International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 5, Issue 11
November, 2022
Pages: 456-463

Cybercrime

Fitore Muqaj

LLM in Criminal Law, Peja. Republic of Kosova

Email: fitoremuqaj@gmail.com

http://dx.doi.org/10.47814/ijssrr.v5i11.789

Abstract

Considering the circumstances and the various challenges of contemporary societies, we have tried to present white-collar criminality as a fairly widespread phenomenon. By researching the literature of criminality, we have also come across this problem, where well-organized individuals and groups act under the guise of defenders of legality through state institutions and organizations, in order to enrich themselves or a certain group. Fighting this phenomenon is a challenge. Their activity is quite sophisticated and challenging for the investigative bodies. The organization and coordination of white-collar crime is usually done from influential people in the governing bodies of institutions and organizations. Since 1939, when the term "white-collar" was first coined, the doctrine has undergone changes and has advanced in the methods for discovering white-collar crime. Corruption and the actions of people in power, political parties, governmental and non-governmental institutions and bodies, including the unfair employment, licensing, tenders, obtaining documents and official permits for trade, education, police, army, parliament, governments, municipalities et cetera. This concept has to do with the upper layers of society. Involvement in these criminal actions is illegal, therefore it is the duty of the investigation and trial bodies that these people who misuse data and state duty are denounced and punished.

Keywords: *Cybercrime; Corruption; Data Misuse*

Introduction

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). This paper investigates the negative phenomenon of cybercrime as a form of criminality in contemporary society. According to research data and studies analyzed by various groups and national and international organizations, it appears that this phenomenon is very widespread and is a challenge in today's society.

Cybercrime - is spreading rapidly day by day, if we take into account the interference in official state software or private. Therefore, in addition to the positives that data digitalization and the Internet gives us, protective measures against piracy and hackers must be seriously considered.

The increase in crime brings fear to the public (Maloku, 2015). The rise of criminality in general and cybercrime 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 a large contribution to the fight against and prevention of criminality in their book Criminal Law and Procedure I and II. These are illegal actions carried out using various advanced technological tools and methods. The activity of certain individuals or groups of interest or even information technology professionals are aimed at obtaining data, manipulating data, including sabotage and terrorism, and in this category the aim is to sabotage the national security of a country.

Through hacker internet networks, criminal groups form their own action groups. Many countries are still faced with providing the legal doctrine, which would make it impossible to receive and process data for certain groups. The sophistication technology has made it increasingly easy for criminals to escape punishment, acting from places where such behavior or action is either not punishable or not prosecuted. They can also create the illusion for law enforcement agencies that they are in a foreign country where they cannot be prosecuted for such an act.

The creation of serious obstacles and access in an unauthorized manner to affect the operation of a computer system by software through the introduction, damage, exchange, alteration, deletion or suppression of data, is sanctioned according to the law. Different countries have defined this criminal offense in different ways. Some have only sanctioned the unathorized access, others have also sanctioned the destruction or learning of the contents of the information.

In today's world, individuals and organizations have a great use of information technology for the performance of daily work, such as the rapid use of information and the rapid exchange of data through the system. The term cybercrime is defined in two forms:

- In the narrow sense;
- In a broad sense.

In a narrow sense, cybercrime is any behavior carried out through electronic actions that are aimed at compromising the security of computer systems and the data processed by them.

While in a broad sense it represents any illegal behavior carried out by them from a computer or computer system, committing various crimes.

In recent times, we also have white-collar criminality, which represents a new form of organized and professional crime. The term for this form of criminality was first used by the criminologist and sociologist Edwin Sutherland.

In research, the use of computer technology is irreplaceable, but this spurt of development, in addition to bringing benefits to people in raising the overall well-being, unfortunately, the great opportunities offered by computer technology are being misused and exploited to carry out a number of crimes. This 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)

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.

Results and Discussion

1. The concept of computer crime as a form of organized crime

Criminality as a negative phenomenon is analyzed in many aspects. The authors Shabani and Maloku (2019) have elaborated exceptionally well in their book Sociology the sociological aspect. 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. The largest group includes individuals (hackers, etc.), who enter the system out of curiosity to see what they can do, without the intention of stealing data or software. Computer crime represents a negative phenomenon that appears in different ways different and from delinquent persons. Regarding this, the American criminologist L. Glick points out that the white-collar criminality is a new form of organized and professional crime and is primarily used in the field of economy. From the analysis done in the USA, over 30 billion dollars are earned from drug profits (Gashi, 2011:75). The studies done by different countries show that they have exceptional abilities for the use of advanced computer technology and action techniques in accordance with the development of the world economy. Investigations have shown that there are three groups of people involved in computer crime.

Organized crime has advanced in the scope of criminal activities. Their activity is done by staying in complete secrecy and hiding the traces (Latifi, 2011:257). Many authors and scientific researchers regarding the definition of cyber crime have the same definition: explaining that computer crime represents methods, without the intention of destroying data. Although at first glance this action seems harmless, it causes damage. Unauthorized use may also be related to the appearance of the virus.

The second group that attacks the computer system from the outside is the one that aims to attack the system and destroy data or software, introduce obstacles into the system, change data, destroy or disrupt the system. This group also uses the so-called malignant viruses, which have the task of destroying certain data in the system.

The third group enters the system to benefit from the use of the system. This group usually includes professionals who enter the system to perform various business transactions, to steal information, to spy, to manipulate data, to steal computer system time, etc.

Some countries such as the USA, Canada, Germany, Japan have created a legal structure with advanced personnel in terms of information technology that deal with the discovery and processing of data from different countries of the globe.

However, there are also some post-communist countries that have not yet started to fight these phenomena, and these criminal organizations take advantage of this loophole to acquire themselves by acting without being punished by the law enforcement agencies.

2. Forms of Computer crime

Looking at the size of the damage of cyber crime, experts rank it in the third place of criminality, right after drug trade and arms trade. In developed countries such as the USA, England, Canada, Germany, the legislation and research related to this criminal phenomenon, which has global dimensions, has also advanced. With all the heterogeneity of computer crime, like all other criminal activities in which information technology is applied, there are also different divisions of computer crime, including:

- Computer misuse - unauthorized access, disclosure of business and other secrets, data damage, hacking, espionage and computer espionage;
- Misuses with the help of the computer - the computer as a tool for committing computer fraud or computer forgery;
- Misuses made with computers - software piracy, computer pornography, offering goods derived from criminal acts.

2.1. Forms of criminal offenses committed through computer crime

The following acts are considered computer criminal activity:

- Thefts - theft of computers and computer parts, data theft, password theft, code theft;
- Fraud - fraud with insurance, taxes and duties, pension funds, social assistance, false presentations;
- Forgeries - forgery of basic accounting documentation, entry of fictitious invoices, entry of fictitious travel accounts, creation of fictitious payment lists, documents, value tokens, tokens for marking goods, money, signatures, seals, letters of value;
- Violation of privacy - accessing private computers via the Internet;
- Sabotage - physical and logical;
- Disclosure of state, military, business or official secrets;
- Espionage - publication of secret data, political activities of the rival, plans and military potential.;
- Coercion - through serious threat;
- Blackmail - through e-mail;
- Pornography - pictures, animations, files, child pornography;
- Propaganda - ideological, religious, nationalist, racist, terrorist, spread of fake news.

2.2. Offenses involving violent crime

Offenses involving violent crime are:

- Vandalism - physical or electronic destruction of the system or equipment;
- Terrorism - aimed at accounting centers, states;
- Murder - in the field of health through the change of patient and therapy data.

3. Comparisons of criminal offenses in the penal code of Kosovo with other legislations

Regarding the Penal Code of different countries, it is worth mentioning the Penal Code of Germany, where Article 202 provides punishment for those who bring to themselves or someone else data provided that they are not specifically dedicated and data that are protected from unauthorized interventions.

In 1990, England issued a special law to combat computer crime.

According to them, the concept of illegal and fraudulent behavior done on purpose and those without purpose is recognized. In Kosovo, the Criminal Code of Kosovo and the Law on Prevention and

Combating Cybercrime have been approved. The Criminal Code of Kosovo contains in article 327: "Access to computer systems" (KPK, article 327):

- Whoever, without authorization and with the intention of unlawfully obtaining financial benefit for himself or another person or causing harm to another person, changes, publishes, deletes, destroys, or destroys data or computer programs or in any other way enter another's computer system, shall be fined and imprisoned for up to three (3) years.
- If the criminal offense from paragraph 1 of this article results in financial benefit exceeding the amount of ten (10,000) euros or material damage exceeding the amount of ten (10,000) euros, the offender is sentenced to a fine and imprisonment of six (6) months to five years (5).

The Convention of the Council of Europe on the Cleansing, Detection, Seizure, and Confiscation of the proceeds of crime entered into force on September 1, 1993. The World Ministerial Conference "On Organized Crime" Naples 1995 approved the UN political declaration and the "Global Plan of Action Against Organized International Crime". (Latifi et al., 2012:194)

If the prevention of computer crime at the international level is not unified and harmonized, national laws present barriers to the capture of computer criminals and their punishment (Latifi et al., 2012:215).

So the security of information is related to the sovereignty of the state and the protection of values. A concrete case when the bust of a Soviet soldier was destroyed in the capital of Estonia, a massive computer attack on Estonian institutions followed, causing a complete chaos in the economy. The Minister of Defense of Estonia declares in the New York Times, "We are dealing with a situation when your ports are bombarded from the sea"

(www.nytimes.com/2007/05/29/technology/29estonia.html)

4. Measures to prevent cyber crime

The security strategy includes the prevention of computer crime attempts.

Today in the world there is the opinion that there is no degree of complete security, but only a degree of high reliability (trust systems). (Russell, 1991:106)

4.1 Administrative and organizational measures

These measures include some actions that are conditional on the planning of financial means to achieve a degree of reliability. This includes the calculation of expenses for the establishment of the application of the security policy, the calculation of damages in case of data loss, the assessment of damages since the data must be returned to their previous state.

4.2 Risk analysis

The program for maintaining security must be adapted to the strategy of what are the targets of the attacks and where the protection is offered, what are the weaknesses of the computer system, what are the possible countermeasures, who are the possible perpetrators, etc.

4.3. Legal protection in response to misuse of computer systems

Today, it is a global problem to cope with the rapid development of technology by countries that are faced with social transitions. In order to achieve an efficient protection, it is necessary to create

protection strategies according to international standards, to introduce new norms or to modify them in time.

4.4. Computer ethics and education

In raising the awareness about the risk of computer crime, the education of users plays an important role. Most importantly the development of moral norms on the use of computers and professional education.

4.5. International cooperation for preventing and fighting computer crime.

The action strategy against computer crime is understood as cooperation between countries, creating common standards. These actions derive from the OECD and other similar international organizations. (Russel, 1991:106)[9]

5. The global challenge of today's society against computer crime

Computer crime or computer fraud, with reason, should be treated as a global problem and the need for permanent cooperation of all subjects at all levels of the country, cooperation between the states of the region and the whole world should be emphasized. This should be done regardless of the geographical extent of the countries and their political system or other characteristics, such as the level of economic development, the level of technical preparation, etc.

Society must provide such an environment to create the belief that any fraud will be discovered sooner or later and the perpetrator will be brought to justice. This cannot be done by any country alone, but only with a well-coordinated action, at regional and wider levels, because the whole world enjoys the benefits of the achievements of computer systems, thus also the consequences of computer fraud.

Faced with this situation, it is very important for the law enforcement agencies to build global legal structures through the relevant international organizations, improving and structuring laws, changing them over time - because new advances in parallel to the development of information technology are a necessity in order to have a quick response for those who commit criminal acts.

In order to investigate computer fraud and criminal actions in general, at the state level, bodies that would monitor the situation in this field, analyze the phenomena, take initiatives, make suggestions and proposals. In this way, the causes and methods of committing such crimes would be investigated and then conclusions would be drawn and proposals would be made for taking measures and actions for the detection, witnessing and prevention of this type of criminal offenses.

Conclusion

This type of crime in today's society is taking large proportions, crossing not only national but also continental borders. Cybercrime can appear in different forms, including theft, fraud, sabotage, terrorism, etc.

The current trends of this social phenomenon show that cybercrime will take a leading place in global policies, for the identification, protection of data and the coordination of legal efforts at different national and international levels.

Various international conventions have established the necessary structure to fight these phenomena, but the independence of some countries is missing or is under development.

There is a need to provide access to modern technology and professional training for the Police, and organizations that protect data or prevent criminal actions, and that have knowledge in pursuing cybercrime. Cybercrime cannot be fought without modern infrastructure and professional training that teaches how to effectively obtain and classify the evidence with which the criminal offense is committed.Research is also significant for social practice and practical reasons such as controlling and properly preventing crime. (Maloku, et al., 2022:172)

References

1. D. Rusel, G.T. Ganggemi. ((1991). Computer Secuty Basics. O'Reakly & Associates Inc.Cambridge.
2. Ejup, Sahiti. Rexhep, Murati. dhe Xhevdet Elshani. (2014). Komentar Kodi i Procedurës Penale. Prishtinë.
3. Elezi, Ismet. (1999). E drejta penale- pjesa e posaqme I dhe II .Tirane.1999.
4. Ismet, Salihu; Hilmi, Zhitija; dhe Fejzullah Hasani. (2014). Komentari Kodit Penal të Republikës së Kosovës. Botimi i parë. Prishtinë.
5. Jasarević, O., Maloku, A. (2021). *Kriminologija (etiologija i fenomenologija kriminaliteta*). Universitet u Travniku. Travnik. Bosna i Hercegovina.
6. Jasarević, O., Maloku, A. (2021). *Krivično procesno pravo I dhe II (opšti i posebni dio).* Universitet u Travniku. Travnik. Bosna i Hercegovina.
7. Kodi i Procedures Penale së Kosovës.
8. Kodi Penal i Republikes së Kosovës.
9. 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
10. Maloku, A. (2016). (2016). Karakteristikat dhe shkaqet e varferise ne Kosove. Regional Journal of Social Sciences REFORMA. Nr.4/2016.pp.6-15.
11. Maloku, A. (2016). Karakteristikat e organizatave kriminale transnacionale. Buletini Shkencor Nr. 5 "DARDANIA. pp. 10-24.: Qendra Kërkimore Zhvillimore – Peja. Peje.
12. Maloku, A. (2019). *Fjalor i terminologjik i viktimologjisë*. Kolegji Iliria, Prishtinë.
13. 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
14. 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
15. 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.
16. Maloku, A., Maloku, E. (2021). *Fajlor i terminologjisë juridiko-penale për gazetarë*. Kolegji Iliria, Prishtinë.

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

18. 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.

1. Ragip Halili. (2016). Kriminologjia. Universiteti Prishtinës. Fakulteti Juridik. Prishtinë.

19. Ragip, Halili. (2007). Viktimologjia. Prishtinë.

1. Rexhep, Gashi. (2011) Krimi i Organizuar. Universiteti Prishtinës. Fakulteti Juridik. Prishtinë.

20. Sahiti, Ejup dhe Murati, Rexhep. (2013). E drejta e Procedurës Penale. Prishtinë.

21. Sesion.W. (1991). Kompjuterski kriminal-trend koji eskalira.Zagreb.

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

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

24. Tierny, J. (1966). Criminology -theory and context. New York.

25. Vesel, Latifi. (2000). Kriminalistika. Prishtine.

26. Vesel, Latifi. (2009).Kriminalistika-zbulimi dhe të provuarit e krimit, botimi i gjashtë, Prishtinë.

27. Vesel, Latifi. (2011) Kriminalistika. Universiteti Prishtinës. Fakulteti Juridik. Prishtinë.

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

Copyrights