The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 04 ISSUE 10 Pages: 43-50
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215)
OCLC – 1176274523 METADATA IF – 7.659
Publisher: The USA Journals

Journal Website: https://theamericanjournals.com/index.php/tajpslc

Research Article

THE CONCEPT, TYPES CRIMES COMMITTED USING THE INTERNET NETWORK

Submission Date: October 15, 2022, Accepted Date: October 25, 2022,
Published Date: October 30, 2022 |
Crossref doi: https://doi.org/10.37547/tajpslc/Volume04Issue10-06

Turaev Sardor Abdukhakim Ugli
Doctoral Student Of Tashkent State University Of Law, Uzbekistan

ABSTRACT

The article highlights issues related to the concept of crimes committed by the author using the Internet, and their characteristics. It also analyzes the criminalization of socially dangerous acts related to the illegal use of information technologies, the need for deep study and effective use of foreign experience in combating these crimes and their prevention, implementation of international law, further improvement of national legislation. In addition, the author lists the features of the development of information and communication means of this type of crime, such as the creation of an animated version of real life - the virtual world, the relative ease of committing crimes in the virtual world. The author tried to distinguish this type of crime from other crimes, using his views and theoretical sources. In turn, the author points out that the number of crimes committed using the Internet is growing rapidly both in quantity and quality, and, accordingly, the need for constant improvement of the legal framework to combat these crimes, and the author also discussed the views of various researchers on this area.

KEYWORDS

Information technologies, digital economy, computer crimes, virtual world, internet, information warfare, cybercrime, cybersecurity, viruses, malware.

INTRODUCTION

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 04 ISSUE 10 Pages: 43-50
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215)
OCLC – 1176274523 METADATA IF – 7.659
Publisher: The USA Journals

The Decree of the President of the Republic of Uzbekistan "On the Strategy of Actions for the further development of the Republic of Uzbekistan" dated February 7, 2017 defines the improvement of administrative, criminal, civil and economic legislation aimed at increasing transparency and efficiency of ensuring human rights and freedoms, the state of economic development, based on modern requirements, international standards., it is also planned to develop a "Concept for improving criminal and criminal procedure legislation for 2018-2021", providing for the broad involvement of information and communication technologies[1].

Information and related regulation of the informatization process plays a special role in the formation of a humane, legal democratic state and civil society. Moreover, in the "age of global informatization and computerization", along with world inventions, such huge problems as computer crime, threatening information security, also penetrate into the life of mankind. Innovations in the field of information technology have made awareness of these areas an urgent problem.

It is noteworthy that when carrying out criminal intentions, computer technology is always used as the main object and means of committing a crime.

Exactly, with the development of a particular sphere of public life, there are those who want to use new technologies and secretly satisfy their needs. This, in turn, leads to the commission of a new type of criminal activity - crimes in the field of information technology. This crime has reached a fairly high level at the present stage. For example, according to the British analytical company - LITS, in 2013, the damage caused to the global economy by computer crimes amounted to 132 billion. In 2012, this figure amounted to $48 billion. in 2014, economic and material damage from computer crimes amounted to $ 411 billion, and in 2015 - about 687 billion. It rose to the US dollar. These statistics indicate an annual increase in material damage from crimes in the field of information technology. The fact is that with the improvement of computer technology, the probability of committing related crimes with dominance increases.

Until recently, computer crime in the Republic of Uzbekistan was considered a phenomenon characteristic only of developed foreign countries, and due to the insufficient computerization of our society, there were no such crimes. But at the same time, the situation in our country is different. The computerization of society, affecting almost all aspects of the activities of people, enterprises, organizations and the state, has given rise to a new sphere of public relations. This sphere, unfortunately, in most cases becomes the object of inhumane acts. A computer information system representing the situation in various sectors of the economy, as well as an objective perception of the country's defense capability, is in dire need of means to ensure legal security against unauthorized penetration into this system by criminal elements capable of causing enormous financial and material damage. Taking into account such circumstances, in the Law of the Republic of Uzbekistan dated November 30, 2007 "On amendments and additions to certain legislative acts of the Republic of Uzbekistan in connection with increased responsibility for committing illegal actions in the field of informatization and data transmission" dangerous acts related to the illegal use of computer systems are defined as crimes, and the current Criminal Code is supplemented with a new chapter XX1 "Crimes in the field of information technology". This chapter is included in the sixth section of the special part of the Criminal Code entitled "Crimes against public safety and public order".

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 04 ISSUE 10 Pages: 43-50
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215)
OCLC – 1176274523 METADATA IF – 7.659
Publisher: The USA Journals

Criminalization of socially dangerous acts related to the misuse of information technologies requires at the same time the study of the legal content and essence of concepts related to both elements of information relations and relations regulated by criminal law.

The appearance of a new chapter in the Criminal Code of the Republic of Uzbekistan on crimes in the field of information technology, on the one hand, poses a task for law enforcement agencies to uncover and investigate these types of crimes.

Considering that crimes committed on the Internet have penetrated the criminal legislation of our country, one of the problems being solved today is a deeper study and effective use of the experience of foreign countries in combating these crimes and preventing them. In the light of the above, it can be noted that the degree of reflection of the issue of crimes in the field of information technology in the legislation of the Republic of Uzbekistan and the definition of the distinctive (positive and negative) sides of these norms from the norms established by the legislation of foreign countries, the need to implement the norms of international law, further improvement of the system of national legislation, as we believe, indicate the relevance of this topic.

The development of information and communication tools has given rise to an animated version of real life - the virtual world. Now the peculiar life of the virtual world has already flared up, in which people "began to live". Today, crimes committed using the Internet have become widely publicized and have become a serious threat to the interests of States and societies.

The improvement of the Internet, the increasing popularity of various social networks in the life of society, in turn, expand its capabilities, as well as increase the social danger of crimes committed in connection with it. In particular, the growing capabilities of the Internet to work with official documents make it difficult to ensure information security, create new types of offenses with official documents that are not provided for by law. Today, information warfare is becoming more dangerous than any nuclear war. Taking into an account the above, it is necessary to focus separately on the concept of a crime committed using the Internet.

In accordance with the Regulation "On the procedure for the preparation of information resources of the Republic of Uzbekistan and their dissemination in data transmission networks, including on the Internet", information security is the state of protection of the interests of the individual, society and the state in the information sphere [2]. In addition, a number of experts in this field have also expressed their opinion on the essence of this expression in their scientific research. In particular, some experts define it as "information security - the state of security of the information environment of society, ensuring its formation, application and development in the interests of citizens, organizations and the state" [3].

It is worth noting that an impartial view of crimes committed using the Internet creates a number of problems. In this regard, the situation in Kyrgyzstan, the Republic of Tajikistan can be noted. Khilyuta V.V. reported that in 2013, 174 crimes were detected in the credit and banking sector in the Kyrgyz Republic, of which more than 60% had signs of fraud using the Internet [4]. In Kazakhstan, 17 cases of the above crimes were also detected in 2012. In fact, in order to prevent the occurrence of such situations, the law "On National Security" was adopted in Kazakhstan on June 26, 1998, which clarified the concept of information security [5]. The victims of crimes are usually enterprises, organizations and institutions in which

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 04 ISSUE 10 Pages: 43-50
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215)
OCLC – 1176274523 METADATA IF – 7.659
Publisher: The USA Journals

automated computer systems are used when working with accounting documents, making payments and other transactions. The target of criminals in most cases are banks.

At the XI UN Congress devoted to the problems of crime prevention and Criminal justice, held in April 2005, special attention was paid to crimes committed using the Internet and the Internet. At this Congress, the Bangkok Declaration on the specifics of cybercrime and the need to develop an integrated approach to combating it was adopted.

For modern society, which is unthinkable without the Internet and information technologies, the fight against crimes committed via the Internet is a top priority. A.S.Belorusov rightly notes that social surveys, court materials and observations of scientists indicate that the world community is facing a serious problem in this area, and cybercrime in developed countries is measured by thousands of crimes, and its economic damage is billions of US dollars [6].

In addition, the situation is aggravated by the fact that the legislation and the state system do not have a perfect mechanism for combating computer crime [7]. Taking into an account the role of computer information systems in the life of society, the increasing scale of their use and processing, the growing number of users of the global Internet, the intensive introduction of computer networks and systems into the activities of public administration in this area, there is such an urgent problem as the protection of these systems and information from criminal encroachments.

Crimes committed using the Internet are not only one of the criminal groups that encroach on criminal legislation in the field of security of preparation, use and dissemination of computer information, information resources, information systems and technologies in criminal law, but also cover the objective side of the crime along with other crimes that can be committed on the Internet [8]. Crimes using the Internet are not only the robbery of someone else's property, but also the spread of electronic viruses and other criminal acts, as well as crimes directed against a certain person.

Only in the Russian Federation alone, from two to ten new viruses are launched monthly. In 2010, a study of computer viruses revealed that viruses caused about $10 billion in damage. June 8, 2010 in the "B B C World News" notes that 45 million computers were affected by the "love" virus, include ng the Pentagon, the FBI and the British government. The damage from this virus amounts to $8.75 billion [9].

For the first time, the definition of computer crime was presented at the American Bar Association conference in Dallas in 1979 under the title "Using or attempting to use a computer, computer system or computer network to obtain money, property or services under false pretexts and false promises or by pretending to be another person; intentional commission of actions that are not permitted for the purpose of changing, damaging, damaging or stealing a computer computing system, computer networks or programs of the mathematical support system contained therein, or data [10]".

As of now, the composition of crimes committed using the Internet has significantly increased and now crimes against the individual are also committed by means of them. The game form of this crime, known as the "Blue whale", has become very popular in recent years.

It should be noted that the opening of only one percent of the crimes committed using the Internet, on average, also confirms our word. V.A.Nomokonov

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 04 ISSUE 10 Pages: 43-50
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215)
OCLC – 1176274523 METADATA IF – 7.659
Publisher: The USA Journals

noted that crimes committed using the Internet network are growing rapidly, noting that in 2020 in the Russian Federation, such offenses were committed more than seven and a half thousand times more than in 2019 [11], noting that the situation in other countries is the same[12]. The information presented shows that crimes committed using the Internet network are growing rapidly both in quantity and in quality, as well as the need for constant improvement of the legislative base in the fight against these crimes.

In the study of internet network crime as a manifestation of crime, the researchers express different opinions. M. Baturin argues that: "crimes committed using the Internet are not legally a separate group of crimes, but it is desirable to talk about aspects of crime related to the Internet, since traditional crimes are modified to the account of the Internet network [13]".

A. N. Karakhanyan understands Internet crimes committing by using of Internet are the illegal actions that are the object or means of committing crimes using the Internet [14]. In fact, crime in the Internet network has a number of specific characteristics, which makes it possible to generalize them into a separate group of crimes: 1) the diversity of the object of aggression; 2) the manifestation of computer technology and information as an object of crime and at the same time as a method of committing a crime; 3) the variety of the subject and methods of the criminal offense; 4) the manifestation of a computer connected to the Internet as a subject of crime or as a means of committing a crime [15]. V.A.Milashev also notes that, having filled the above opinion, the possibility of committing a misdemeanor action without standing on the Internet, the urgency of committing a crime and the ability to ensure the confidentiality of one's identity allow this crime to be active in recent years [16]. In this sense, it is worthwhile to separate the internet crime into a separate group.

Among the crimes committed using the Internet network, the robbery of the property of other persons using the Internet takes a special place. The share of these crimes in the Computer Crime system is immense and it is desirable to start their research from the computer crime classification, which is important for a clear understanding of the position of these crimes in the Computer Crime system. A.A.Ortikov, A.T.Isakhodzhaev and A.V.Shestakov notes that these crimes are classified as follows: 1) physical abuse (violation of inventory, loss, destruction of programs or information, and etc.); 2) operational abuse (fraud, use of computer data without sanctions); 3) software abuse; 4) electronic abuse [17].

Sudanese expert Mudavi Mukhtar, dwelling on this issue, emphasizes that in some cases, crime on the Internet, called cybercrime, is a serious problem, and distinguishes between two categories of crimes on the Internet: a) crimes in which the network is used as a means of facilitating criminal activity; b) crimes in which a computer is used to steal or hack information, attack a bank, commit illegal monetary transactions, steal credit card numbers, as well as as a weapon of crime [18].

English scientist N. Batley, however, distinguishes between two types of Internet crimes: in the first, the Internet is considered as an object of crime, and in the second - as a means of crime. In the first case, it is a hacker attack and the spread of various viruses and malware, etc.; in the second case, the transfer of pornographic products and illegal computer programs, fraud on the Internet in order to appropriate someone else's property, as well as the legalization of illegally obtained income [19].

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 04 ISSUE 10 Pages: 43-50
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215)
OCLC – 1176274523 METADATA IF – 7.659
Publisher: The USA Journals

The US Department of Justice has identified the following types of computer crimes: robbery of other people's property using the Internet, computer fraud, penetration into a computer system for the purpose of unauthorized modification or distortion of the information contained therein, illegal access to computer systems and databases.

Crimes in the field of information technology is an illegal socially dangerous act that poses a threat to information security, committed directly by means of computer technology or by means of information technology. In such cases, the information of an electronic computer, computer, computer system or computer network is meant as the subject of a crime, instrument or means of committing a crime. In most cases, this term is also referred to as "computer crimes".

There are so many types of computer crime that scientists have not yet come to a definite conclusion about this. In particular, Y. M. Baturin and A. M. Zhodzinsky [20] listed the following main types of crimes directly related to computer technology: 1) unauthorized access to computer information; 2) access to the "logic bomb" software, which contributes to the partial or complete failure of the computer system under certain conditions; 3) the spread of computer viruses; 4) criminal actions in the use, preparation and production of software systems; 5) forgery of computer information; 6) theft of computer information.

According the criminal legislation of the Republic of Uzbekistan, a separate chapter XX1, including 6 articles, is devoted to these crimes.

The modern realities of social progress, the transition of technological processes to electronic means management methods, the giving of legal force to acts carried out using computers have also created conditions for the use of these processes to commit crimes in the field of information technology. Illegal interference in the operation of components of telecommunication networks, computer programs operating in their environment, illegal modification and destruction of computer information can disrupt the operation of the most important elements of the state infrastructure and lead to the death of a large number of people, causing significant property damage or other socially dangerous consequences.

The Criminal Code of the Republic of Uzbekistan provides for such crimes as article 103 (incitement to suicide), article 1031 (assisst to suicide), article 1881 (illegal activity to attract funds and (or) other property), article 2441 (production, storage, distribution or demonstration of materials threatening public safety and public order), Article 278 (organization and conduct of gambling.

Similarly, computer information is the subject of information technology crimes committed on the Internet. For example, such circumstances are explicitly stated in the dispositions of Articles 2781, 2782, 2784 and 2786 of the Criminal Code. In other cases, the establishment of the subject is associated with the identification of other elements of the corpus delicti (Articles 2783 and 2785 of the Criminal Code).

The creation of a worldwide information network - the Internet, which unites representatives of almost all countries of the world, allows you to commit an act even far from the place of occurrence of harmful consequences. In such cases, Russian researchers Y. I. Lyapunov and A.V. The place of the crime is understood to be the territory of the state in which the act was committed, regardless of where the place of the consequences is located.

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 04 ISSUE 10 Pages: 43-50
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215)
OCLC – 1176274523 METADATA IF – 7.659
Publisher: The USA Journals

Foreign criminological studies have established that 52% of persons committing crimes on the Internet are persons who have received special training in the field of computer information processing; 97% are employees of state organizations and institutions using the Internet and information technologies in their daily activities; 30% are providers directly related to the operation of computer equipment.

CONCLUSION

In conclusion, we can say that the circle of persons committing crimes using the Internet is relatively wide. As can be seen from the results of the study, the subjects of the crime can be persons of all ages, from representatives of the most diverse strata of society, from 16 to 60 years old, with a level of training - from inexperienced to specialists or with minimal knowledge in the field of computer technology.

REFERENCES

1. Decree of the President of the Republic of Uzbekistan dated February 7, 2017 No. PF-4947 "On the Action Strategy for further development of the Republic of Uzbekistan". Collection of Legislation of the Republic of Uzbekistan, 2017, No. 6, Article 70.
2. Annex to the Resolution of the Cabinet of Ministers of the Republic of Uzbekistan dated March 26, 1999 No. 137. // Collection of normative and legal documents on information and informatization. - Tashkent: Adolat, 2008. - P. 107–110.
3. Muhammadiev A. Protecting the interests of the individual, society and the state from the impact of poor-quality information, violations of the order of dissemination of information. State and law: a scientific-theoretical journal. 2003, №2 (14). - P. 85.
4. Khilyuta V.V. Forensic problems in the investigation of banking fraud. ... diss. for the degree of Cand. jurid. sciences. - Minsk, 2004. - P. 2.
5. Law of the Republic of Kazakhstan "On National Security". // Normative acts. - Almaty: Ayan Edet, 1998. - P. 47.
6. Belorusov A.S. Some aspects of the investigation of computer crimes // Collection of scientific papers of the international conference "Information technology and security". Issue 3. - Kiev: National Academy of Sciences of Ukraine, 2003. - P. 13-22.
7. Baranov O. Digital legislation // Dzerkalo tyzhnya. - No. 20 (395). - 1-7 worms 2002 p.
8. Legal encyclopedia / Ed. ed.: B.N. Topornin. - M .: Jurist, 2001. - P. 849
9. Konyavsky V.A., Lopatkin S.V. Computer crime. In 2 volumes. Vol. 1. - M .: RFK - Image Lab, 2006. - P.109–187.; N.N. Bezrukov Computer Virology. - Kiev, 1990. - P. 185
10. Criminal law. Special part: Textbook for universities. Resp. ed .: Doctor of Law, prof. I.Ya.Kozachenko, Doctor of Law, prof. Z.A. Neznamova, Ph.D., Assoc. G.P. Novoselov. - M .: HOPMA, 2000. - P.554-555
11. Crime in Russia at the beginning of the XXI century and the response to it. - M., 2004. - P. 104.
12. V.M. Nomokonov New information technologies in the fight against crime: www.crime.vl.ru.
13. Baturin Yu.M. Computer law problems. - M .: Jurid. lit., 1991. - P. 27
14. Some aspects of computer crime // Problems of crime in capitalist countries. M.: VINITI, 1990. - No. 6. - P.12-13.
15. Selivanov N.A. Problems of Combating Computer Crime // Legality. - No. 8. –1993.– P.36–40

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 04 ISSUE 10 Pages: 43-50
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215)
OCLC – 1176274523 METADATA IF – 7.659
Publisher: The USA Journals

16. Milashev V.A. Problems of tactics of search, fixation and removal of traces in case of illegal access to computer information in computer networks. Abstract of thesis. diss. for the degree of Cand. jurid. sciences. - Moscow, 2004. - P. 3
17. Ortiqov A.A., Isaxodjaev A.T., Shestakov A.V. The Secret Economy: A Textbook. / Responsible editor yu.f.d., prof. U.Tadjixanov. - Tashkent: Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, 2002. - P. 148–149.
18. Mukhtar M. Cybercrime. // Vladivostok Organized Crime Research Center: www.crime.vl.ru.
19. Batley N. Computer crime: Per. to the whale. the language of Hao Haiyan. Publishing House of Liaoning Education, 1998.
20. Baturin Yu.M., Zhodzinsky A.M. Computer crime and computer security. - M., 1991. - P. 11-19