International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 10, Issue 6
June, 2023
Pages: 230-239

Criminal Procedure for Computer Crimes

Edon Azemi

Student in LLM in Department of Criminal Law, Faculty of Law / UBT - Higher Education Institution, Pristina, Republic of Kosovo

http://dx.doi.org/10.18415/ijmmu.v10i6.4884

Abstract

Work on criminalistic procedures for computer crimes that must be undertaken for data protection. In the paper, cybercrimes are researched throughout history until today, the categorization of cybercrimes is analyzed and researched. The purpose of the paper is to analyze and research with special emphasis cybercrimes against the individual, cybercrimes against property, cybercrimes against the organization as well as cybercrimes against society. The paper uses the analysis method, the comparative method as well as the deductive and inductive method. This paper will help lawyers and individuals who deal with the prevention and combating of computer crimes.

Keywords: *Computer Crimes; Cybercrimes Against the Individual; Cybercrimes Against Property; Cybercrimes Against the Organization; Cybercrimes Against Society*

1. Introduction

Criminality is antisocial behavior which is in conflict with legal and moral norms of behavior (Maloku,2019:174). Criminality represents the set of all actions that endanger and/or harm fundamental human values (protected by law) (Maloku,2021:60).

The importance of protecting data from others is very great, but the eventual omissions we can make can be fatal for us and society as a whole. We must save data and be careful about any information we share on the Internet. Malicious attacks cost businesses billions of dollars each year. This has led many IT researchers to deal with data security and the possibility of protecting users from computer crimes. These crimes, in addition to material damage, also cause psychological damage because they can affect children or even adults for online fraud and what is considered online pornography. Cyber crime should be fought as much as possible so that others can use software and hardware without fear of crime. (www.slideshare.net/cyber-crimekrimet-kibernetike). Cyber terrorism can also act on medical services, resulting in severe losses through access to the system, and the set goals (Janny, 2015). The very dynamic increase of this type of criminality (Maloku, 2015:119, 2019a,2019b; Gabela & Maloku, 2022, 2023), as a form of organized crime, should undoubtedly be countered in a repressive and preventive manner. In order to combat international organized crime, it is more than necessary that the competent governmental institutions harmonize legislation with world standards to cooperate among themselves, especially in the field of exchange of information that is important for Preventing and Combating Organized Crime

(Maloku, 2015: 461). Prevention of computer attacks from terrorism can be achieved with a special education against various cyber crimes (which will help reduce the number of various scams), with a more dedicated regulation of the government towards criminal violations, etc. This paper is an attempt to highlight the growing phenomenon (Maloku & Maloku, 2020:21) of this negative occurrence that has hit Kosovo.

Authors Jasarevic & Maloku (2021) in their book Criminology (etiology and phenomenology of criminality) analyze and elaborate the etiology and phenomenology of criminality, they elaborate on various factors that influence the growth of criminality.

Also, Jararevic and Maloku (2021) in the book Criminal Procedural Law I and II (general and special part) the authors affirm that Criminal Procedural Law and Criminal Material Law constitute the right in a broader sense, which in itself imposes their close connection, because in the end they practically serve the same purpose, to achieve procedural criminal protection and security of society from criminality.

2. Methodology

This study is based on the use of multiple research methods. Special scientific (Maloku, 2021:53). The historical method will reflect the birth and spread of cybercrime, and the development of global legislation on the prevention and combating of cybercrime. The descriptive method will also describe the definitions of the nation of "Cybercrime", the victims and their types that appear as a result of cybercrime, and the tools that are used to investigate these crimes. Using comparative, theoretical and meta-analysis methods, the views of several different perpetrators will be presented (Maloku, 2021:170) regarding cybercrime. While, through the statistical method, the most frequent cases of these crimes have been reflected through various applications that are usable nowadays. The research design is not experimental.Since it is clear that this topic is inherently complicated, the paper also uses the content analysis method (Maloku, 2020:323) as a necessary method to study multidimensional research on cybercrime.

3. Results and Discussion

3.1. The history of Cyber Crime

Crime is considered a problem, which mostly affects the quality of life not only of individuals but also the wider circle where we live (Maloku. 2015:29). With the development of human society, various forms of criminality have also developed, and in particular the emergence and rapid development (Maloku, 2016:10) of cybercrime. Nor a form of widespread criminality has appeared since 1960 and since that year the use of so-called hacking began.

Online dating is no longer limited to humans. In 2008 the number of things connected to the Internet exceeded the population of the Earth. According to Evans (2011), these things are not just smartphones and tablets, they are everything from internet-connected cars to animal husbandry systems managed by applications that use wireless. According to Evans, by 2020 the number of devices connected to the Internet will increase to 50 billion. The expansion of the Internet has provided great benefits in various fields such as telecommunications, education, transport and many other fields, but alongside it, crimes have also developed with the aim of profiting from the people who target them. The birth of cybercrime brought with it consequences of information technology crime attacks, intellectual crime and cybercrime. One of the first documented computer crimes is that of Kevin Mitnick committed in 1970. This guy was able to access a telephone company's network through modems and dial-up where he was able to access connections and make calls. free of charge. In 1984, the Computer Crimes Act was enacted in the US for the Forged Access to Devices and Computer Fraud and Abuse Acts. This act has not only protected criminal acts but has prohibited the use of the computer as a tool to cause damage to other computer systems. In the early 1990s, it was realized that hackers are not only ordinary people who use the Internet to carry out activities, but there are also other people who use the Internet to commit criminal crimes known to the law (such as remote bombings and child pornography). FBI agents have discovered that pedophiles are using the Internet to lure children in order to achieve their dirty goals. They have also used chat rooms to convince children to meet and go to homes. In 1995, the FBI launched the Innocent Images National Initiative, where agents built a website to consult computer crime wikis, which led to the arrest of more than 7,000 criminals in the USA.

3.2. What Do We Mean by Cyber Crime?

Computer Crime - Computer crime refers to crimes involving computers and computer networks.

Dr. Debarati Halder and Dr. Using the Internet" Often, during online deviance movements, the term cybercrime is used. Another definition can be: computer crime is a criminal offense that is created with the technology of technology, or as a traditional crime transformed into a computer crime.

3.3. Categorization of Cyber Crime

Cyber crimes are not only of one type, they are divided into several types and several subcategories.

We can mention three general types of these crimes classified by Brenner:

- Computer/machine crimes (hacking, spreading viruses)
- Crimes using computers (online fraud, child pornography) and
- Crimes in the car (manipulation of data for criminal activities)

Another type of computer crime divisions that is roughly the same as the above types can be:

- Crimes committed through the Internet and
- Internet-based crimes.

Cybercrimes are types in which the Internet and other network data are used, but are not necessary for the commission of the crime. Crimes committed via the Internet can be executed offline, such as identity theft or credit card attacks, but are more likely to occur online. Some other types of classifications are those that involve considering factors other than the role that the computer system plays in the commission of computer-related crimes.

These factors include: threats, attackers, attacks (Kanellis et al, Chakrabarti and Manimaran), motives, and victims. (www.slideshare.net/KrenareRexhepi/cyber-crimekrimet-kibernetike)

3.4. Cybercrime

Challenge for today's society The use of new information technologies and especially the Internet has taken on a special importance in everyday life. This phenomenon affects not only the activities of an organization, be it state or private, involved in the sphere of business or a non-profit activity, but it can also affect the common man in his daily activity, in his private or professional sphere. . Like any new technology made available to a large number of users, the Internet presents not only good things and benefits, but at the same time a number of problems. Being a technology that has been "liberalized" for some time, as it is used in the jargon, it is not worth discussing the benefits that the use of this technology brings. The benefits side can be summarized for the moment in a single phrase: communication (in the broadest sense of the word) fast, inexpensive and completely independent of the notion of distance. In this article we will focus mainly on the avoidance of the primary purpose of using this technology (communication). Its misuse by criminal elements is known as cybercrime. In daily practice, there are two types of behavior in the face of the phenomenon of cybercrime. On the one hand we have the everyday user who is very often guided by the idea that "evil always goes to others". On the other hand, we have the specialists in the field who are diametrically guided by the opposite, namely that "we are all equal, at least in mathematical terms, to the probability of being the object of a criminal attack". Unlike the ordinary user, the specialist devotes time to the analysis of the phenomenon to understand its operation. It should be emphasized that at no time and under no circumstances should we fall prey to the idea that one day we can make this probability zero. This statement takes on great importance when it comes to new technologies and IT security. By nature, new technologies are constantly evolving and therefore the risks associated with this technology evolve in the same way. Scott Peck, a well-known American psychiatrist and successful book author writes: "The only way to have security in life is to know uncertainty." So what is cybercrime, where does it come from, what helps it to be so widespread, how can we prevent it and are we prepared for this phenomenon? These are some questions that specialists, be they computer scientists, information systems specialists, criminologists, lawyers, economists, etc., try to address in their daily activities. In fact, cybercrime should be distanced a little from a general notion of what is called computer crime. The latter is related to a criminal activity that has the computer as its object or as a way of committing the crime. Cybercrime is therefore in this prism a subcategory of computer crime and has to do with the criminal activity developed in the network.

The Internet is one of the most global networks and the most used today. After this clarification, we can prove that being on the network exposes us to the risk of a possible attack. It would be unprofessional to advise a disconnection from the grid, because in today's increasingly global economic structure, disconnection would transform the organism into a non-competitive organism. Another aspect that must be addressed to understand the phenomenon of cybercrime is the technology used. An ordinary computer or Internet user, from the moment everything works normally for him, no longer cares what actions, calculations or protocols the computer performs to reach this result. On the other hand, producers of programs, devices, ISP, etc., do not have a spontaneous will to inform the user about the way of operation, and to be coherent this would be unrealistic. So in conclusion the technology remains more or less non-transparent for the user. Regarding the Internet, several other factors make this technology vulnerable and therefore a very fertile ground for the development of crime. - From a technological point of view, we can mention the fact that the Internet is a public technology and open to all. Historically, the communication network was developed as a tool of the military field to then be used by university students to facilitate communication between them. This vision of use meant that in its beginnings, Internet technology did not include the aspect of security as long as communication (both in the military and in the university) was between people who knew and trusted each other. Internet technology is a "best effort" technology. This means that in its conception "we did what we could" to reach the desired result, without imagining what deviation could be made to its use. From a network and system point of view, in the case of the Internet we are dealing with a great freedom in terms of configuration, the way segmented security is handled and what is more important in our case, the total lack of control. It is not for nothing that the Internet is identified as a "network of networks" and its structure is often compared to a spider's web. - From a legal point of view, the Internet is conceived and functions in such a way, that for it the notion of borders does not exist. In the legal field, a crime is primarily sanctioned by a law. This law belongs to a particular country and is enforced by a competent court of a particular country. The notion of the state is closely related to the notion of territory, that is, to state borders. This greatly affects the prosecution phase of the crime. Imagine a hacker who commits his criminal act from say, China, attacking a bank in Switzerland and transferring the stolen amount electronically to Italy. Which judicial institution and which law is competent in this case? China, the place from which the perpetrator committed the crime, Switzerland, the place where the victim is located, or Italy, the place where the result was achieved? Three countries so different in terms of location, legal culture and perception of the notion of crime, will they be able to agree on the prosecution and trial of this act? The answer is not very obvious. - Finally, if we consider the problem from a user's point of view, then we have touched the

Achilles' heel. Is the user aware of the consequences that the use of the Internet can bring? The answer is negative in most cases. In a program broadcast recently on one of the Albanian televisions, a bank executive brought as an argument the fact that banking programs are so sophisticated that it is very difficult to "break", which represents a part of the truth. When banking operations are carried out online, as is the case with e-banking, which is starting to be practiced in Albania, the user is vulnerable regardless of the strength and algorithms used in the bank's software. There is also a very important fact that should be emphasized: the crime will try to hit the weakest, most unprepared victim, that is, the most attractive target for him.

Experience shows us that over 50% of attacks have the person as their object. But even if we consider the organization of the bank itself and the fact of sophisticated software, experience in the field of cybercrime has shown that over 70% of attacks have internal origins. This can come from a disgruntled subordinate, a profit-driven subordinate, etc. The list of motivations is long. In this aspect, the technological complexity does not help much and it is the managerial structure of the institution and all its constituent aspects that take on special importance. In the show in question, the level of very rigorous control over personnel, which is known as "management through fear" (fear management), was brought as a fairer example. But at the same time the results of this strategy are very controversial in the circles of human resources professionals. In our opinion, considering the high degree of importance of information systems in the functioning and survival of the organism, we would have leaned more towards a management style focused on communication, education and sensitization of subordinates on the consequences both on a personal level and professional. This, explaining that technology alone cannot solve the problems related to IT security and IT crime and that the human factor is of primary importance. To return to the notion of cybercrime and to understand what is called the modus operandi of committing the crime, we must refer to the triangle theory that is often cited in the literature of criminology. This theory tells us that in order to commit a crime, at the same time, we must have a concordance of three factors: a motivated criminal, a vulnerable object who are in the same place, at the same time. Starting from this theory and considering the elements we cited above: - the limited knowledge of the Internet on the part of the victim, - the motivation, opportunity and facilities that criminals have to commit the criminal act via the Internet, - the ideal and constant meeting place as the network is, we can conclude that cybercrime is and will increasingly become a very attractive ground for criminality. Practice shows that organized crime has already understood the importance and benefit from the phenomenon of cybercrime. The anonymity that the Internet offers means that organized crime is slowly starting to take interest and take control of this phenomenon. As an example, we can take the case of the Bank of Sicily in 2000, where a group of 20 people, of course with specific knowledge in the field of IT and connected to several mafia families, managed to create a clone of the bank's e-banking service . Thus, in this way, they managed to acquire the sum of $400 million made available by the European Community for regional development. After embezzling the amount in question, they used other online banking services to launder the money and lose track of it, implicating well-known banks such as the Vatican Bank, several banks in Switzerland and Portugal (wikipedia.org/wiki /cyber_crimes). At this stage, it should be emphasized that in order not to be noticed, the sums appropriated by cybercrime are, in most cases, small sums of money. According to the IC3 2004 Internet Fraud – Crime Report, 43% of the amounts embezzled are no more than $100 per act and 25.6% do not exceed $1,000. So it is very difficult to attract the attention of specialists or to justify a judicial procedure. It is understandable that one article cannot deal in detail with all the components of the cybercrime phenomenon. The message we wanted to convey is that cybercrime is a phenomenon that affects a number of competencies, such as those in the field of informatics, criminology, economics, justice, etc. Cybercrime is therefore a complex phenomenon and the only way to deal with it would be a global way of dealing with the problem. For this, the cooperation of all the experts in the above-mentioned fields is needed to avoid segmental solutions. For this reason, it is important to conceive a global information security architecture that takes into consideration the technical and operational dimension, the legal and regulatory dimension, the organizational and economic dimension, not forgetting the human dimension.

3.5. Cyber Crimes and Their Classification

> ***Cyber threat/attack*** *is considered any directed/intentional attempt to access, manipulate, interfere with or damage the integrity, confidentiality, security and/or availability of data, an application or computer system data, without having legal authority to to do this.*

Classification of cybercrimes

Computer crimes can be classified into 4 major categories:

1. Cybercrime against the individual
2. Cybercrime against property
3. Cybercrime against the organization
4. Cybercrime against society

3.5.1. To Individuals

A). Email Spoofing

A spoofed email is one in which the email header is forged so that the email appears to originate from one source, but is actually sent from another source.

B). Spamming

Sending mass emails with the purpose of collecting information, installing a virus, mass fraud.

C). Slander

This happens when defamation is done with the help of computers and/or the Internet. Eg someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.

D). Harassment & Cyber Stalking

This Is Done By Following The Movements Of An Individual's Activity Over The Internet. This Can Be Done With The Help Of Many Protocols Available Such In E-Mail, Chat Rooms, Net User Groups.

3. 5.2. About the Property

A). Identity Theft

The computer space is used to obtain personal information of the victims, such as the social security number, license number, etc., by modifying, adding or changing the identity data of the person, to commit criminal acts or obtain property rights, or money or use credit cards or bank accounts belonging to the victim. For example, a phone number registered in an address book may belong to a known drug dealer and become a criminal record holder.

B). Intellectual Property Crimes

These include Software Piracy: illegal copying of programs, distribution of copies of software, copyright infringement, trademark infringement, theft of source code, etc.

C). Theft of Internet Time

The Use Of Internet Hours By An Unauthorized Person, Which Was Actually Paid By Another Person.

3. 5.3. To The Organization

A). Unauthorized Access to the Computer

Using the computer / network without permission from the owner. It can be of 2 forms:

-Change / deletion of data: Unauthorized change of data.
-Computer espionageComputer espionage is about discovering "information", or "evidence".

An industrial spy may seek to discover secret information on a Microsoft project manager's laptop that specifically concerns the future of the company by neutralizing operating systems. Depending on the information, it can be processed in certain evidences. Besides information and evidence, there are two important concepts in computer espionage: The activity is typically unknown and unauthorized. In many cases, the victim is not going to give explicit or implicit permission to allow someone to poke their noses into their computer. Exceptions may be the cases of workplaces, in which employees are monitored.

B). Denial of Service

A DoS (Denial of Service) attack is an attack that exploits a vulnerability in the target's OS or software, or Internet Protocols such as TCP/IP, bringing down the attacked service, and sometimes all services. of the sacred system. In short, this attack denies legitimate users the specific service offered by the victim system. A simple example of such an attack would be the ping command. In unpatched versions of Win 95 systems, the TCP/IP protocol could only manage a data packet smaller than 64400 bytes; such a ping: ping -t -l 65500 will cause the system to crash or reboot. This would be the simplest example of DoS used at the time.

Today, ping attacks are a bit overrated. You would have better luck with sophisticated techniques such as SYN Flooding, Tear Drop, Smurf, TARGA3, Semirandom, etc.

C). Computer Contamination/Viruses

A computer virus is a program which can infect other computer programs by modifying them and copying itself. Viruses can infect files or affect the computer's boot sector.

Worms, unlike viruses, do not need a host to infect.

D). Email Bombing

Sending a large number of emails to individuals, companies or mail servers, which may result in crashing.

E). The Salami Attack

When negligible amounts are removed and accumulated into something larger. These attacks have been used to commit financial crimes.

F). Logic Bombs

A program that depends on an event, the moment the certain event happens, it crashes the computer, releases a virus or something else harmful.

G). Trojan Horse

an unauthorized program that acts as if it is an authorized program, thereby hiding what it is actually doing.

3.5.4. To Society

A)**. Falsification**

When a criminal changes data recorded in a computer system, the crime committed may be forgery. In this case, the computer system may be the target of criminal activity. However, computers can be used as tools by which counterfeiting is carried out. A generation in the field of forgery was rapidly added when the first color laser photocopiers became available. These photocopies have an extremely high resolution for copying and editing documents, creating a false document with no difference from the original. In addition, they produce documents whose quality is indistinguishable from the real ones and for which an expert review is necessary.

B). Cyber Terrorism

Using the computer/internet to incite terror in others.

Cyberterrorism is a combination of terrorism and cyberspace. It is defined as a premeditated, political, motivated attack against information, computer systems or programs, and data that results in violence, against targets by international groups or clandestine agents. Attacks that cause death, bodily harm, explosions, plane crashes, water contamination or various economic losses can be examples. Dangerous attacks can be carried out against the infrastructure and be computer crimes, depending on their impact.

C). Web Jacking

Hackers gain access and control over someone else's website by exploiting vulnerabilities, and they can even change the content of the website to fulfill a political objective or for money. (wordpress.com/2015/04/25/cyber-crimes-and-their-classification/)

4. Conclusion

Cybercrime is a field for which we have to work and study a lot, so that we basically understand the problems that this phenomenon/crime can cause. The problems that may appear can be either easily overcome or severe or insurmountable. People who may be victims of these crimes must be informed accurately and in simple language to overcome the consequences caused by the attacks. The people who are the cause of these crimes, for their own interests, harm others, therefore they should be punished with the highest possible penalties, within the framework of the laws in force. The police, the secret services and the people responsible for the security of the various programs must cooperate with each other to detect the crimes since these crimes have existed since the time of the existence of computer devices and have developed and become more sophisticated with each passing day. Since with the expansion of technology and the opportunities it offers us, the use of the Internet also increases, it is very likely that computer crimes will expand even more, so we must fight these crimes by getting as much information about them as possible, and inform others to protect themselves from these crimes.

References

1. Gabela, O., Maloku, A. (2022). Genocid: osnovni aspekti u poimanju, shvatanju i istraživanju zločina. Univerzitet u Sarajevo. Institut za istraživanje zločina protiv čovječnosti i međunarodnog prava. Sarajevo.

2. Gabela, O., Maloku, A. (2023). Genocid: fundamental aspects of understanding, comprehending and investigating crime. University of Sarajevo: Institute for Research on Crimes against Humanity and International Law. Sarajevo.

3. Haka, E. (2020). Krimi Kibernetik dhe Legjislacioni Ndërkombëtarë. Academia. Available at:

https://financesonline.com/cybercrime-statistics/ Last accessed: 09.2.2022.

4. Jasarević, O., Maloku, A. (2021). *Kriminologija (etiologija i fenomenologija kriminaliteta*). Universitet u Travniku. Travnik. Bosna i Hercegovina.

5. Jasarević, O., Maloku, A. (2021). *Krivično procesno pravo I dhe II (opšti i posebni dio).* Universitet u Travniku. Travnik. Bosna i Hercegovina.

6. Jay, A. (2022). Important Cybercrime Statistics: 2021/2022 Data Analysis & Projections. Finances Online - Reviews for Business.

7. Jenny, S. (2015). Krimet Kibernetike dhe Klasifikimi i tyre. Bota Ndryshe: Available at: https://botandryshe.wordpress.com/ Last accessed: 15.28.2022.

8. Karović, S., Maloku, A., & Shala, S. (2020). *Juvenile Criminal Law in Bosnia and Herzegovina With Reference to the Criminal Legal Position and Responsibility of Juveniles*. *Kriminalističke Teme*, (1-2), 107-122. Available at: https://krimteme.fkn.unsa.ba/index.php/kt/article/view/205.

9. Maloku, A. (2015). *Bashkëpunimi ndërkombëtar policor në luftimin e krimit të organizuar*. Regional Journal of Social Sciences Reforma. No.2. 2015 pp. 119-127.

10. Maloku, A. (2015). Fear of Violence and Criminality in the Region of Gjilan, Kosovo. Mediterranean Journal of Social Sciences, 6 (2 S5), 29–36. Doi:10.5901/mjss.2015.v6n2s5p29.

11. Maloku, A. (2015). *Rregullimi ndërkombëtar ligjor për të parandaluar abuzimin e drogave dhe substancave psikotrope*. Balkan Journal of Interdisciplinary Research. Vol.1. No. 1. 2015. pp. 461-472.

12. Maloku, A. (2016). Karakteristikat e organizatave kriminale transnacionale. Buletini Shkencor Nr. 5 “DARDANIA. p. 10-24.: Qendra Kërkimore Zhvillimore – PEJA. Peje.

13. Maloku, A. (2019). *Fjalor i terminologjik i viktimologjisë*. Kolegji Iliria, Prishtinë.

14. Maloku, A. ., Qerimi, I. ., & Maloku, E. . (2022). The Scope of Crime by Social Origin in the Region of Gjilan. Academic Journal of Interdisciplinary Studies, 11(4), 172. https://doi.org/10.36941/ajis-2022-0107.

15. Maloku, A., Kastrati, S., Gabela, O., & Maloku, E. (2022). Prognostic scientific research in planning and successful management of organizations in the security sector. Corporate & Business Strategy Review, 3(2), 138–150. https://doi.org/10.22495/cbsrv3i2art12.

16. Maloku, A., Maloku, E. (2020). *Protection of Human Trafficking Victims and Functionalization of Institutional Mechanisms in Kosovo*. Acta Universitatis Danubius. Juridica, 16 (1), 21–44.

17. Maloku, A., Maloku, E. (2021). *Fajlor i terminologjisë juridiko-penale për gazetarë*. Kolegji Iliria, Prishtinë.

18. Maloku, Ahmet. (2015). Kodi i te burgosurve. Revista shkencore nderkombetare DISKUTIME. Volume.4, Issue.15. pp.34.41. Qendra per marredhenie nderkombetare dhe studime ballkanike, Akademia diplomatike shqiptare Tetove.

19. Maloku, Ahmet. (2016a) Medunarodna saradnja u borbi protiv transnacionalnog organizovanog kriminala. Universitet u Travniku. Pravni Fakultet. Travnik. Bosna i Hercegovina.

20. Maloku, Ahmet. (2018). Drustvena dezorganizacija i obiljezja kriminaliteta na podrucju regije Gnjilane (Kosovo) u periodu 2010-2014. Univerzitet u Sarajevu: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije. Sarajevo.

21. Maloku, E., Jasarevic, O., & Maloku, A. (2021). *Assistance of the psychologist expert in the justice bodies to protect minors in Kosovo*. EUREKA: Social and Humanities, (2), 52-60. https://doi.org/10.21303/2504-5571.2021.001649.

22. Rexhepi, K. (2013. *Krimet Kibernetike - Kosovë.*, nga Akademia: Available at: https://www.academia.edu/21816119/Krimet_Kibernetike. Last access: 011.18.2022.

23. Shabani, Alisabri, Maloku, Ahmet. (2019a). Sociologjia. Kolegji Iliria, Prishtinë.

24. Shabani, Alisabri, Maloku, Ahmet. (2019b). Tema te zgjedhura nga Patologjia Sociale. Kolegji Iliria, Prishtinë.

Internet Resources

25. https://www.slideshare.net/cyber-crimekrimet-kibernetike.

26. https://www.slideshare.net/KrenareRexhepi/cyber-crimekrimet-kibernetike.

27. https://sq.wikipedia.org/wiki/Krimet_kibernetike.

28. https://botandryshe.wordpress.com/2015/04/25/krimet-kibernetike-dhe-klasifikimi-i-tyre/.

Copyrights