International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 6, Issue 2
February, 2023
Pages: 266-274

Computer Crime

Laureta Qunaj

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

E-mail: lq69690@ubt-uni.ne

http://dx.doi.org/10.47814/ijssrr.v6i2.991

Abstract

In the last decades, we have an exceptionally large increase in computer crime, therefore, bearing in mind this fact, we have tried to present computer crime as a fairly widespread form both in Kosovo and in the region. By researching the criminality literature of different authors, we were able to focus our research on the analysis of the appearing forms of this phenomenon. The purpose of this paper is also to analyze the features or characteristics of cybercrime as a form of white collar crime as well as the forms of presentation of computer criminality. The paper uses methods of analysis, content, qualitative methods and comparative methods.

Keywords: *Cybercrime; Characteristics of Cybercrime; Computer Fraud; Theft of Information; Computer Sabotage*

1. Introduction

In contemporary society and with all its evolution towards the permanent development of life and progressive technology, it is important that even this rapid development be studied in different aspects, as well as looking at it with a critical eye.

In the continuation and above of this paper, one of the issues that is of great importance in the days we are living in will be discussed, so we will talk about one of the many types of white-collar crime or, as it is expressed differently, a type of crime. which is performed by persons with a higher authority (official persons).

The use of the computer and international information networks in the contemporary world has influenced radical changes in human life and work. Therefore, the application of the computer has given a great impetus to the development of science and human well-being.

It is not always necessary to see that only classic crimes or murder crimes are the ones that lead us to believe that they are the most frequent, but also the following treatment of cybercrime has its undeniable peculiarities for research aspects.

Criminality as a negative phenomenon is analyzed in many aspects. In the Sociological aspect, the authors Shabani and Maloku (2019) have elaborated exceptionally well in their book Sociology. Likewise, the same authors Shabani and Maloku (2019) in their book Selected topics from social pathology elaborate on phenomenology and pathological social phenomena in relation to criminality. Criminality as antisocial behavior is in conflict with legal and moral norms of behavior. (Maloku, 2019:174). Criminality represents the group of all actions that endanger and/or damage basic human values (protected by law). Those basic values can be individual (human life, physical or bodily integrity, freedom, wealth, security, etc.), or collective or shared values (social regulation, state security/institution, economic or social system of the state, etc. (Maloku & Maloku, 2021:60).

Another very important thing is the aspect of fighting this harmful phenomenon for society. Therefore, in the framework of this, we will see that many countries have systematized the legislation regarding cybercrime, but at the same time, they also welcome cooperation with other countries in this regard. field.

The paper is based thematically and essentially on the theoretical conceptions of this problem in the field (Maloku, 2021:76) of Criminal law. The paper gives a brief summary of the criminal law aspect, namely the material law aspect. (Maloku, 2020:21).

Cybercrime - Cybercrime - is spreading rapidly day by day, taking into account the interference in software with data from state or private activities. The increase in crime brings fear to the population (Maloku, 2015), criminality in general and computer criminality as a form of criminality have been analyzed and elaborated very well by the authors Jasarevic and Maloku (2021) in their book Criminology (etiology and phenomenology of criminality). The authors Jasarevic and Maloku (2021) have made an extremely large contribution to the fight against and prevention of criminality in their book Criminal Law and Procedure I and II. Research is also significant for social practice and practical reasons such as controlling and properly preventing crime. (Maloku, et al., 2022:172).

2. Methodology

The research is based on the use of research methods such as inductive and deductive methods.

Content analysis as a necessary method will be used to study the numerous literatures, in which this problem has been addressed in various respects. This method is unavoidable in the study of normative acts (laws and international acts). (Maloku et al., 2021:53) In the end, it should be stated that during the research, qualitative data on the subject of the research were obtained and their complementarity was ensured. The reliability of data sources was crucial for drawing relevant conclusions based on scientific premises (Maloku et al., 2022:141). The comparative method was also used in the research.

3. Results and Discussion

3.1. Understanding Computer Crime

Computer crimes are also considered to be one of the most frequent forms of white collar crime. This form of criminality is showing a large increase in contemporary society and is expected to increase further along with the rapid growth of Internet users. (Gashi, 2012:47))

According to some international definitions, the term computer crime is divided into two categories:

a). In a narrow sense, computer crime will be understood as any behavior carried out through electronic actions which are aimed at the security of computer systems and the data processed by them;

b). In a broader sense, computer crime will mean any illegal behavior committed by or through a computer or computer system, including crimes such as illegal processing, provision or distribution of information from a computer or network, for abused and attracted attention with forms such as those for supporting terrorist groups, neo-Nazis, pornography and pedophilia. This will also include types of fraud crimes, violating network security such as illegal gambling, pyramid schemes, credit card fraud and other types of illegal activities. In cybercrime, the "cyber" component is usually referred to to qualify the new offenses enabled by information technology or the interaction of computer space, in many traditional activities. (wikipedia.org/wiki/Krimi_komputerik)

The notion, as well as the phenomenon itself, was presented in the United States of America. Von zur Muhlen-1973 was the first to write an extensive scientific paper on computer crime (Latifi, 2009:336). are misused and are being used to commit a large number of crimes and delinquent behaviors that were not so easily committed before

The technology and the opportunities it offers, has encouraged delinquents and criminals to use this as a powerful and very sophisticated tool and method, for committing a series of crimes, offering opportunities for them to hide their tracks, and more difficult to discover. Regarding the computer and the phenomena of criminality, a lot has been written and discussed during the last decade and in this direction scientific and professional debates and gatherings have been organized in many countries of the world in order to find methods and tools to prevent the misuse of the computer for criminal purposes. . Some countries such as the USA, England, Germany, Japan, Canada, etc., have largely managed to issue specific and special provisions regarding the prevention of computer misuse for criminal purposes.

In the criminological literature, the prevailing opinion is that computer crime has to do with criminal actions against property and against the economy. However, the computer as a tool and as a method of committing crimes is also used for the commission of other criminal behaviors. Some authors call such criminality a form specifics of organized crime, namely, of White Collar Crime. (Halili, 2011:211-212)

The author, E.H. Sutherland, in his work Is "White Collar Crime", finds the beginnings of the appearance of computer crime in the appearance of "white collar" crime at the beginning of the 20th century. 5 Other authors connect the beginnings of the appearance of computer crime

with the development of digital electronic computers, in the second half of the 20th century and their wide application in various areas of life, from where the first misuses with the help of computers began. 6 The first case presented, related to computer misuse

was recorded in 1958, while in 1966, the first case was recorded that the computer was used as a means of committing theft at a bank in Minnesota (USA). (Sumida: Computer crime, taken from the Internet: http://www.webnerds.com/computercrime/main.html).

3.2. Computer Crimes and Traditional Crimes

In looking at computer criminality, we note that these crimes can be committed for various reasons, starting from national security interests to financial espionage, financial theft, and personal revenge.

Unlike traditional crimes, computer crime is a global crime. These types of crimes are committed through computer spaces and networks and do not stop at conventional state borders. They can be prepared from anywhere and against a computer user anywhere in the world.

In addition to the increase in the rate of criminal activity in computer crimes, there is a tendency to avoid traditional categories of violations. When part of the categories consists in the use of information technologies to commit a traditional crime, computer crime can manifest itself as a new variety of activity, which cannot be followed by referring to the traditional categories of offenses.

The "Love Virus" case has proven this. Experts soon discovered the virus coming from the Philippines. Using information obtained from an Internet service provider, investigators from the Philippine National Investigation Agency and the FBI identified the persons suspected of distributing the virus. However, there were some problems with the investigation, due to the lack of specific laws, so creating and spreading a virus was not a crime. In this case, the investigators did not have enough time and opportunities to investigate, find evidence and convict the perpetrator.

The inadequacy of the current laws or their lack, to act on the new forms of anti-social activities, such as computer crimes, as well as the shortcomings of the existing criminal laws in this regard, create a permanent challenge for all the legislators of the world. On the other hand, offenders have the ability to exploit loopholes in the laws of their own countries, as well as others, to victimize citizens, thus remaining unpunished. In this sense, computer crime is a global crime. (wikipedia.org/wiki/Krimi_komputerik)

3.3. Categories of Perpetrators of Computer Crime

According to the author Sesion, the federal agency of US investigations has defined three categories of perpetrators or persons who misuse the computer for criminal purposes.

1. The First Category - consists of individuals who enter a foreign computer just to satisfy their desire or concern, to supposedly prove the skills they have associated with computer manipulation and use. These people are usually young and they want to be praised for the fact that they are able to do things with a computer. These people do not steal, do not destroy data, do not have material goals.
2. The second category of computer abusers consists of people who, in a planned and organized manner, hack into the systems and programs of other computers or computer centers, with the aim of destroying, fixing, changing the programs, etc. the centers and various computer programs are put out of action. These actions are taken not for material greed, but because of rivalry, envy, eventual competition, revenge, etc. The case of the I LOVE YOU virus mentioned above.
3. The third category - of the perpetrators of computer crimes is the one who undertakes these actions for the purpose of profiting and realizing material financial interests, etc. These in an unauthorized way enter programs and receive various data and notes that are considered secret or intimate. Then they materialize these notes by selling them or asking for large sums of money.

The perpetrators of these crimes are called HACKERS, while the act of penetrating the computer for profit is called HACKING. (Halili, 2011:213)

3.4. Features or Characteristics of Cybercrime as a Form of White Collar Crime

Computer crime has several features that distinguish it from other forms of criminality. These features are related to the following situations:

1. These crimes are committed at the speed of light and not in seconds as previously estimated (Rino 1999).
2. The presence of the perpetrator of computer-related criminal acts is not necessary at the place where the crime was committed.
3. Individuals as well as large economic and financial enterprises and corporations, institutions and research centers whether private or state, banks, stock exchanges, police, other military institutions and other entities in which usually security and secrecy are at the highest level.

Such cases are often called "computer terrorism" or "cyber terrorism".

4. The other feature of this criminality is that it is difficult to find out, that such perpetrators do not leave traces because there are rarely witnesses who verify the commission of this crime.
5. Research and studies on this type of criminality prove that the dark number of this criminality (cybercrime) is between 80 and 90%. (Halili, 2011:214)
6. The perpetrators of computer criminal offenses cannot be identified with the perpetrators of classic forms of criminality due to the specifics of this type of criminality.
7. These types of perpetrators of cybercrime must possess a relevant fund of knowledge and skills in the field of computer technology and forensic informatics. (Halili, 2011:214)

3.5. Computer Crime Reporting Forms

For the successful detection and securing of certain evidence, in addition to defining the notion of computer crime and processing its basic characteristics, the importance

special is the search for the forms of its presentation and their concretization in certain criminal acts.

There are different possibilities of computer abuse. They can be classified in different ways. One of the most widespread is that all abuses fall into these groups:

1. Changes,
2. Annihilations,
3. Publications,
4. Unauthorized uses or theft of data,
5. Alteration, destruction, unauthorized publication or theft of the program,
6. Damage and theft of computer system components,
7. Unauthorized use of computer or computer time. (Halili, 2011:214)

While the German author Hans Goppinger emphasizes that computer criminality only stands out in the commission of some crimes which he divides into several actions. First of all, I mention

1. Computer manipulations which are manifested through input-output manipulations.
2. The other action is the so-called computer espionage, which is carried out through certain programs, starting from games to various economic, financial and strategic programs, which bring great financial benefits to the perpetrators.
3. The other form is the so-called Computer Sabotage, which involves legal and illegal intervention in various computer systems and programs with the aim of disrupting, destroying or causing great material damage to their owners.

Likewise, the Italian criminologist Gian Luigi Pontiflet for the most frequent forms of crimes committed using the computer as a means of committing them. These crimes are most often:

1. Frauds,
2. Piracy
3. Theft of Programs,
4. Unauthorized access to programs,
5. Entry into private programs and disclosure of intimate private secrets,
6. Various other manipulations,
7. Political espionage, etc. (Halili, 2011:214))

So the numerous data let us know that many white-collar crimes are committed through the use of the computer. The most frequent crimes that can be committed through the computer are: computer fraud, manipulation of programs (input-output manipulation), piracy, theft of programs, unauthorized access to programs, entry into private programs and disclosure of intimate private secrets, political and industrial espionage, computer sabotage, etc. (Gashi. 2012:48)

3.6. Computer Fraud

Computer frauds are like the oldest forms of misuse of computer technology. Considering the number and place they have in the structure of this criminal phenomenon, they are the most dangerous social forms of computer crime. They usually consist of entering or recording incorrect data in order to provide myself or others with illegal financial benefits.

Computer fraud is possible in any economic system or other business in which the use of the computer information system can affect the progress of the distribution of goods and money. They are more numerous in the field of controlling the progress of financial capital and are usually presented in the form of frauds related to the business of bank accounting, frauds related to investments. related to insurance, frauds related to tax obligations, frauds related to the declaration of bankruptcy, frauds related to "money laundering".

3.7. Theft of Information

Theft of information is one of the frequent forms of computer crime.

The danger that this form causes is not small compared to those related to computer fraud. The technical possibilities for stealing information with the help of computers are very large.

Special forms of information theft are the illegal copying of home and personal computer programs, the theft and copying of computer equipment, as well as the theft of computer time. When people who otherwise have the legal ability to work with computer equipment, use their capacities and processing power for purposes that do not belong to their true dedication, we are dealing with the theft of computer time. The perpetrators of these crimes are mainly computer operators who abuse their workplace by taking activities for personal gain. (Latifi. 2009:338-339)

3.8. Computer Sabotage

The computer and the computer equipment can be attacked in different ways, starting from those that have a hooligan character, with the aim of revenge against former employees who have left their jobs, to terrorist attacks that are ready to destroy certain banks. data. Computer sabotage has two distinct forms:

1. Total or partial destruction, damage or disabling of the data processing mechanism.
2. Deleting, changing or preventing the use of data.

The most frequent cases of computer sabotage are those that attack the computer system and exploiting programs, especially those that serve as data banks located on the computer. The motives of such crimes are different and are brought about by revenge, concealment of fraud or any another form of cyber criminality, up to the desire to demonstrate the weaknesses of the system, etc.

3.9. Unauthorized Access to Computer Systems

As another form of misuse of computer crime that manifests itself as white collar crime is the unauthorized access to computer systems. This action consists in bypassing the skills of all protection mechanisms and entering the central computer system. The perpetrators of these crimes are usually Hackers, who want to publicly demonstrate their power and make the world aware of the weaknesses of the big ones.

3.10. Modification of Data or Programs

This category of criminal activities includes those types of unauthorized access to a computer system through the use of disruptive software. Unauthorized modification of computer data or functions, with the intention of erasing the normal functioning of the system, is a pure criminal activity and is often related to computer sabotage. It can serve as a means to gain economic advantages over a certain competitor, to promote illegal activity with ideological or terrorist motives, or to steal data or programs for extortion purposes. On one occasion, a computer operations supervisor at a New Jersey bank used a program to increase the account balances of some of his associates. His friends withdrew the money and then he destroyed the withdrawal trail. His plan was to stop the theft before the end of the audit period, to avoid detection. His friend, however, was too greedy to stop and forced him to proceed further. When auditors found a fraudulent transaction in the computer system's balance, they investigated to see who might have caused the discrepancies. The supervisor was the only one who had the ability to enter invoices. (wikipedia.org/wiki/Computer crime).

Conclusion

Despite the successes that have been achieved in terms of combating and preventing this type of white-collar crime, computer crime remains one of the most dangerous forms of underground crime (white-collar crime), presenting one of the challenges great for the bodies of detection, prosecution and judgment of its perpetrators.

Cybercrime is a persistent international evil that transcends national borders in a way that makes this form of organized crime a global concern. Cybercrime can take many forms, including online fraud, theft and cyber terrorism. Now one of the main reasons that facilitate the commission of such a crime is the globalization of technology and the revolutionary advances of Communication and Information Technology and, thus influencing criminal activity. Electronic and computer tools and equipment are increasingly being used to commit crimes.

Current trends show that in the future, computer crime will take place as the main object in the implementation of global policies to fight and prevent this form of organized crime, through the exchange of information, the increase in the level of human intellect, the coordination of legal efforts in national, regional and international levels, as well as the creation of a global network at a high level of cooperation between law enforcement agencies and institutions.

Reference

Elezi, Ismet. (1999). E drejta penale- pjesa e posaqme I dhe II. Tirane.(1999).

Gashi, Rexhep. (2012). Krimi i Jakës së Bardhë. Universiteti i Prishtinës, fakulteti juridik. Prishtinë.

Halili, Ragip. (2011). Kriminologjia, Universiteti i Prishtinës, fakulteti juridik. Prishtinë.

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

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

Latifi, Vesel. (2009. Kriminalistika, Universiteti i Prishtinës, fakulteti juridik. Prishtinë.

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.

Maloku, A. (2016). Karakteristikat dhe shkaqet e varferise ne Kosove. Regional Journal of Social Sciences REFORMA. Nr.4/(2016).pp.6-15.

Maloku, A. (2016). Karakteristikat e organizatave kriminale transnacionale. Buletini Shkencor Nr. 5 "DARDANIA. pp. 10-24.: Qendra Kërkimore Zhvillimore – Peja. Peje.

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

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.

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.

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.

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

Maloku, Ahmet, "DEVIANT BEHAVIOR OF JUVENILE DELINQUENTS" (2021). *UBT International Conference*. 76. https://knowledgecenter.ubt-uni.net/conference/(2021)UBTIC/all-events/76.

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.

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

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.

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.

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

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

Qerimi, I. ., Kastrati, S. ., Maloku, A. ., Gabela, O. ., & Maloku, E. . (2023). The Importance of Theory and Scientific Theories for the Scientific Study of Genocide in the Context of the Contribution to the Development of the Science of Genocide. *Academic Journal of Interdisciplinary Studies*, *12*(1), 183. https://doi.org/10.36941/ajis-(2023)-0016.

Vesel, Latifi. Ismet, Elezi dhe Vasilika, Hysi; (2012). Politika e Luftimit te Kriminalitetit.

Internet Resources

http://sq.wikipedia.org/wiki/Krimi_kompjuterik.

J.Sumida: Computer crime, marrë nga internet :http://www.webnerds.com/computercrime/main.html.

Copyrights