UDC: 343.3/.7:004.738.5(497.7)
343.3/.7:004.738.5(497.5)
343.3/.7:004.738.5(497.115)
Original scientific paper

COMBATING CYBER CRIME IN THE ERA OF ARTIFICIAL INTELLIGENCE – ANALYZING LEGAL IMPLICATIONS IN THE REPUBLIC OF ALBANIA, REPUBLIC OF KOSOVO AND THE REPUBLIC OF NORTH MACEDONIA

Entoni MISKA

Department of Legal Studies, Faculty of Law, International Balkan University
**Corresponding author e-mail: enton.miska.ibu@ibu.edu.mk*

Abstract

In the digitalization era in which we now live, individuals can easily communicate with government bodies and fulfill their needs. Unfortunately, the dynamics of digitalization have brought not only benefits but also challenges, one of which is cybercrime, defined as a criminal offense that can be committed through a computer or any other technological device. Within this dynamic, the Republic of Albania, the Republic of North Macedonia, and the Republic of Kosovo have built their protective mechanisms against any form of cyber-attack. Such a mechanism begins with the implementation of legal frameworks and strategic documents that the respective states have undertaken, and then continues with the establishment of responsible institutions for protecting citizens' personal data from any form of cybercrime involving the misuse of personal data. Moreover, the challenges faced by these three Western Balkan states concerning cybersecurity and digital capacity persist, as the risk of illegal intervention remains high due to weak digital infrastructure and inadequate protective mechanisms. In this situation, the respective states in the region are increasingly becoming easy targets for any cyber-attack, primarily originating from outside. In conclusion, what is important is that in order for these three regional states to become more resilient to such attacks, they must build bridges of cooperation and invest in strengthening the infrastructure already established.

Keywords: Western Balkans, Cybercrime, Government, Digitalization, Region

Introduction

In the world that we live in, digitalization has become a life-trend, where people now are communicating between each other electronically. This kind of communication has expanded not just between individuals, but also between individuals and the government. Through this format of communication, people are getting more and more fast services than they used to get before the digitalization became a revolution and a life-changing impact for the people. In the meantime, we can say that the digitalization is a coin with two sides. The dark side of it is the new form of criminal activities, which now are not just only being conducted physically but also electronically and this form is called cybercrime. According to Goni (2022), cybercrime is defined as any criminal activity, which takes place on or over the medium of computers, internet or other forms of technology recognized by the Information Technology Act. Cybercrime includes any illegal activity where the tool or the target or both is either computer or internet. In this situation, with the increase of the cybercrime, many criminal activities with the purpose

https://doi.org/10.62792/ut.freedom.v5.i9-10.p2893

of hacking personal data of individuals has been increased, where the center of attacks are the governmental portals.

In amidst of the digitalization dynamics, Western Balkan region is trying to adapt with the changes and develop a cyber-defense mechanism in order to prevent any form of cybercrime including outside intervention from other powers. This paper will delve into the legal, policy and institutional framework that the three countries of the Western Balkans are taking in order to prevent cybercrime and ensuring a safe cyberspace in the time of uncertain events. Firstly, the paper will explain the legal and policy framework of each country of the Western Balkans, checking the advantages and the loopholes, and secondly, it will explain the institutional framework of each country, explaining the defense mechanisms, the novelties as well as the challenges that the region is facing. Last but not the least, the paper will provide an overview of the gaps that Albania, North Macedonia and Kosovo has when it comes to the cybersecurity and digital literacy, as well as the possible solutions that would help them to become stronger and stable in the fight against cybercrime. The methodology that is used in the paper is a secondary research analysis, providing findings from the other authors, strategic frameworks, legal frameworks, and other related documents that were very important for the content of the research paper.

As for the problem statement, one of the crucial problems that is discussed in the paper is the strengthening of the digital infrastructure and the defense mechanisms in the fight against cybercrime. Research questions that are discussed are:

1. Which are the legal and policy frameworks that three of the countries of the Western Balkans are taking in the fight against cyber-crime?
2. Which are the institutional frameworks that three of the countries of the Western Balkans are using as a defense mechanism the fight against cyber-crime?
3. What are the challenges and the ways that the countries of the Western Balkans shall take in order to strengthen the cybersecurity mechanisms?

Ensuring a Safe Cyber Space in Albania, North Macedonia and Kosovo

Legal and Policy Framework on Cybersecurity

When it comes to the legal framework on cybersecurity, Albania has created an effective legislation, which was developed in line with the European Union (EU) directives and in adherence with the Council of Europe (CoE) conventions. The first legal act is the Law No.7895/1995 Criminal Code of Albania, which in general terms prescribe the criminal acts in the area of Information and Communication Technology (ICT). Such criminal acts include intrusion into the citizen's privacy, spreading of personal information and violation of private correspondence, all of which have specific measures that protects the right to private life. The next piece of legislation is the Law No.2/2017 "On Cybersecurity" that ensures security in cyberspace and furtherly applies to communication networks and information systems. The Law No.9918/2008 "On Electronic Communications" ensures two important things: the secrecy of electronic communications between the citizens and the citizens with the institutions and the protection of personal data, while the interference in communication can be allowed only when it is legally required, mostly in cases of criminal investigation (Reci and Kelmendi, 2022).

The legal framework on cybersecurity in Kosovo began to be developed during the first few years from the Declaration of Independence in February 2008. The first legal act was implemented on 10 June 2010 with the law "On the Prevention and Fight against Cybercrime", continuing with the Law "On Information Society Services", and culminating with the law "On the Protection of Personal Data" enacted on 30 January 2019. The law is focusing on several elements such as the definition of legal protection and institutions responsible for monitoring the legality of data processing, the access to public documents and sanctions that are related with the protection of personal data and privacy of individuals (Peci and Ukshini, 2022). In terms of the policy framework, the first strategy was the Electronic and Communication Sector Policy-Digital Agenda for Kosova (2013-2020), focusing on developing Information and Communication Technology (ICT), developing electronic content and services, and enabling Kosovo residents to use ICT's. The main outcome of this document was the establishment of the National Computer Emergency Response Team (CERT), responsible for prohibition of the security incidents related to electronic communications networks and services. The new Cybersecurity Strategy (2023-2027) has been drafted and approved by the government of Kosovo on September 2023.

The most important piece of legislation in terms of the protection of personal data in North Macedonia is the law "On Personal Data Protection", which was initially enacted in 2005. With the establishment of the law, the legal concept of the right to privacy was introduced for the first time and more specifically, it established the protection of personal data of citizens in the country's legal system. Fifteen years later, on February 2020, a new law "On Personal Data Protection" was adopted, complying as such with the EU General Data Protection Regulation (GDPR) (Jashari, Arsovski and Zylbeari, 2022). The policy framework started with the adoption of the National Cybersecurity Strategy and National Cybersecurity Action Plan both from 2018 until 2022. The purpose of those strategies were simply to have a safe, secure, reliable and resilient digital environment backed up with high-quality capacities.

Maintaining Cybersecurity through Institutional Framework

Currently within the government of Albania, there is no institution that possess centralized and policymaking competencies when it comes to the matters of cybersecurity. Since the topic of this paper is about cybersecurity, two important institutions are dealing more closely with such matters in Albania, especially in cases of violation of personal data. The first is the National Cyber Security Authority (NCSA), responsible for overseeing the implementation of the Law Nr.25/2024 "On Cyber Security" and Law Nr.107/2015 "On Electronic Identification and Trusted Services". Among other functions, NCSA has the main duty to co-ordinate its activities with the security and defense institutions, as well as to co-operate with Cyber Security Incident Response Teams (CSIRT) and international authorities in the field of cyber security through joint agreements and in accordance with the legislation in force. The other body is the National Agency for Information Society (AKSHI), a subordinate agency of the Prime Minister's office. This agency is responsible for the maintenance of the central infrastructure of electronic services and the provision of electronic services (Article 22, the Law Nr.43/2023 "On Electronic Governance").

The previous National Cyber Security Strategy 2016-2019 in Kosovo laid the foundations for cybersecurity governance. This is mainly because of the creation of the National Cyber Security Coordinator, as well as the National Cyber Security Council (NCSC) under the purpose of strengthening multi-stakeholder involvement and coordinating in relation to "cyberspace" security (Peci and Ukshini, 2022). The coordinator can be the Minister of Internal Affairs, or a person that is authorized by the Minister to coordinate, guide, monitor and report on the implementation of the policies, activities and actions that are related to cybersecurity. The

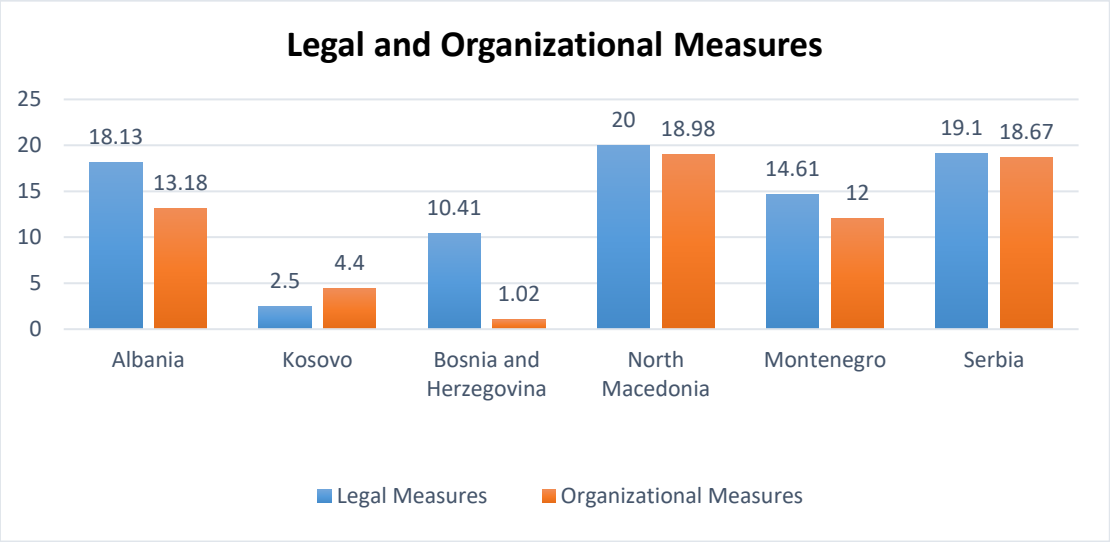
National Cyber Security Council (NCSC) is headed by the National Cyber Security Coordinator (National Cyber Security Strategy 2023-2027, 2021). Furthermore, there are other key stakeholders in Kosovo that are playing a huge role in combating cybercrime. One of those institutions is the Agency for Information Society (AIS), the competences of which are to coordinate, lead and supervise the processes and mechanisms of electronic governance in relation to ICT infrastructure, to expand the internet services in the institutions of the Republic of Kosovo and to disseminate as well as to protect the electronic and data communication infrastructure through the establishment of State Electronic Data Center (National Cyber Security Strategy 2023-2027, 2021).

In North Macedonia, there are several bodies that are serving for the protection of personal data of citizens, and one of them is called the Agency for Electronic Communications (AEC). In addition, the Law on Electronic Communications established the National Centre for Computer Incident Response (MKD-CIRT) as a separate unit of the AEC with a purpose on institutionalizing the protection of network and information security, especially for entities that have a critical infrastructure (Jashari, Arsovski and Zylbeari, 2022). In the Article 26, paragraph 2 of the Law on Electronic Communications, the annual program for the work of National Centre for Computer Incident Response is prepared by the Director of the Agency and the Minister in charge, which they submit it for adoption to the Government of the Republic of North Macedonia (Article 26, Law on Electronic Communications).

Challenges and Way Foreword

As we noticed above, the three countries of the Western Balkan region has somehow more or less prepare themselves in ensuring a safe cyberspace by adopting legal and strategic frameworks and as well establishing responsible institutions based on those legal and policy frameworks. However, the question remains: Are those countries of the Western Balkan region ready to face this new form of threat? According to Bregu (2024), the Western Balkans have seen a significant increase of 40% in cyber incidents in the past year. When it comes to the personal records, according to Bregu (2024), there are more than 1.2 million personal records that are exposed due to the data violation in the region and ransomware attacks have grown by 200% over the past two years. In terms of the preparations against such malware attacks, according to Sollaku (2023), the national frameworks about cybersecurity are either incomplete or they have a lack of enforcement. Furthermore, it is noted that the region's technical capacity is not advanced as it has to be, containing outdated systems that barely functions and non-useful equipment, creating vulnerabilities for cyber-threat, especially in the public sector (Sollaku, 2023). In the table below, we will see more clearly the tabloid of the cybersecurity in the Western Balkans made by the last Global Cyber-Security Index in 2020.

Table 1.

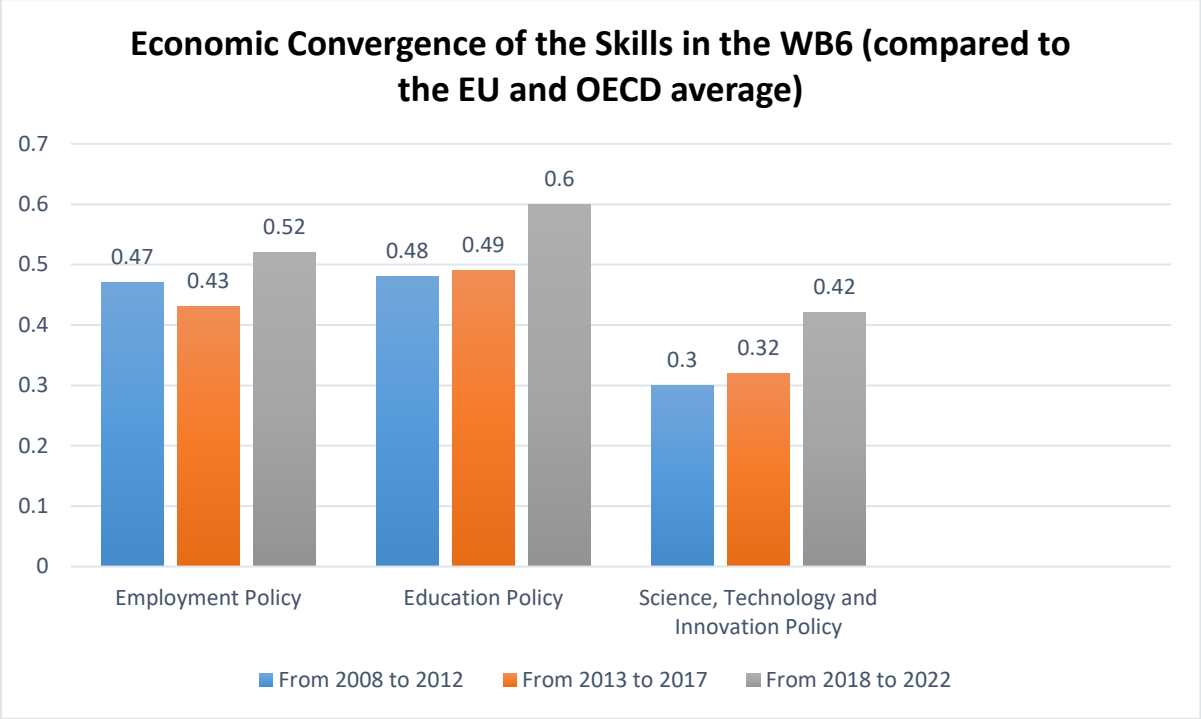


Source: Global Cyber-Security Index 2020
National Cyber-Security Index 2016-2023 (For Kosovo only)

As we see on the table above, each country has its own cybersecurity situation based on two focal elements: legal measures and organizational or institutional measures. From the legal standpoint, North Macedonia it is seemed to have a more effective legal framework according to the index with 20 points, as well as in the organizational measures standing with only 18.98 points compare to the other countries of the Western Balkans. Generally speaking, according to the index, the development of a legal and regulatory framework to protect society and promote a safe and secure digital environment is important and should be a paramount step toward the efforts in cybersecurity (Global Cyber-Security Index 2020).

When it comes to the organizational measures, in order for the institutions to function better in the fight against cyber-crime, one indicator need to be taken into consideration and that is digital skills. Within the digital skills, according to Parezanin (2023), the OECD takes a closer look at several indicators that fall within the concept of digital skills and those are: employment policy, education policy and science, technology and innovation policy. Parezanin (2023) argues that although there is a positive trend toward those three indicators, still the Western Balkan region is significantly behind EU and OECD countries, especially in the field of science, technology and innovation policy. The table below is showing more clearly the three important areas:

Table 2.



Source: OECD, 2023 (Parezanin, 2023, pg.37)

According to Parezanin (2023), the reason for the low value of this indicator, is the result of insufficient investments in research and development. In education, there are lower standards compared to the average standards of the OECD countries, bringing a lack of the concept of lifelong learning in the Western Balkans in terms of digitalization and cybersecurity. Having lower education standards, brings a lower employment policy standard, the consequences of which are low productivity of workers and their contribution as an added value. On the employment policy, Albania scores with only 0.66 points, Kosovo with 0.64 points, and North Macedonia 0.58 points. On education policy and science, technology and innovation policy the following scores were realized: Albania: 0.36 points, Kosovo: 0.26 points, and North Macedonia: 0.48 points, Serbia: (Parezanin, 2023). As we see, more or less all six countries of the Western Balkans have the same issue when it comes to employment policy, education policy and science technology and innovation policy.

For both of the elements, legal and institutional framework, regional co-operation is the key. According to Popovska (2016), the regional co-operation between countries of the Western Balkans is a necessity due to the fact that they are dealing with more or less the same situation when it comes to cyber-security. Popovska (2016) sees the institutional co-operation as a must, but on the other side, such initiations are under-construction and that happens because of the myriad of issues such as lacking of the political will, missing of the human capacities as mentioned above, as well as an overall understanding of the problem.

Therefore what Popovska (2016) proposed was a cooperation with institutions and bodies between the countries of the Western Balkans in the field of cybersecurity which is necessary. Furthermore, with the institutional co-operation it means as well some unique solutions that each country can bring, which can be shared, compared and implemented on all six countries.

The good point, as Popovska (2016) is stating, is that due to the fact that all countries are more or less in the same level it can provide joint-contribution and harmonization of the solutions preserving them for later interventions. Additionally, Popovska (2016) emphasize that the very nature of cyber domain requires cooperation, because the cyber space itself is very specific and doesn't recognize borders and nations.

Regional co-operation and EU integration will always be essential pillars of successful digital transformation both in the policy implementation and functioning of the institutions. According to the report made by the Digital WB6+ Initiative (2018), the regional cooperation can be seen very beneficial and crucial, because the coordination, harmonization and interoperability with each other and with EU firstly will reduce costs for the three countries of the Western Balkans and encourage the emergence of transnational business and government cooperation, mitigating the small economies and the work of the administrations in the region (Bieber et al., 2018). Such initiatives can be very fruitful in the times when there are a lot of attacks of cyber nature. In addition, the cooperation between the countries of the Western Balkans will not just only bring economic benefits but also better improvements because if one country will evolve, the others will follow until they reach the standards required under the auspices of EU.

Generally speaking, there have been initiatives taken as part of the regional cooperation, and here we can include several of them. The first one was the Western Balkans Digital Summit, initiated as part of the Berlin Process. This summit provided a framework for high-level regional discussion on digital transformation and coordination for EU accession of the region. Until now there is a total of four summits being held so far, where the most important topics related to the digital transition were discussed (Mrdovic, 2023). The second regional cooperation was the establishment of the Regional Cooperation Council (RCC), which plays an important role for the digital transformation in the region and most importantly for the cooperation between the Western Balkan countries, shortly abbreviated as WB6. As such, the RCC purpose is to foster the regional capacities by creating strategies on the digital skills, as well as developing a sustainable regional framework in order to support digital upskilling (Parezanin, 2023).

In the end, despite the developments taken and attempts for co-operation, the topic of cybersecurity will always remain open. Based on the geostrategic position, the region has always been influenced by major powers, and because of the poor digital infrastructure and poorly developed defence mechanisms, it always became an easy target for the "outside predators". It is important that within the regional cooperation, countries of the Western Balkans shall upgrade and strengthen its cybersecurity in order to ensure a proper functioning of the state institution mechanisms and above all protection of the personal data of every legal and natural person (Mrdovic, 2023).

Conclusions and Recommendations

On the occasion of the fight against cybercrime, all the countries of the Western Balkans have undertaken legal and policy measures, as well as established responsible institutions based on the legal and policy measures. Generally speaking, the region has taken initiatives and all the three countries have aligned their legal and strategic frameworks with the legal frameworks of EU. From the institutional perspective, the region has established its defense mechanisms that would protect the cyberspace in the region and ensure that the malware attacks to be even lower. However, from the other side, the countries of the Western Balkans have faced tremendous challenges, especially with the emphasis on Science, Technology and Innovation policy, which as it is clearly mentioned, still it is resulting on poor digital infrastructure and poorly developed defense mechanisms, leaving Albania, Kosovo and North Macedonia open for malware attacks from the outside powers. Therefore, even though the initiatives for regional co-operation have started, such co-operations need to be even more consolidated, especially in this period when cyber-attacks are more outstanding.

Recommendations are as follows:

- **Involving stakeholders in the strategic frameworks more.** This is important the countries of the Western Balkans, since involvement of the citizens, non-governmental organizations, experts on the field and many more, would contribute in establishing better policies and combating cybercrime better. A strategic framework with the contribution of the stakeholders will help on ensuring a safe cyber-space.
- **Establishing cooperation on raising the digital literacy.** The three countries of the Western Balkans shall ensure cooperation between each other in the field of education and employment. It is crucial to establish common curricula on three levels of education, as well as trying to reach the rural areas and minority groups in involving them in the process of digital literacy. Better-educated youth will contribute on better workforce, and as such ensuring free movement of the workforce, will help on strengthening the region.
- **Better cooperation on fighting cyber-crime.** Since the region is prone to cyber-threats is important for the countries of the Western Balkans to co-operate between each other. This includes inter-governmental meetings in the form of the roundtable, expert-level meetings that can be conducted annually, improvement of the current regional organizations by taking measures in the field of cybersecurity.
- **Public-Private Partnerships in developing the digital infrastructure.** With the involvement of the foreign investors in the field of digital infrastructure, it will not just improve economically but also make the digital infrastructure more safe on the fight against cyber threats.

References:

[1]. Bieber F. (2018) "*The Impact of Digital Transformation on the Western Balkan –Tackling the Challenges towardsPolitical Stability and Economic Prosperity*" Digital WB6+, Graz, Austria.
[2]. Bregu: All Inclusiveness is Paramount In Implementing Cybersecurity Measures Across the Western Balkans, Regional Cooperation Council (2024), Sarajevo, Bosnia and Herzegovina
[3]. Global Cybersecurity Index 2020, International Telecommunications Union (ITU) (2020), ITU Publications, Geneva, Switzerland
[4]. Goni.O (2022) "*Introduction to Cyber Crime*" International Journal of Engineering and Artificial Intelligence, Amman, Jordan
[5]. Jashari B., Arsovski G. and Zylbeari E (2022) "*North Macedonia, Driving Implementation to Strengthen Stakeholder Inclusion*" Geneva Centre for Security Sector Governance, Geneva, Switzerland
[6]. Ligji Nr.43/2023 "*Per Qeverisjen Elektronike*" (Eng.)The Law Nr.43/2023 "*On Electronic Governance*"
[7]. Mrdovic P. (2023) "*The role of digitalisation in transforming Western Balkan societies*" The Austrian Society for European Politics, Vienna, Austria.
[8]. National Cyber Security Authority (2024) Retrieved from https://aksk.gov.al/en/home-2/
[9]. National Cyber Security Strategy 2023-2027, The Government of Kosovo (2021), Prishtina, Kosovo
[10]. Parezanin M. (2023) "*Bridging Progress: Digital Transformation in the Western Balkans*" ASPEN Western Balkans Initiative, Berlin, Germany
[11]. Peci.L and Ukshini V. (2022) "*Kosovo, Strengthening New Foundations and Institutions*" Geneva Centre for Security Sector Governance, Geneva, Switzerland
[12]. Popovska.V (2016) "*The Urge for Comprehensive Cyber Security Strategies In the Western Balkans*" Sofia, Bulgaria

[13]. Reci M. and Kelmendi S. (2022) "*Albania, Bridging the Gap Between Cyber Policy Fragmentation and Human Rights*" Geneva Centre for Security Sector Governance, Geneva, Switzerland

[14]. Sollaku O. (2023) "*AI for Good Governance and Cybersecurity in the Western Balkans: Opportunities and Challenges*" Geneva Centre for Security Sector Governance (DCAF), Geneva, Switzerland

[15]. ЗАКОН ЗА ЕЛЕКТРОНСКИТЕ КОМУНИКАЦИИ (2005) (Eng.) Law "On Information Security" Retrieved from Zakon_za_elektronski_komunikacii_konsolidiran_032018 (mioa.gov.mk)