Criminal Justice Issues
Journal of Criminal Justice and Security
Year XV, Issue 5-6, 2014. p. 23-34
ISSN 1512-5505

ASSESSMENT OF COMPLIANCE OF THE CRIMINAL CODES IN BOSNIA AND HERZEGOVINA WITH THE COUNCIL OF EUROPE CYBERCRIME CONVENTION

Review Paper

Arben MURTEZIĆ

Abstract

Inspiration for the Paper and Issue(s) Addressed: The inspiration for this work is to evaluate directly and indirectly applicable legislation in Bosnia and Herzegovina regarding one of the most serious and the fastest growing threats in the modern world.

Aims of the Paper (scientific and/or social): The aim of the Paper is to provide analysis of compliance with the Convention.

Methodology/Design: This research is descriptive and partly comparative. Basic information about the Convention are provided prior to undertaking a detailed analysis of relevant legislation in Bosnia and Herzegovina.

Research Limitations/Paper: There are no particular limitations.

Results/Findings: The influence of the CoE Cyber Convention and considerable efforts to follow its standards are obvious. However, discrepancies and gaps are identified as well as differences between the laws in two entities.

General Conclusion: A specific problem of Bosnia and Herzegovina is the fact that there are various superfluous legislative inconsistencies in the different parts of the country due to its complex constitutional structure.

Research/Paper Justification: This assessment might be of particular importance since the Council of Europe, surprisingly, has made very limited efforts to critically evaluate legislation of the parties to the Convention, especially of the substantive criminal law provisions.

Keywords

Convention on Cybercrime, Substantive Law, Computer Crime, Criminal Code

INTRODUCTION

A country in transition with a sudden explosion in the use of information technology and tight constraints on the funding of law enforcement is rife for the modern day threat of cybercrime which can have a debilitating effect on a country's ability to attract investment. Bosnia and Herzegovina surely can not be an exemption. Moreover, the burden of recent history, complex legal system and struggling economy make the framework conditions for the fight against sophisticated forms of crime rather cumbersome. On the other hand, such circumstances are also making the need to establish the rule of law even greater.

Also, in the international context, the position of BiH, a member state of the Council of Europe (CoE) and striving to become an EU member state, is a sensitive one. The overall situation concerning organized crime is of utmost importance for achieving this goal. Also, Bosnia and Herzegovina is under scrutiny regarding the compliance of its domestic legislation with relevant international documents. The Council of Europe Cybercrime Convention is surely among those.

This paper might be of particular importance since the Council of Europe, surprisingly, has made very limited efforts to critically evaluate legislation of the parties to the Convention, especially of the substantive criminal law provisions. Namely, the "*Cybercrime legislation - Country Profiles*", provided within the framework of the Council of Europe's capacity building projects on Cybercrime (CoE, 2012), contains just plain extracts from the national laws, supposedly corresponding to relevant provisions of the Convention. This is presented in tabular format, without a visible effort to assess given provisions, neither comparatively or in the national legal context. Since in the theory of legal interpretation it is notorious that words have different meanings even in dictionaries, not to mention different legal systems (Holmes, 1899), information provided by the CoE is rather ineffectual. Additionally, the complex constitutional and legal system of Bosnia and Herzegovina requires an even more thorough approach.

COUNCIL OF EUROPE CYBERCRIME CONVENTION

After four years and twenty-seven drafts, the forty-one nation Council of Europe (CoE) aided by the United States, Canada, Japan and South Africa, as newly joined observers of the Council of Europe, drafted the Cybercrime Convention, (Piazza 2001, Keyser 2003). It was adopted by the Committee of Ministers on 8 November 2001, opened for signature in Budapest, on 23 November 2001 and entered into force in July 2004.

Its main aim, as set forth in the *Explanatory Note* is:

"1) harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation".

Accordingly, the Convention is broken up into four chapters: (I) Use of terms; (II) Measures to be taken at domestic level – substantive law and procedural law; (III) International co-operation; (IV) Final clauses.

The first chapter defines just four terms vital to the treaty i.e. computer system; computer data; service provider and traffic data. It seems that with such an unusually limited number

of definitions, the authors of the Convention wanted to avoid controversies and discussion in the areas which had been characterized by debates on terminology. Namely, the area of Information and Communications Technology and subsequently, the topic of cybercrime, contains a number of specific terms central to understanding the main issues. Nevertheless, while the first three definitions (computer system; computer data; service provider) did not give rise to any dilemmas, the term "traffic data" created some controversy. To be precise, the term "traffic data" is defined as any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service" [Article 1 (d)]. This means that "Traffic data" lasts for only a short period of time and thus Article 16 of the Convention makes the Internet Service Providers responsible for the preservation of such data, which significantly increases the costs. Interestingly, despite numerous written analyses and overviews of the Convention, there has been certain oversight in that some of its procedural provisions are not limited to cybercrimes: rather they extend to any crimes for which evidence must be collected "in electronic form." Therefore, the title: "Convention on Cybercrime" is a "misnomer or is at least a misleadingly narrow description of the Convention's substance" (Vatis, 2010, p. 208).

Section 1 of Chapter II (substantive law issues) firstly defines 9 offences grouped in 4 different categories:

1. Offences against the confidentiality, integrity and availability of computer data and systems. This group includes the following offences: Illegal access (Art 2), Illegal interception (Art. 3), Data interference (Art. 4), System interference (Art. 5), Misuse of devices (Art 6).
2. Computer-related offences. This group includes Computer-related forgery (Art. 7) and Computer-related fraud (Art. 8).
3. Content-related offences. This group includes offences related to child pornography (Art. 9).
4. Copyright-related offences. This group includes Offences related to infringements of copyright and related rights (Art. 10).

This typology is not entirely consistent, as it is not based on a sole criterion to differentiate between categories. Therefore, three categories (1, 2 and 3) focus on the object of legal protection whereas the fourth category titled "computer-related offences" does not focus on the object of legal protection rather it looks at the method used to commit the crime. This inconsistency leads to a certain overlap between categories. As a consequence, some criminal acts mentioned in the Convention, such as "cyberterrorism" (2.9.1.) or "phishing" (2.9.3) fall within several categories (Gercke, 2011, p. 30).

However, the following examples of the significant contemporary forms and types of crimes might contribute to better understanding of this categorization.

For the first category, absolutely the most important is the notorious "ransomware". This word is even added to The Oxford Dictionary and defined as: "A type of malicious software designed to block access to a computer system until a sum of money is paid". Surely, this definition is too general and describes different kinds of extortion, including the situations when the illegal or compromising materials are installed in the computer belonging to the victim and ransom is

demanded for not reporting to the officials or public (Jouhal, 2017). Still, the modern meaning of this term denotes "more subtle kind of malware, originally called cryptovirus…where the malware typically encrypts and then deletes your original data files, and asks for a ransom to hand them back to you" (Hernandez-Castro, Cartwright & Stepanova, 2017, p 1). Ransom is asked in bitcoins, and "success" of this type of the crime is perhaps the best illustrated by the fact that large businesses in the west are buying and holding significant amounts of the bitcoins in case they need to pay a ransom (Parker, 2016).

Regarding the second category, the forgery by computer is perhaps the oldest and the most known type of crime that is mentioned in the Convention. However, with new generations of computers and increased reliance on the internet systems it appears in different and more dangerous forms. This includes the creation of the phantom users with unauthorized bank accounts and direct involvement in the computer operations to change the normal process for illegal profit. Closely connected is the computer fraud, the term that describes both identity theft and financial fraud. Surely, the most frequent form, that is sometimes taken as synonymous for the computer fraud is the credit card fraud (Arief, Adzmi & Gross, 2015).

Regarding the third category, i.e. the content related offences, the Convention limits it on raising problem of child pornography, which is today dominantly spread through internet (IWF, 2017). This complex problem is outlined below in the following sub-chapter. However, it has to be mentioned that this is the category which obviously should be amended and expanded, at least to the content that supports illegal, mostly violent behavior. The latest phenomena, the "Blue Whale" game is the most obvious example, of the danger that can be caused through this type of content.

Digital piracy presents the threat that is often neglected in developing countries, but has huge overall importance since it is estimated that creative industries generate $ 2,250 billion and nearly 30 million jobs globally and surely represents important part of the international economy (Fact, 2017). Protection of these businesses and people working for them is surely equally important as the protection of everyone. However, it is reported that top pirate sites earned $ 227 million through the advertising, i.e. nearly 10% of the of the complete profit of the creative industry (Digital Citizens Alliance, 2014).

The rest of the Section on substantive law issues deals with ancillary liability and sanctions. In this part the Convention follows the trend of many legal systems which limit the offences for which their attempt is punished. Namely, the Convention prescribes criminalization of any attempts of the following: illegal interception, data interference, system interference, computer-related forgery and computer-related fraud. Regarding child pornography, any attempts at producing child pornography for the purpose of its distribution through a computer system are punishable.

The ever-present issue of jurisdiction is solved in the Convention by using traditional principles, meaning that criteria for jurisdiction are based on the principle of territoriality (Article 22). Arguably, this option as chosen by the CoE Convention is not adequate in the fight against cybercrime since the cross-border character of cybercrime makes it easy for criminals to move their activities from one state to another at short notice and so it is very difficult to determinate the *locus committi delicti* (Foggetti, 2008, p. 35). To counter this, the Article under subsection d) establishes the application of the alternative principle of criminal citizenship, typical for many States that apply the traditions of civil law. This means that a Member State can establish

jurisdiction if the offence is committed by one of its nationals and if the offence is punishable under the criminal law of the location where it was committed.

In Section 3 (International Cooperation), the Convention contains a series of provisions relating to the mutual legal assistance that Member States must afford each other. The principle that co-operation is to be provided "to the widest extent possible" is dominant and emphasized (Article 23 and Article 25).

The Additional Protocol to the Convention, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems was adopted on November 7, 2002.

APPLICABLE LEGISLATION IN BOSNIA AND HERZEGOVINA: COMPLIANCE WITH THE COE CONVENTION

Bosnia and Herzegovina signed the Convention on 9/2/2005, ratified it on 19/5/2006, and it entered into force on 1/9/2006.

The assessment in this chapter will be more detailed regarding the substantive criminal law section, since some of the provisions from the procedural law section are assessed in a separate Cybercrime Convention Committee Report (T-CY, 2012, 10 REV) which will be presented briefly. Also, the provisions on international co-operation are rather self-explanatory and universal, and as such, probably do not require a comprehensive evaluation.

Brief background information on the legislative framework of Bosnia and Herzegovina

Bosnia and Herzegovina (BiH) is composed of the Federation of Bosnia and Herzegovina (FBiH) and Republika Srpska (RS), which are self-governing entities each with its own Criminal Code (hereinafter the "CC") and the Criminal Procedural Code (hereinafter the "CPC"). Also, at the state level (BiH), there is the Criminal Code of BiH which defines specific criminal offences, mostly the most serious. These include crimes against humanity; organized crime; crimes against the integrity of Bosnia and Herzegovina and others. In the context of this study, it is interesting to note that the BiH CC also covers the infringement of a copyright as a criminal offence.

Definitions and substantive criminal law

Regarding definitions, in the BiH legislation, the definitions of the "computer system" and "computer data" are, interestingly, provided only in the BiH CPC. The definitions match almost verbatim with those provided in the Convention. Still, the purpose of providing these definitions in the CPC is not primarily related to cybercrime, they are given in the procedural context explaining the possibilities for search and seizure in any criminal investigation. Meanwhile, other definitions contained in the Convention such as: "service provider" and "traffic data" are not provided in the criminal legislation in Bosnia and Herzegovina. However, many terms, such as "computer", "program" or "data", probably do not have to be specifically defined in academic and legal texts, because the word should be given its ordinary meaning (UK Law Commission, 1988) In the most cases, there is no need to depart from this approach (Walden, 2004). Still, having in mind the relative novelty of these terms for most judges and prosecutors in BiH, it might be useful to provide these definitions in the applicable Criminal Codes.

Regarding the offences against the confidentiality, integrity and availability of computer data and systems, the criminal legislation in BiH, partially comply with the Convention. Firstly, illegal access (Article 2) is criminalised in compliance with the Convention, including the qualifying element: "infringing security measures". Still, Ikanovic thinks that proving the existence of "security measures", without broad definition being provided of what these measures actually involve, can cause practical problems in the prosecution and trials (2012, p. 17). Moreover, while the German Criminal Code (Strafgesetzbuch) understandably insists only on legal protection of data "especially protected against unauthorized access", it is questionable whether that is suitable for BiH and its neighbours, who also adopted the same solution. This is because of limited affordability of the computer security for average user in the Balkan region, which can lead to unpunished access to hundreds of thousands of computers in the region. Secondly, illegal interception is also criminalised under the criminal legislation in Bosnia and Herzegovina, in the same way as illegal access. Moreover, Article 3 (Illegal Interception) of the Convention does not require the breach of security measures as a condition for criminalization of illegal interception. Still, illegal interception is criminalised under the criminal legislation in Bosnia and Herzegovina and all its neighbouring states, in the same way as illegal access.

Article 6 (Misuse of devices) of the Convention was debatable among drafters regarding whether the devices whose production, sale, procurement for use, import, distribution is punishable, should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. Resultantly, this Article provides the possibility for the reservation concerning the limitation of this offence on the sale and distribution of a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed (Article 6, Paragraph 1 a.ii). As mentioned before, Bosnia and Herzegovina signed the Convention without reservation. Yet, the relevant provisions of FBiH and RS Criminal Codes are formulated in that narrower sense meaning that providing items that are to be used for accessing a computer system is criminalised. However, a request arising from full acceptance of Article 6 (misuse of devices for "the purpose of committing any of the offences established in accordance with Articles 2 through 5") is covered by the general Criminal Codes provisions on manufacturing and purchasing weapons and items for the purpose of committing a criminal offence.

Definitely, one of the major inconsistencies between the two Criminal Codes is related to computer-related forgery (Article 7) and computer-related fraud (Article 8). Namely, the FBiH CC contains separate provisions for these offences, which are essentially compliant with the Convention, just with small difference in terms, where computer-related forgery is titled "Electronic Forgery". On the other hand, the RS CC recognizes only computer-related fraud. In the mentioned CoE BiH Country Profile, the Criminal Code provision on Computer fraud is confusingly presented as the one complying with Article 7 (Computer-related forgery) of the Convention. The same situation may be noted in the Country Profiles of Montenegro and Serbia, while the Croatian legislation makes the distinction between these two crimes. Nevertheless, if there is no separate provision, it might be more appropriate to claim that computer-related forgery is covered by the provisions on ordinary crime of forgery, since "If existing offences already cover such conduct, there is no requirement to amend existing offences or enact new ones" (Explanatory note, Title 2). All the same, because of "possible gaps in criminal law

related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data", it may be recommended to introduce the provisions on forgery that are computer-related.

Content-related offences

Naturally, the production, distribution and other activities related to child pornography are criminalised under relevant legislation in Bosnia and Herzegovina. The legislation recognizes two categories of minors: juvenile - a person who has not reached eighteen years of age and child - person who has not reached sixteen years of age. However, the exploitation of both categories is punishable, with the difference in severity of sanctions, which means that legislation in BiH complies with the Convention (Article 9.3.). Still, the legislation in FBiH does not in any way connect this offence with computers or internet. On the other hand, the RS CC stipulates more severe sanctions for those who commit this crime trough internet. Having in mind increased danger and potential harm for the victim and to the society as a whole, which the use of the mass media or internet brings along, this seems not only justifiable but needed. Definitely, this solution should be introduced in the FBiH, too. Respective legislation of Croatia and Serbia contains separate provisions on the use of computer network or communication for committing child pornography-related crimes and provides for more severe sanctions, without substantive differentiation from ordinary crime. The lack of substantive criminal law on child pornography on the internet is not only typical of the region, which is kind of surprising. This because today the absolute majority of the child pornography crime is computer related and the use of the Internet as the primary instrument for trading such material is ever-increasing (Explanatory note, Article 9). In this connection, the Convention provides a rather comprehensive and precise overview of the forms of child pornography offences. In this respect, apart from the "minor engaged in sexually explicit conduct" and/or "person appearing to be a minor engaged in sexually explicit conduct"; particularly interesting is the following definition of child pornography that is provided in the Convention: "realistic images representing a minor engaged in sexually explicit conduct". Obviously, the creation and distribution of the described images do not harm a particular minor, but it does stimulate the demand for such material. Moreover, the development of ICT technologies is enabling tremendous possibilities for production and dissemination of such material which makes this activity particularly socially harmful. Still, BiH criminal legislation does not criminalise these acts, and it is certainly an aspect that should be considered.

The complex structure of Bosnia and Herzegovina is reflected in the way offences related to infringements of copyright and related rights (Article 10 of the Convention) are regulated. Namely, unlike most other offences defined in the Convention, the "Impermissible Use of Copyrights" is an offence covered by the BiH (State-level) Criminal Code. Most probably, this is due to the intention of the international community in BiH to provide the highest possible protection of copyright and related rights and the obligations arising from the relevant international documents (Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organization (WIPO) (Rajić, 2005, p. 500). Nevertheless, the BiH CC does not make any reference to IT technologies, but it covers a general problem of copyright infringement. This might be sufficient, since the Explanatory Note on the

Convention indicates that internet primarily influences the frequency of this offence, and it is not insisting on specifics. Further, the amendments of the BiH CC from 2013 also underlined importance of the intangible property, through the definition of the term "property", specifying that it can be tangible as well as intangible. Also, the same amendments prescribed that proof of the ownership can be in digital form. According to the official reasoning from Ministry of Justice these amendments are not adopted because of the compliance with the Convention, but because of the Moneyval recommendations and compliance with the other CoE Convention, i.e. the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No.141, 1990). Even though, this precise defining can be helpful in case of different procedures regarding the cybercrime, having in mind the formalistic approach prevailing among the BiH Judiciary.

The Convention (Article 11 thereof) requires its signatories to criminalise aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the Convention. Regarding the attempt, the Convention prescribes criminalisation of the attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

The Criminal Codes in Bosnia and Herzegovina provide uniform regulations for aiding and abetting an attempted crime. This means that whoever intentionally commences execution of a criminal offence, but does not complete such offence, shall be punished for the attempted criminal offence when, for the criminal offence in question, the punishment of imprisonment for a term of three years or a more severe punishment may be imposed, and for the attempt of another criminal offences when the law expressly prescribes punishment of the attempt alone. Regarding the aiding of a crime, it is prescribed that whoever intentionally helps another to perpetrate a criminal offence shall be punished as if he/she personally perpetrated such offence, but the punishment may be reduced. Whoever intentionally incites another to perpetrate a criminal offence shall be punished as if he/she has perpetrated such offence. Therefore, it is obvious that aiding and abetting are criminalised in accordance with the Convention. Still, as the criminalisation of the attempt is regulated as presented above, an analysis of the prescribed sanctions is needed. Furthermore, it is known that criminal penalties and other kinds of legal sanctions reflect the public attitude and state attitude (Allen, 1959, p. 228).

Firstly, under the FBiH CC illegal interception is punishable by a term of imprisonment of more than three years only in the case of it being committed by an official person while carrying out their duty. Otherwise, the sanction is imprisonment for a term not exceeding six months, which is the same as the sanction for unauthorized opening of a letter, telegram or any other sealed written material. The RS Criminal Code prescribes that if the illegal interception has resulted in electronic processing and transfer of data or of the network, or other grave consequences, the offender shall be punished by imprisonment up to three years. It can therefore be concluded that attempted illegal interception is not punishable in BiH and this clearly is not in accordance with the Convention. The situation is different when it comes to *system interference*. As noted, this offence is regulated separately from *illegal access*, and it is punishable by imprisonment up to five years. On the other hand, *system interference* in the RS Criminal Code is regulated by the same provision as *illegal access* and the same punishment – up to three years is foreseen. This practically means that an attempt at *system interference* is punishable in one part of the country and not in the other. Namely, the differences regarding the regulation of computer

forgery between the FBiH and RS Criminal Codes are naturally reflected in the sanctions prescribed for this kind of offence.

In the FBiH, when computer forgery is perpetrated in regards to computer data or programs of governmental bodies, public services, public institutions or business enterprises of special public interest, or if a considerable damage is caused, the perpetrator shall be punished by imprisonment for a term between three months and five years. In the absence of such circumstances, computer forgery is punishable with imprisonment for a term not exceeding three years. Interestingly, the sanctions for "ordinary" forgery are the same and similarly divided into two groups. The RS Criminal Code does not recognize computer forgery as a separate offence, but, the same as the FBiH Criminal Code it foresees an imprisonment term not exceeding one year for falsification of credit cards. An imprisonment term between one and eight years is foreseen for perpetrator who acquired property gain the value of which exceeds 10,000 KM.

The Criminal Codes in Bosnia and Herzegovina are following the current legal trend of recognising corporate liability (Horrigan, 2008), which is also promoted by the Convention (Article 12). The provision on sanctions (Article 13) just repeats a general rule that sanctions have to be "effective, proportionate and dissuasive", which is the catchphrase that can be noted in many EU documents and decisions of the European Court of Justice (Harding, 1997).

Procedural law

The introductory, common provisions (Article 14 & 15) of the Convention prescribe the conditions and safeguards for the adequate protection of human rights and liberties. In this regard the Convention calls for respect of standards provided by the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and the 1966 United Nations International Covenant on Civil and Political Rights. As these documents are incorporated in the BiH Constitution, the compliance with this requirement is ensured on the highest level.

The section on procedural law of the Convention relates mostly to traditional procedural measures and actions, such as search and seizure (Article 19) and interception of content data (Article 21). In this respect the Convention requires adjustments to the new technological environment. The Criminal Procedure Codes in Bosnia and Herzegovina fully comply with this requirement since all provisions on actions to obtain evidence, seizure of objects and special investigative measures explicitly include computers and computer systems. Furthermore, the principles and rules on jurisdiction proclaimed by the Convention (Article 22 thereof) fully comply with the territoriality principle that is traditionally incorporated in the Criminal Justice System of Bosnia and Herzegovina. This also applies to variants of the territoriality principle concerning ships, aircrafts etc., as well as subsidiary application of the nationality principle.

Nevertheless, the most interesting and significant provisions contained in the procedural law section are related to the expedited preservation. This is because the "data preservation is for most countries an entirely new legal power or procedure in domestic law" (CoE, 2001). Furthermore, data preservation is seen as extremely relevant to a particular criminal investigation and even as a "key to improving the counter-terrorist capabilities of law enforcement officials worldwide" (Archick, 2002, p. 3). Probably, these are the reasons why

the data preservation provisions are the only specific provisions of the Convention that are reviewed by the competent Council of Europe body in the terms of their implementation.

Specifically, in January 2013 the Cybercrime Convention Committee (T-CY) adopted the Assessment Report: *Implementation of the preservation provisions of the Budapest Convention on Cybercrime* (T-CY 10 REV). The Report concludes that Bosnia and Herzegovina is partially in line with Articles 16 & 29 of the Budapest Convention which are related to expedited preservation on the domestic (Article 16) and international level (Article 29).

In the absence of a specific legal provision on expedited preservation, the possibility of expedited production orders may allow the authorities to secure traffic data held by service providers in an expedited manner (Cybercrime Convention Committee, 2013, p. 20).

Furthermore, regarding international requests for traffic data, it has been noted that legislation in Bosnia and Herzegovina enables mutual legal assistance in criminal matters; a 24/7 Point of Contact has been established and some requests have been sent and received. The findings of the assessment of the provisions concerning disclosure of traffic data on domestic (Article 17) and on international level are similar. Namely, following the analysis of the applicable Criminal Procedure Codes and Law on Mutual Legal Assistance in Criminal Matters (BiH Official Gazette, No. 53/09) the TCY concludes that Bosnia and Herzegovina is partially in line with the CoE Convention (p. 55). Still, as it was the case with some provisions on substantive law, it is advised that Bosnia and Herzegovina adopt specific provisions in line with the Budapest Convention (TCY, 2013, p. 56).

Conclusion

Regarding the legislation in place in Bosnia and Herzegovina it can generally be said that the cybercrime threat is not ignored. Moreover, the influence of the CoE Cyber Convention and considerable efforts to follow its standards are obvious. A similar conclusion can be drawn for most countries of the region. However, the opinion coming from the CoE that the Convention is currently partially applied in the legislation in the countries of the region, including Bosnia and Herzegovina, seems to be a fair conclusion as some discrepancies and gaps are noticeable. Still, such shortcomings are understandable given the relative novelty of the crime itself and the Convention on one side and conservativeness as the common characteristic of the criminal justice systems on the other. As a result, the comparative analyses provided by this study, shows that there are a number of differences between the laws in the two entities in spite of the fact that legislators in both entities have incorporated, at least partially, principles of the CoE Convention in the relevant laws.

However, the comparative analyses provided by this study, shows that there are a number of differences between the laws in the two entities in spite of the fact that legislators in both entities have incorporated, at least partially, principles of the CoE Convention in the relevant laws. It is ironic that these differences are present in such a small country in an area of law which for various reasons requires global harmonisation. It is hard to imagine how harmonisation in this area could jeopardize the interests of one of the ethnic groups, which is often claimed as a reason for rejecting legislative changes. Therefore, there is simply no justification for the inconsistencies noted and described in this study. However, any legislative initiative should avoid uncritical copying of solutions from developed countries, because of the characteristics and particularities of BiH.

REFERENCES

- Allen, F. A. (1959). Criminal Justice, Legal Values and the Rehabilitative Ideal. *The Journal of Criminal Law, Criminology, and Police Science*, 50(3), 226-232.
- Archick, K. (2006). *Cyber crime: The Council of Europe Convention*. (Report for Congress No. 21208). Washington, DC: Congressional Research Service. Retrieved from: http://www.ncpc.org/cms-upload/ncpc/File/cybercrime.pdf
- Arief, B., Adzmi, M. A. B., & Gross, T. (2015). Understanding Cybercrime from its Stakeholders' Perspectives: Part 1--Attackers. *IEEE Security & Privacy*, 13(1), 71-76.
- Council of Europe (1990). *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*. Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/141
- Council of Europe. (2012). *Cyber Crime Legislation Country Profiles – Bosnia and Herzegovina.* Retrieved from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/cyber_cp_BiH_2010_June.pdf
- Criminal Code of BiH, *Official Gazzete of Bosnia and Herzegovina*, No. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07,8/10, 47/14, 22/15, 40/15 (2015).
- Criminal Code of FBiH, *Official Gazzete of Federation of Bosnia and Herzegovina*, No. 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14 i 46/16 (2016).
- Criminal Code of RS, *Official Gazzete of Republic of Srpska*, No. 49/03, 108/04, 37/06, 70/06, 73/10, 1/12 i 67/13 (2013).
- Criminal Procedure Code of BiH, *Official Gazzete of Bosnia and Herzegovina*, No. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05,48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09 i 72/13 (2013).
- Criminal Procedure Code of FBiH, *Official Gazzete of Federation of Bosnia and Herzegovina*, No. 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 9/09, 12/10, 8/13, 59/14 (2014)
- Criminal Procedure Code of RS, *Official Gazzete of Republic of Srpska*, No. 53/12 (2012).
- Digital Citizens Aliance (2014). *"Good Money Gone Bad"*. Retrieved from: http://media.digitalcitizensactionalliance.org/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/4af7db7f-03e7-49cb-aeb8-ad0671a4e1c7.pdf
- FACT (2017). *"Online Piracy"*. Retrieved from: https://www.fact-uk.org.uk/the-problem/digital-online-crime/online-piracy/
- Foggetti, N. (2008). Transnational Cyber Crime, Differences between National Laws and Development of European Legislation: By Repression. *Masaryk University Journal of Law and Technology*, 2 (2), 31- 62
- Gercke, M. (2011). *Understanding Cybercrime: A Guide for Developing Countries* (*2nd edition).* Geneva: International Telecommunication Union
- Hernandez-Castro, J., Cartwright, E., & Stepanova, A. (2017). Economic Analysis of Ransomware. *SSRN Electronic Journal*.

- Holmes, O. W. (1899). Law in Science and Science in Law. *Harvard Law Review*, 12 (7), 443-463.
- Horrigan, B. (2010). *Corporate Social Responsibility in the 21st Century: Debates, Models and Practices Across Government, Law and Business*. Cheltenham: Edward Elgar Publishing.
- Ikanovic, V. (2012). Krivična djela kompjuterskog kriminala u Krivičnom zakonodavstvu Bosne i Hercegovine [Criminal Acts of Cybercrime in Criminal Legislation of Bosnia and Herzegovina], *Pravo i Pravda,* 1, 15 – 35
- Jouhal, J. (2017). The Rise of Ransomware and How to Avoid Being Held Hostage. *New Statesman, Spotlight on cybersecurity*, pages 8–9, February 2017.
- Keyser, M. (2002). Council of Europe Convention on Cybercrime, *Journal of Transnational Law & Policy*, 12 (1), 287-32.
- Parker, L. (2016). Large UK Businesses are Holding Bitcoin to Pay Ransoms. Bravenewcoin.com News, 9 June 2016. Retrieved from http://bravenewcoin.com/news/large-uk-businesses-holding-bitcoin-to-pay-ransoms/
- Rajic, Z. (2003). *Komentar zakona o krivičnom postupku* [Commentary of the Criminal Procedure Code]. Sarajevo: Kancelarija Vijeća Evrope.
- Walden, I. (2004). Harmonising Computer Crime Laws in Europe. *European Journal of Crime, Criminal Law and Criminal Justice, 12*(4), 321-336.
- Wall, D. S. (2015). *The Internet as a conduit for criminal activity*. Sage Publications.

About the Author

Arben Murtezić graduated from the Faculty of Law of the University of Sarajevo and earned his Master's degree at the University of Portsmouth. From 2010 to 2016, he served as a Chief Disciplinary Counsel of High Judicial and Prosecutorial Council of Bosnia and Herzegovina. Currently Director of the Centre for Judicial and Prosecutorial Training of the Federation of Bosnia and Herzegovina. E-mail: arben.murtezic@myport.ac.uk; arben.murtezic@cest.gov.ba