic of Serbia by relying on the Convention provisions are the Act on the Organization and Jurisdiction of State Authorities in Combating High-tech Crime;[17] the amended Criminal Code of the Republic of Serbia;[18] the Criminal Procedure Code of the Republic of Serbia;[19] the Act on Special Measures for the Prevention of Crimes against Sexual Freedom Involving Minors;[20] the Law on informational security,[21] the Act on Seizure and Confiscation of the

content/uploads/2012/11/images_files_Dodatni%20protokol%20uz%20Konvenciju%20o%20visokotehnoloskom%20kriminalu.pdf, (04.02.2022).

[17] "On The Organisation and Competences of Government Authorities Combating Cyber Crime", *Official Gazette of the Republic of Serbia,* 2009, No 61/2005 and 104/2009; Službeni Glasnik RS, *Zakon O Organizaciji I Nadležnosti Državnih Organa Za Borbu Protiv Visokotehnološkog Kriminala*, 16 December 2009, https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2005/61/7/reg, (04.02.2022).

[18] "Criminal Code", *Republic of Serbia*, 2019, https://www.mpravde.gov.rs/files/Criminal%20%20%20Code_2019.pdf, (03.02.2022); Službeni Glasnik RS, *Zakon o izmenama dopunama Krivičnog zakonika Republike Srbije*, 2019, https://www.paragraf.rs/izmene_i_dopune/210519-zakon-o-izmenama-i-dopunama-krivicnog-zakonika.html, (03.02.2022).

[19] "Criminal Procedure Code", *Official Gazette of the Republic of Serbia*, No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021- Constitutional Court Decision, 62/2021; Službeni Glasnik RS, *Zakonik o krivičnom postupku,* 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021, 62/2021.

[20] "Act on Special Measures for Preventing the Commission of Sex Crimes against Minors", *Official Gazette of the RS*, no. 32/13; Službeni Glasnik RS, *Zakon o posebnim merama za sprečavanje vršena krivičnih dela protiv polne slobode prema maloletnim licima*, 2013, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2013/32/1/reg, (05.02.2022).

[21] "Law on Information Security", *Official Gazette of Republic of Serbia*, 2019, https://www.ratel.rs/uploads/documents/empire_plugin/Law%20on%20Information%20Securty%20%28Sl.%20glasnik%20RS%206-16%2C%2094-17%20and%2077-19%29.pdf, (05/02/2022); Službeni Glasnik RS, *Zakon o informacionoj bezbednosti Republike Srbije*, 2019, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2016/6/5/reg/20191108, (05.02.2022).

Proceeds from Crime;[22] the Secrecy of Data Act[23] and the Act on Special Authorities for Effective Protection of Intellectual Property Rights.[24]

When we talk about the legal regulation of deviant behavior and criminal acts related to cyber security, The Criminal Code of the Republic of Serbia (Serbian: Krivični zakonik Republike Srbije, 2005)[25] contains substantive provisions relating to cybercrime. The provisions related to the field of computer crime are also contained in the general part of the Criminal Code, in article 112 paragraphs 16-20 and 33-34, defining terms like computer data, computer network, computer software, computer virus, computer, and a computer system. Chapter 27 envisages several criminal offenses against the security of computer data, as well as any other criminal offenses which may be considered as computer-related crimes based on the Convention on Cybercrime and enacted positive legislation. The criminal offenses falling into the category of cybercrime, which is penalized in the Criminal Code can be classified into three groups: (1) criminal offenses related to the security of computer data as a collective object of protection; (2) criminal offenses against intellectual property, property, business, and legal transactions, in which the object or the instrument of committing these offenses are computers, computer networks, computer data, and their products in a material or electronic form, if the number of copies of copyrighted works exceeds 2,000 pieces or if the financial damage exceeds one million dinars; and, (3) criminal offenses against the human rights and civil freedoms of man and citizen, sexual freedom, public order and peace, constitutional order and security of the Republic of Serbia,[26] which undoubtedly fall into the category

[22] Službeni Glasnik RS, *Zakon o oduzimanju imovine proistekle iz krivičnog dela*, 2019, https://www.paragraf.rs/propisi/zakon_o_oduzimanju_imovine_proistekle_iz_krivicnog_dela.html, (05.02.2022).

[23] "Data Secrecy Law", *Official Gazette of the Republic of Serbia*, 2009, https://www.legislationline.org/download/id/5486/file/Serbia_Data_Secrecy_law_2009_en.pdf, (06.02.2022); Službeni Glasnik RS, *Zakon o tajnosti podataka*, 2009, https://www.paragraf.rs/propisi/zakon_o_tajnosti_podataka.html, (06.02.2022).

[24] Službeni Glasnik RS, *Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine*, 2021, https://www.paragraf.rs/propisi/zakon_o_posebnim_ovlascenjima_radi_efikasne_zastite_prava_intelektualne_svojine.html, (06.02.2022).

[25] Službeni Glasnik RS, *Krivični Zakonik*, 2019, https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html, (07.02.2022).

[26] Službeni Glasnik RS, *Krivični Zakonik*, 2019, *ibid*., Articles 298-304a.

of cybercrime due to the manner or the instruments applied in the commission of these acts.[27]

Amendments to the Criminal Code of the Republic of Serbia introduced as a new criminal offense stalking (Article 138a of Chapter XIV - Criminal offenses against the freedom and rights of man and citizen) and gender harassment (Article 182a of Chapter XVII - Criminal offenses against sexual freedom).[28]

Another important law in this area is the Law on Information Security of the Republic of Serbia,[29] which was passed in 2016 and, in addition to explaining the terminology, it also deals with the security of ICT systems of special importance. According to Article 6 of this Law, ICT systems of special importance are systems used 1) in performing tasks in government bodies, 2) for processing special types of personal data, in terms of the law that regulates the protection of personal data, 3) in performing activities of general interest and other activities (like energy, transport, health, banking, and financial markets, digital infrastructure, goods of general interest, information society services, etc.) as well as legal entities and institutions established by the Republic of Serbia, autonomous provinces or local unit self-government to perform these activities. The Law also provides measures for the protection of ICT systems of special importance (Article 7) and the manner of informing about incidents (Article 11) that may have an impact on the violation of information security (Article 11a). A special part of this Law is dedicated to the prevention and protection from security risks in ICT systems in the Republic of Serbia (Articles 14-19), protection of children using ICT (Article 19a), and crypto security and protection from compromising electromagnetic significance (Article 20- 27).

Perhaps the most significant legal advancement is the establishment of the National Center for Security Risk Prevention (CERT), a body

[27] Article 3 of the Act on the Organization and Jurisdiction of State Authorities in Combating High-tech Crime "On The Organisation and Competences of Government Authorities Combating Cyber Crime", *Official Gazette of the Republic of Serbia,* 2009, No 61/2005 and 104/2009; Službeni Glasnik RS, *Zakon O Organizaciji I Nadležnosti Državnih Organa Za Borbu Protiv Visokotehnološkog Kriminala, ibid.*

[28] "Criminal Code", *ibid.*; Službeni Glasnik RS, *Zakon o izmenama dopunama Krivičnog zakonika Republike Srbije, ibid.*

[29] "Law on Information Security", *ibid.*; Službeni Glasnik RS, *Zakon o informacionoj bezbednosti Republike Srbije, ibid.*

accountable for quickly responding to incidents as well as gathering and exchanging data on the security risks of information and communication systems. The law also establishes an Information Security Coordination Body, which is in charge of fostering collaboration and coordinated engagement in the national information security system, as well as starting and monitoring preventative and other interest measures. This Coordination Body, which is unusual in the Republic of Serbia, is the key authority evidence of the political desire to establish a public-private organization for certain aspects of data security.

Concerning the regulations governing access to information security, risk analysis is mentioned in the Decree concerning closer regulation of measures for the protection of ICT systems of special importance,[30] but this Decree does not clearly define who is responsible for conducting risk assessment and how thorough that assessment should be. Despite proposals to include comprehensive information security risk assessment and analysis as one of the priority activities in the Strategy, neither the adopted bylaws nor the adopted Strategy address this shortcoming.

4. Information security in Strategies for information society and information security development in the Republic of Serbia

According to the Republic of Serbia's Law on Information Security, information security is described as; "*a set of measures that enable data handled through information and communication systems to be protected from unauthorized access, it is inseparable from the right to protection of personal data, which represent a large part of data stored within the ICT system*".[31]

With the approval of the first Strategy for Information Society Development in the Republic of Serbia until 2020 more than a decade ago, the relevance of information society development in the Republic of Serbia

[30] "Regulation on the procedure for data submission, lists, types and importance of incidents and importance of incidents and procedures of notification on incidents in information-communication systems of special importance", *Official Gazette of the Republic of Serbia*, Number 94, November 24, 2016; Službeni Glasnik RS, *Uredba o bližem uređenju mera zaštite informacionokomunikcionih sistema od posebnog značaja*, 2016, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2016/94/2/reg, (07.02.2022).
[31] "Law on Information Security", *ibid*.; Službeni Glasnik RS, *Zakon o informacionoj bezbednosti Republike Srbije*, *ibid*.

was recognized.[32] This Strategy covered all priority areas that contribute to the development of the information society: "*electronic communications, governance, e-health and e-justice, ICT in education, science, and culture, e-commerce, ICT business sector, and information security*".[33] Information security, which is one of the topics covered in this Strategy, has become increasingly important in recent years as the use of new technologies has increased the risks that arise as a result.

Accordingly, in 2017 the Government of the Republic of Serbia adopted the Strategy of Information Security Development for the period from 2017 to 2020,[34] which defined the principles of information security, priority areas, and strategic goals related to the security of citizens, economy, and state. This document is cross-sectoral and, thus, relevant for its development are planning and strategic documents in the field of new generation networks.

The Strategy for Information Society Development and Information Security in the Republic of Serbia for 2021-2026[35] (hereafter: the Strategy) is also a cross-sectoral strategy that determines the goals and measures for the development of the information society and information security. The Strategy consists of nine areas of interest: description of the current situation, vision and desired changes, general and specific objectives, a mechanism for implementing the Strategy and method of reporting on implementation results

[32] Government of Serbia Strategies, "Information Society Development Strategy in the Republic of Serbia until year 2020", *Serbian Government General Secretariat*, http://www.gs.gov.rs/english/strategije-vs.html, (07.02.2022); Službeni glasnik RS, *Strategija razvoja informacionog društva u Republici Srbiji do 2020*, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2010/51/2/reg, (07.02.2022).

[33] "Law on Information Security", *ibid.*; Službeni Glasnik RS, *Zakon o informacionoj bezbednosti Republike Srbije*, *ibid.*

[34] "Strategy for the Development of Information Security in the Republic of Serbia for the period from 2017 to 2020", *Official Gazette of the Republic of Serbia*, Number 53/2017; Službeni glasnik RS, *Strategija razvoja informacione bezbednosti za period od 2017. do 2020*, 2017, https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2017/53/1/reg, (08.02.2022).

[35] "Information Society and Information Security Development Strategy of The Republic of Serbia for the Period 2021-2026", *Official Gazette of the Republic of Serbia no. 30/18*, 2021, https://mtt.gov.rs/extfile/sr/35314/Information%20Society%20and%20InfoSec%20Strategy%202021-202611.pdf, (08.02.2022); Službeni glasnik RS, *Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021 do 2026*, 2021, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2021/86/1/reg, (08.02.2022).

as well as a description of negotiation with stakeholders during the writing of the Strategy, assessment of financial resources and analysis of financial effects, action plan for the implementation of the Strategy in the Republic of Serbia for the period from 2021 to 2026, the final part and the Action Plan for the period from 2021 to 2023.

Within the description of the current situation in the Republic of Serbia, the Strategy referred to the previously adopted two strategies and their implementation, but also describes the use of ICT in Serbia and the acquisition of e-skills. Special attention is given to the creation of services such as e-government, e-justice, e-education, e-health, e-culture, e-business, e-commerce, e-tourism, e-construction, e-agriculture, e-mining, and e-energy. The principles of information security, in general, are also highlighted, with special emphasis on information security of the citizens, the economy, and systems of special importance.

The Strategy of Information Society Development embraced in 2010 pointed toward fostering the information society and the exploitation of the capability of data and communication technologies advancements, to expand work effectiveness, financial development, higher employment rate and to raise the personal satisfaction for all residents of the Republic of Serbia. One of the objectives was additionally to construct and support open, accessible, and high-quality Internet access and, accordingly, to foster e-business, including e-government, e-commerce, e-justice, e-health, and e-education. In the implementation of this Strategy, through the implementation of the Action Plan for the period from 2018 to 2019, some results were achieved. For instance, the Republic of Serbia adopted new laws and by-laws in the field of e-government and electronic documents, electronic identification, and trusted services to strengthen the legal infrastructure and ensure the security of information in an online environment. Additionally, the government improved the functionalities, services, and service buses of the e-government Portal and Health Information System. In addition to these new improvements, the Republic of Serbia established a system for electronic data exchange in the judiciary system, and communication between the judiciary system and other state bodies. Other important points can be mentioned as:

1. In the field of e-education, e-science, and e-culture:
- Improved ICT infrastructure in primary and secondary schools;
- Raised competencies in ICT skills for teachers and employees in public administration;

- Raised awareness of children, parents, and teachers in the field of children's safety on the Internet;
- Improved digital services in the field of culture;
- Established and improved e-education services;
- To introduce teaching computer science in primary schools.

2. In the field of e-commerce:
   - Adopted legislation in the field of e-commerce;
   - Formed and published a public list of qualified trusted services;
   - Developed a payment system for instant payment- IPS NBS system.
3. In the field of health and justice, information systems have been developed to speed up work processes and enable the exchange of data contributing the reducing the costs of bureaucracy.
4. In the field of education (ie. in primary and secondary schools), as well as in the field of science and culture, it is stated that some progress has been made, which is a prerequisite for modernizing the educational process using new technologies and in enabling the development of digital services.
5. In the field of e-commerce, normative obstacles have been removed through legislative changes, and then activities have begun on information, education, and promotion of e-commerce.
6. In the field of the information society, it is necessary to intensify further activities, especially concerning the further improvement of infrastructure, development of electronic services, and raising awareness and digital skills of citizens.

The Strategy of Information Security Development adopted in 2017 aimed at developing and improving information security in the Republic of Serbia and maintaining it at an adequate level by raising the level of security of information and communication systems, combating cybercrime, and improving the information security of national importance. With the implementation of this document, the Republic of Serbia were achieved important results, such as, in the field of information and communication systems security, the government established a system for exchanging data on incidents and responding to incidents, employed and trained staff in the field of information security, implemented a campaign to raise awareness of risks and actions in case of incidents, and annual analysis of the National CERT on threats in the cyberspace of the Republic of Serbia. Also, realized activities of the National Contact Center for Children Safety on the Internet, conducted

annual IT caravan campaigns, ICT Girls' Day, Digital Hour, etc., and The Law on Personal Data Protection was adopted in the field of safe use of new technologies.

One of the other important development was conducted training of judges and public prosecutors on handling cybercrime cases in the field of fighting-tech crime. In order to achieve this goal, the Republic of Serbia defined an information security system of national security importance and established a CERT of independent CT system operators.

The development of information security began intensively with the adoption of the Law on Information Security,[36] which primarily provided the main institutional pre-conditions for the development of this area, and then other conditions necessary to establish adequate levels of information security. One of the most important questions in the implementation of the Action Plan is certainly the establishment of a special system for exchanging data on incidents and responding to incidents, which is a mechanism for monitoring the situation in this area, but also numerous activities (seminars, conferences, training, panels) to raise awareness of the risks of the incident and deal with the incident.

Great progress has been made in the field of information security of children through the work of the National Contact Center for Children Safety on the Internet. With the implementation of activities from the Action Plan, certain actions have been taken to raise the capacity of ICT systems of special importance, but in this segment, there is a lot of space for improvement, which would include investments in infrastructure, raising staff capacity, and raising users' skills in this area. The data on the use of ICT in the Republic of Serbia, which represents the basic indicators for the development of the information society, is contained in the publication of the Republic Bureau of Statistics named "The use of ICT in Serbia, 2021".[37] The data were collected through telephone survey interviews, conducted in the period from February 15 - February 28, 2021, which included 2,800 households and 2,800 individuals between the ages of 16 and 74.

[36] "Law on Information Security", *ibid.*; Službeni Glasnik RS, *Zakon o informacionoj bezbednosti Republike Srbije*, *ibid.*

[37] Republican Bureau of Statistics, "Use of information and communication technologies in the Republic of Serbia", *Republic of Serbia*, 2021, https://publikacije.stat.gov.rs/G2021/Pdf/G202116016.pdf, (09.02.2022).

The main findings of this study indicate that 76.7% of households in the Republic of Serbia own a computer, which is an increase of 2.4% compared to 2020, and 3.6% compared to 2019. Differences can be seen in comparing the prevalence of computers in urban and other parts of Serbia: 82.4% versus 67.2%. The computer is mostly owned by households with a monthly income exceeding 600 euros (95.4%), while the share of households with an income of up to 300 euros is only 48.7%.

When it comes to the use of computers by individuals, in the Republic of Serbia there are significant differences in the prevalence of Internet connections in urban and other parts of Serbia: 85.6% compared to 74.7%. Compared to 2020, in urban parts of Serbia, a decline of 1.5% was recorded, while in other parts of Serbia the growth rate is 4.3%. There is a significant disparity in the availability of internet connections, similar to the frequency of computers in households. When we look at the structure of families by monthly income, it can be seen that those homes with a monthly income of more than 600 euros (96.6 percent) have the most Internet connections, while those with an income of fewer than 300 euros have just 58.7%.

In Serbia, 74.8% of people used a computer in the last three months, 2.1% used a computer more than three months ago, 5.5% used a computer more than a year ago, and 17.6% never used a computer. In comparison to 2020, the number of computer users climbed by 2.1%, 4.1% in 2019, and 5.2% in 2018.

The Republic Bureau of Statistics research[38] in the section entitled "Privacy and Personal Data Protection" (Module Ъ) presents data related to the information security of citizens, ie. the risks and threats to which they were exposed. The research consisted of four questions related to the 1) management of access to personal data, 2) what cookies are used for, 3) whether users have restricted cookies on the devices they use and 4) whether the software is used to limit the ability to monitor online activities. Statements on privacy policy before providing personal data are read equally by men and women, mostly in the population aged 16-24 (41.6%) and 25-34 (41.9%), as well as with the student population (59.3%). These age groups mostly restricted access to their geographical location (16-24 years - 53.9% and 25-34 years - 54.4%). Women are more restricted in accessing their profile on social networks (37.8%), as well as younger users of social networks aged 16-

[38] Republican Bureau of Statistics, *ibid.*

24 (54.9%). 38.4% of Internet users aged 25-34 refused to use their personal data for advertising purposes, compared to 8.9% of the population aged 65-74. A very small number of users of all ages (3.8-12.2%) have previously checked whether the website on which they entered their personal data is secure, while 2.4% of users aged 55-64 are at least once asked the website administrator to update or delete their information. Male users are more aware that cookies can be used to track Internet traffic (60.3%), while, on the other hand, users rarely decide to change the settings in their browser to prevent or restrict cookies on any of the devices they use (men - 74.2%, women - 84.6%). According to the same research, very few Internet users of all ages use software that limits the ability to monitor online activities (men - 87.3%, women - 94.6%).

5. Information security of children

Information security of children in the Republic of Serbia was originally regulated by the Decree on Security and Protection of Children in the Use of Information and Communication Technologies,[39] and then by amendments to the Law on Information Security.[40] These documents provide measures for the safety and protection of children on the Internet, which are implemented through the activities of the National Contact Center for the Safety of Children on the Internet.

The National Contact Center is primarily responsible for preventing cyberviolence, creating awareness and information about the benefits and risks of using the Internet, and advocating safe Internet use. Preventive measures for children's online safety and protection are implemented through the National Contact Center's education and information of children, parents, and teachers, as well as in collaboration with competent authorities and institutions, such as schools, the media, the civil and private sectors, academia, and prominent individuals in the field of contemporary creativity

[39] Government of the Republic of Serbia, "Decree on Safety and Protection of Children When Using Information and Communication Technologies", *Official Gazette RS* 2016; Službeni Glasnik RS, *Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija*, 2020, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2020/13/4/reg, (09.02.2022).

[40] "Information Security Law", *Official Gazette RS 77/2019*, 2019, https://www.dataguidance.com/news/serbia-information-security-law-published-official, (09/02/2022); Službeni Glasnik RS, *O Izmenama I Dopunama Zakona O İnformacionoj Bezbednosti*, 2019, https://www.paragraf.rs/izmene_i_dopune/311019-zakon-o-izmenama-i-dopunama-zakona-o-informacionoj-bezbednosti.html, (09.02.2022).

and the creative industry, among other subjects.

In addition to prevention, the National Contact Center is a place to report security threats on the Internet, which are then forwarded to relevant institutions depending on the type of threat: Ministry of Interior, Special Prosecutor's Office for High-Tech Crime or Ministry of Education, Science and Technological Development, as well as Centres for social work and health centers. Until December 2020, the total number of communications registered in the National Contact Center via telephone calls, e-mails, applications via the website and social networks since its establishment of the Center was 20,050 complaints.

6. International cooperation in the field of information security

Given that the aspiration and officially declared national strategic goal of the Republic of Serbia is to become a member state of the European Union, Serbia should resolve "all cyber issues" by the EU framework[41] Given that the Republic of Serbia is still at a relatively early stage in the development of its comprehensive national framework governing cyber security, it is even easier to introduce practices based on EU standards rather than going through painstaking processes of changing already established practices to align it with EU accession.

Republic of Serbia institutions actively participate in international information security activities through bilateral cooperation or cooperation within international organizations such as the United Nations, the Organization for Security and Cooperation in Europe, the International Telecommunication Union, the Global Cyber Expertise Forum, the Geneva Security Sector Management Center, and others, institutions of the Republic of Serbia play an active role in international activities in the field of information security as is stated in the strategy document.[42]

The Republic of Serbia has a full mandate in the UN Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security for the years 2016-2017. (UN GGE). The Republic of Serbia has been a member of the UN

[41] Irina Rizmal, *Vodič kroz informacionu bezbednost u Republici Srbiji 2.0*, Grid Studio, Belgrad 2018, p. 17.
[42] "Information Society and Information Security Development Strategy of the Republic of Serbia for the Period 2021-2026", *ibid.*

Open Working Group on Information Security (UN OEWG) since its foundation in 2018 and actively participates in its activities.

Serbia has been a member of the Global Cyber Expertise Forum since its inception in 2019 (GFCE). Serbia also acknowledged the significance of the French initiative "*Paris Call for Trust and Security in Cyberspace*",[43] which was supported by active involvement in Serbia's working groups.

The Republic of Serbia actively participates in the work of the Informal Working Group on Cyber Security established by OSCE Decision No. 1039,[44] determining a political and technical contact point for cooperation in the event of cross-border incidents.

The Ministry of Defense takes part in international military exercises on a regular basis in order to establish and improve information security and cyber defense. Conducting a worldwide cyberspace exercise called "Cyber Tesla" in partnership with the Republic of Serbia's governmental and corporate sectors, as well as experts in the field of information security and members of the Ohio National Guard, is an example of such cooperation.[45]

The UN Office for Project Services (UNOPS), the Ministry of Trade, Tourism, and Telecommunications of the Republic of Serbia, the Regulatory Agency for Electronic Communications and Postal Services (RATEL), and the Norwegian Ministry of Foreign Affairs, represented by the Norwegian Embassy in Belgrade, signed a Memorandum of Understanding in 2019 to cooperate in strengthening the Republic of Serbia's information security.[46] The project, which ran from 2020 to 2021, aimed to improve local

[43] For more information, "Paris Call for Trust and Security in Cyberspace", 2021, https://pariscall.international/en/, (09.02.2022).

[44] For more information, see: OSCE, "Decision no. 1039 Development of confidence - building measures to reduce the risks of conflict stemming from the use of information and communication Technologies", *Organization for Security and Co-operation in Europe Permanent Council*, 2012, https://www.osce.org/files/f/documents/e/7/90169.pdf, (10.02.2022).

[45] Ministry of Defense Republic of Serbia, "Exercise Cyber Tesla 2021 Successfully Completed", 09/12/2021, https://www.mod.gov.rs/eng/18127/uspesno-zavrsena-vezba-sajber-tesla-2021-18127, (05.02.2022); Ratel, "Exercise Cyber Tesla 2021", 10/12/2021, https://www.cert.rs/en/vest/750-Odr%C5%BEana+ve%C5%BEba+%22Cyber+Tesla+2021%22.html, (05.02.2022).

[46] Vlada Republike Srbije, "Podrška Norveške jačanju informacione bezbednosti", https://www.srbija.gov.rs/vest/431766/podrska-norveske-jacanju-informacione-bezbednosti.php, (05.02.2022).

infrastructure, promote Serbia's EU integration process, and boost Serbia's information security by providing support and easier employment for vulnerable groups and social inclusion in underdeveloped municipalities. This project supported the development of recommendations for critical information infrastructure in the Republic of Serbia, as well as the procurement and establishment of a platform for conducting information security exercises in RATEL, as well as the strategic and regulatory framework in the field of information security.

7. Objectives and desired changes achieved by the implementation of the Strategy

The Strategy has its general goal, which is achieved through three specific goals. The general goal of the Strategy is to develop an information society and electronic administration in the service of citizens and the economy and to improve the information security of citizens, public administration, and the economy. The improvement of citizens' digital knowledge and skills, the capacity of public and private sector employees to use new technologies, the improvement of digital infrastructure in educational institutions, the digitization of services and business in both the public and private sectors, and the improvement of citizens', public administration's, and the economy's information security are all special goals.

Every citizen, member of the public administration, and the economic sector now use ICT, and it has a significant impact on everyday life, as well as the economy and the entire business sector. In this regard, it is vital to adapt to the changes that ICT brings, as well as to concentrate on maximizing the benefits that it provides.

The basic changes that are to be achieved are:

1) The existence of a digitalized public administration that will efficiently and transparently provide services to citizens and the economy;

2) Higher level of digital skills for all citizens who can freely use ICT, both for everyday life and for communication with public administration;

3) Transformation of the economy, through the implementation of digitalization, to support the application of information technology to modernize business in all industries;

4) The existence of an information and security environment with a sufficient level of risk awareness but also the benefits that new

technologies provide to citizens, public administration, and the economy.[47]

Conclusion

The expansion of criminal offenses falling into the category of cybercrime has necessary imposed the need for its regulation at the international level.[48] As a transnational social phenomenon, cyber criminality affects the basic values of every society. Therefore, all countries worldwide have the interests to take part in creating global legal documents that would be binding for signatory states to adjust their criminal law and criminal procedure legislation accordingly, to criminalize types of behavior that fall into the category of cybercrime, and to provide evidence for its detection.

At the beginning of 2016, the Law on Information Security began to be applied in the Republic of Serbia. The law defined the ICT systems of special importance and stipulates that every company, whose ICT system is of special importance, belongs to one of three groups: work in public authorities, in the field of data processing which is considered to be particularly sensitive personal data or in performing activities of general interest. These legal subjects must implement all 28 protection measures recommended by this Law that provide prevention of incidents, or minimization of the damage, or else, the fines range up to 2,000,000 RSD.

By adopting the Law on Information Security with all related by-laws, as well as by taking on the National Strategy for Information Security Development and the accompanying Action Plan, the Republic of Serbia has positively gained ground towards laying out a comprehensive cyber security framework. It is presently important to audit the current standardizing system, as far as disposing of all as of now existing irregularities and inadequacies, as well as to really comprehend the advantages of full harmonization with existing standards, norms, and practices, essentially inside the European Union.

The current ambiguity of certain legal provisions in the national normative framework concerning information security can be overcome in a

[47] "Information Society and Information Security Development Strategy of the Republic of Serbia for the Period 2021-2026", *ibid.*
[48] Vilić, *op.cit.*, p. 90-130.

shorter period by adopting specific guidelines for the actors to whom these legal provisions apply. To implement the adopted amendments, and given the speed of the changes that occur daily in the field of cyber security, attention should also be on the increase of the capacity of relevant institutions, with special emphasis on monitoring the adoption of current changes at regional and global level, to update national normative and strategic frameworks.

Given the many opportunities and possibilities which are open to the Republic of Serbia regarding the establishment and strengthening of the national framework for cyber security through the use of membership and engagement in and with various regional and international regimes and organizations, as well as to their relatively low utilization, the implementation should be considered through the awareness-raising programs and campaigns, through the establishment of more efficient mechanisms for informing stakeholders about opportunities and by providing support and guidance for applying and using these opportunities for capacity building and/or establishing channels of international cooperation with colleagues around the world.[49]

Serbia recognizes the importance of digitalization and information security, and the Strategy thus covers two important areas: the information society and the information security, whose further development is a precondition for complete digitalization. Adoption and implementation of this kind of strategic document in the field of information society development and information security are important in order to continue with the further improvement of digital knowledge and skills of all citizens, raising the capacity of employees in both public and private sectors to use new technologies, and in improving digital infrastructure. In addition, it is necessary to continue and intensify activities related to the digitalization of services in both public and private sectors, and by developing the capacity of relevant institutions, raising public awareness, encouraging public-private partnerships and regional and international cooperation.

The legal framework for preserving information security in the Republic of Serbia must be completed by forming an independent government body that will deal exclusively with cyber security issues and play a key role in coordinating and formulating policies in this area.

[49] Rizmal, *op.cit.*, p. 58.

REFERENCES

"Act on Special Measures for Preventing the Commission of Sex Crimes against Minors", *Official Gazette of the RS*, no. 32/13.

ANDREW, M. Colarik, JANCZEWSKI, Lech, "Establishing Cyber Warfare Doctrine", *Journal of Strategic Security*, Vol. 5, No. 1, 2012, pp. 31-48.

BUKVIĆ, Rajo, PETROVIĆ, Dragan, "Manufacturing and Information Society in Serbia: Current Status and Prospects", *11th International Conference Economics and Management-Based on New Technologies*, 20-23 June 2021, Vrnjačka Banja (Serbia), pp. 1-10.

BURTON, Joe, "NATO's cyber defence: strategic challenges and institutional adaptation", *Defence Studies*, Volume 15, Number 4, 2015, pp. 297-319.

CARR, Madeline, "Public-private partnerships in national cyber-security strategies", *International Affairs*, Volume 92, Number 1, 2016, pp. 43-62.

ČEKEREVAC, Zoran, PRIGODA, Ludmila, BOGAVAC, Milanka, ČEKEREVAC, Petar, "Digital administration in the Republic of Serbia", *Biblioteka*, pp. 1-12, https://cekerevac.eu/biblioteka/K67.pdf, (08.03.2022).

"Criminal Code", *Republic of Serbia*, 2019, https://www.mpravde.gov.rs/files/Criminal%20%20%20Code_2019.pdf, (03.02.2022).

"Criminal Procedure Code", *Official Gazette of the Republic of Serbia*, No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021-Constitutional Court Decision, 62/2021.

"Data Secrecy Law", *Official Gazette of the Republic of Serbia*, 2009, https://www.legislationline.org/download/id/5486/file/Serbia_Data_Secrecy_law_2009_en.pdf, (06.02.2022).

GOSPIĆ, Nataša, MURIĆ, Goran, BOGOJEVIC, Dragan, "Managing Critical Infrastructure for Sustainable Development in the

Telecommunications Sector in the Republic of Serbia", *E-society Journal: Research and Applications*, Volume 3, Number 2, 2012, pp. 51-59.

GOVERNMENT OF THE REPUBLIC OF SERBIA, "Decree on Safety and Protection of Children When Using Information and Communication Technologies", *Official Gazette RS*, 2016.

GOVERNMENT OF SERBIA STRATEGIES, "Information Society Development Strategy in the Republic of Serbia until year 2020", *Serbian Government General Secretariat*, http://www.gs.gov.rs/english/strategije-vs.html, (07.02.2022).

"Information Security Law", *Official Gazette RS 77/2019*, 2019, https://www.dataguidance.com/news/serbia-information-security-law-published-official, (09.02.2022).

"Information Society and Information Security Development Strategy of the Republic of Serbia for the Period 2021-2026", *Official Gazette of the Republic of Serbia no. 30/18*, 2021, https://mtt.gov.rs/extfile/sr/35314/Information%20Society%20and%20InfoSec%20Strategy%202021-202611.pdf, (08.02.2022).

"Law on Information Security", *Official Gazette of Republic of Serbia*, 2019, https://www.ratel.rs/uploads/documents/empire_plugin/Law%20on%20Information%20Securty%20%28Sl.%20glasnik%20RS%206-16%2C%2094-17%20and%2077-19%29.pdf, (05.02.2022).

MINISTRY OF DEFENSE REPUBLIC OF SERBIA, "Exercise Cyber Tesla 2021 Successfully Completed", 09/12/2021, https://www.mod.gov.rs/eng/18127/uspesno-zavrsena-vezba-sajber-tesla-2021-18127, (05.02.2022).

"On The Organisation and Competences of Government Authorities Combating Cyber Crime", *Official Gazette of the Republic of Serbia*, 2009, No 61/2005 and 104/2009.

OSCE, "Decision no. 1039 Development of confidence – building measures to reduce the risks of conflict stemming from the use of information and communication Technologies", *Organization for Security and Co-operation*

in Europe Permanent Council, 2012, https://www.osce.org/files/f/documents/e/7/90169.pdf, (10.02.2022).

"Paris Call for Trust and Security in Cyberspace", 2021, https://pariscall.international/en/, (09.02.2022).

PAVIĆEVIĆ, Marko, OBRADOVIĆ, Maja, OBRADOVIĆ, Ana, "Information and Communication Technologies: Use by Companies in the Republic of Serbia", *International Scientific Conference on Information Technology and Data Related Research*, Sinteza, 2021, pp. 214-219, https://portal.sinteza.singidunum.ac.rs/Media/files/2021/214-219.pdf, (10.03.2022).

RATEL, "Exercise Cyber Tesla 2021", 10/12/2021, https://www.cert.rs/en/vest/750-Odr%C5%BEana+ve%C5%BEba+%22Cyber+Tesla+2021%22.html, (05.02.2022).

REPUBLICAN BUREAU OF STATISTICS, "Use of information and communication technologies in the Republic of Serbia", *Republic of Serbia*, 2021, https://publikacije.stat.gov.rs/G2021/Pdf/G202116016.pdf, (09.02.2022).

"Regulation on the procedure for data submission, lists, types and importance of incidents and importance of incidents and procedures of notification on incidents in information-communication systems of special importance", *Official Gazette of the Republic of Serbia*, Number 94, November 24, 2016.

RIZMAL, Irina, *Vodič kroz informacionu bezbednost u Republici Srbiji 2.0*, Grid studio, Belgrad 2018.

RIZMAL, Irina, RADUNOVIĆ, Vladimir, KRIVOKAPIĆ, Đorđe, "Guide through Information Security in the Republic of Serbia", *OSCE*, 2020, pp. 1-82, https://www.osce.org/files/f/documents/2/7/272171.pdf, (06.02.2022).

SLUŽBENI GLASNIK RS, *Zakon o tajnosti podataka*, 2009, https://www.paragraf.rs/propisi/zakon_o_tajnosti_podataka.html, (06.02.2022).

SLUŽBENI GLASNIK RS, *Zakon o Potvrđivanju Konvencije o Visokotehnološkom Kriminalu*, 19 March 2009, http://atina.org.rs/sites/default/files/ZAKON%20o%20potvrdjivanju%20Konvencije%20o%20visokotehnoloskom%20kriminalu.pdf, (04.02.2022).

SLUŽBENI GLASNIK RS, *Zakon O Potvrđivanju Dodatnog Protokola Uz Konvenciju O Visokotehnološkom Kriminalu Koji Se Odnosi Na Inkriminaciju Dela Rasističke I Ksenofobične Prirode Izvršenih Preko Računarskih Sistema*, 19 March 2009, http://ravnopravnost.gov.rs/wp-content/uploads/2012/11/images_files_Dodatni%20protokol%20uz%20Konvenciju%20o%20visokotehnoloskom%20kriminalu.pdf, (04.02.2022).

SLUŽBENI GLASNIK RS, *Zakon O Organizaciji I Nadležnosti Državnih Organa Za Borbu Protiv Visokotehnološkog Kriminala*, 16 December 2009, https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2005/61/7/reg, (04.02.2022).

SLUŽBENI GLASNIK RS, *Strategija razvoja informacionog društva u Republici Srbiji do 2020*, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2010/51/2/reg, (07.02.2022).

SLUŽBENI GLASNIK RS, *Zakon o posebnim merama za sprečavanje vršena krivičnih dela protiv polne slobode prema maloletnim licima*, 2013, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2013/32/1/reg, (05.02.2022).

SLUŽBENI GLASNIK RS, *Uredba o bližem uređenju mera zaštite informacionokomunikcionih sistema od posebnog značaja*, 2016, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2016/94/2/reg, (07.02.2022).

SLUŽBENI GLASNIK RS, *Strategija razvoja informacione bezbednosti za period od 2017. do 2020*, 2017, https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2017/53/1/reg, (08.02.2022).

SLUŽBENI GLASNIK RS, *Zakon o izmenama dopunama Krivičnog zakonika Republike Srbije*, 2019, https://www.paragraf.rs/izmene_i_dopune/210519-zakon-o-izmenama-i-dopunama-krivicnog-zakonika.html, (03.02.2022).

SLUŽBENI GLASNIK RS, *Zakon o informacionoj bezbednosti Republike Srbije*, 2019, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2016/6/5/reg/20191108, (05.02.2022).

SLUŽBENI GLASNIK RS, *Zakon o oduzimanju imovine proistekle iz krivičnog dela*, 2019, https://www.paragraf.rs/propisi/zakon_o_oduzimanju_imovine_proistekle_iz_krivicnog_dela.html, (05.02.2022).

SLUŽBENI GLASNIK RS, *Zakonik o krivičnom postupku,* 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021, 62/2021.

SLUŽBENI GLASNIK RS, *Krivični Zakonik*, 2019, https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html, (07.02.2022).

SLUŽBENI GLASNIK RS, *O Izmenama I Dopunama Zakona O İnformacionoj Bezbednosti*, 2019, https://www.paragraf.rs/izmene_i_dopune/311019-zakon-o-izmenama-i-dopunama-zakona-o-informacionoj-bezbednosti.html, (09.02.2022).

SLUŽBENI GLASNIK RS, *Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija*, 2020, http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2020/13/4/reg, (09.02.2022).

SLUŽBENI GLASNIK RS, *Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine*, 2021, https://www.paragraf.rs/propisi/zakon_o_posebnim_ovlascenjima_radi_efikasne_zastite_prava_intelektualne_svojine.html, (06.02.2022).

SLUŽBENI GLASNIK RS, *Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026*, 2021, http://www.pravno-informacioni-

sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2021/86/1/reg, (08.02.2022).

"Strategy for the Development of Information Security in the Republic of Serbia for the period from 2017 to 2020", *Official Gazette of the Republic of Serbia*, Number 53/2017.

VILIĆ, Vida, "Legal framework for fighting cybercrime and criminal activities on social networks: the example of former Yugoslavia", *Contemporary Issues in International Relations: Problems of the International Community*, 2020, (ed.) Mehmet Emin Erendor, Mehmet Fatih Oztarsu, Cambridge Scholars Publishing, Newcastle 2020, pp. 90-130.

VLADA REPUBLIKE SRBIJE, "Podrška Norveške jačanju informacione bezbednosti", https://www.srbija.gov.rs/vest/431766/podrska-norveske-jacanju-informacione-bezbednosti.php, (05.02.2022).

VULETIC, Dejan, SARANOVİC, Jovanka, MARCEK, Jan, "Lack of Computer Emergency Response Team in the Republic of Serbia - A Securıty Challenge", *Međunarodni Naučnı Skup International Scientific Conference*, 3-4 March 2015, Belgrade, pp. 183-188.