ISSUES OF LIABILITY IN THE CRIMINAL CODE OF FOREIGN COUNTRIES FOR LOOTING THE PROPERTY OF OTHERS USING COMPUTER TOOLS

Yodgorov Muhammad Furqat o'g'li
Tashkent State Law University Specialized Branch of Criminal Law Lecturer in the Department of Science

Mamanazarov Orzumurod Muhammadnazar o'g'li
3rd Year Student of the Specialized Branch of Tashkent State Law University

Annotation
This article discusses the concept of the crime of looting the property of others, which is one of the most common crimes in international criminal law and the largest in terms of the amount of damage, its social danger, what documents have been adopted in the fight against this crime. the criminal code of national and foreign countries covers issues of liability

Keywords: Information terrorism, Information crime, use of a dominant position in the information space to harm the interests and security of other states, computer crime, personal data.

Criminal use of information and information technology is the world today is becoming one of the biggest problems facing the community. If you go into the field, each other you can meet close crimes. For example, it is a member state of the Shanghai Cooperation Organization Governments signed on June 16, 2009 "On Ensuring International Information Security" In the transaction, we can find "information crime" and "information terrorism". Crimes in this area the issue of prevention and punishment is of particular importance in the legislation of each state. Combating crimes in the field of computer technologies in most countries of the world despite the fact that the legal foundation of the issues has been created, the current information environment does not support this system in the legislation
requires revision. One of the main reasons for this is computer crime is increasing.
The biggest threats to information security are political relations, national security, defense and society It is felt in the aggressions carried out in other important areas of the political sphere. Today society's information security, especially on the global

Internet, chaos to people's lives, serious related to attacks that may cause panic, chaos, and information attacks is facing trials. As an example, in some countries of the former Soviet territory - Georgia, Ukraine, Kyrgyzstan (Tulip and Orange Revolutions), North Africa and the Arab Spring in the Middle East we can bring tragic events. The growth of crime is international, leaving the territory of one country several international organizations focused on the fight against crime caused it to come into existence.Today, data protection is international and state level provided by legal acts, directly related to the computer in many developed countries Laws regulating crimes are in force. Information and computer crimes The first regulatory document adopted in the field was adopted in 1978 in the US states of Florida and Arizona "Computer crimes" act.

About the object of crimes in the field of information technologies and security in scientific literature there is no single opinion, the complexity of the problem lies in the criminal legislation of foreign countries It is also based on the different interpretation of concepts. Most countries in the legislation, crimes are reflected in the form of computer crime. For example, the Russian Federation, In the Criminal Code of Kyrgyzstan and Kazakhstan, responsibility for these crimes is defined as "Computer" Crimes in the field of information", this chapter is against public security and public order included in the crime department.

"Computer information security" in the Criminal Code of Armenia "Crimes in the field of computer science" in the Criminal Code of Moldova in the chapter "Crimes in the field of computer science" if caught, in the Criminal Code of the Republic of Tajikistan, in the chapter "Crimes against information security".

given Crimes in the field of information are in a separate chapter in the criminal legislation of some countries not shown. According to the Criminal Code of the People's Republic of China, "Against public order and administrative order "Crimes" chapter contains only some articles that define liability for computer crimes.For fraud committed using a computer in the Criminal Code of the Republic of Korea liability is defined in one article.

Studying the criminal legislation of foreign countries in the field of computer technologies divides crimes into the following groups.

1) illegal acquisition and seizure of computer equipment and data carriers,
crimes aimed at destruction or damage;

2) illegal use of computer information, modification, creation of virus programs
crimes aimed at output, use or distribution;

3) computer and other computer equipment as a weapon or means of committing a crime aimed at using, exchanging information or entering false information into the computer system allows to distinguish crimes.

UK law specifically deals with computer crime through. In particular, "On sexual crimes" adopted in 1956 and in 1978 from computer technologies in accordance with the laws "On Child Protection". Persons who prepared and distributed pornographic images usingmust Also, "On Telecommunications" adopted in 1984 and adopted in 1990

Acts "On misuse of computer" also refer to computer crimes are the main documents determining responsibility. This is also the act "On personal data"is of great importance. "On Electronic Communications", "On Terrorism". Acts areillegal use of a computer, unauthorized access to a computer network or system

and caused great damage as a result of illegal use of computer information or was introduced in order to bring responsibility for cases aimed at terrorist goals.

Computer crimes sanctioned by the French Penal Code can be divided into 3 categories:

1) crimes against a person committed using a computer;

2) crimes against property committed using a computer;

3) crimes against the interests of the nation and the state committed using a computer.

French criminal law is the criminal law of some foreign countries, while Uzbekistan is a criminal law

contrary to the law, it is not only for individuals, but also for committing crimes

determines the issue of criminal liability for legal entities found to be

Provisions on crimes in the field of information technologies of the Luxembourg Criminal CodeIt is mentioned in Articles 509-1, 509-2, 509-3, 524. Article 509-1 of the Luxembourg Criminal Code unauthorized access to the system or part of the data transmission system and illegal access to such system assumes responsibility for use. The penalty for this crime is a fine or two months shall be given in the form of deprivation of liberty for a period of time. If these actions change the data in the system if it leads to change or destruction, the upper limit of the prison term is increased to 2 years. Article 509-2 to prevent or change the operation of the automatic data transfer system forbids. Violation of the norm is punishable by a fine or imprisonment from three months to three years is used.

Provisions on crimes in the field of information technologies of the Luxembourg Criminal Code It is mentioned in Articles 509-1, 509-2, 509-3, 524. Article 509-1 of the Luxembourg Criminal Code unauthorized access to the system or part of the data transmission system and illegal access to such system assumes responsibility for use.

The penalty for this crime is a fine or two months shall be given in the form of deprivation of liberty for a period of time. If these actions change the data in the systemif it leads to change or destruction, the upper limit of the prison term is increased to 2 years. Article 509-2 to prevent or change the operation of the automatic data transfer system forbids. Violation of the norm is punishable by a fine or imprisonment from three months to three years is used.

Article 509-3 of the Luxembourg Criminal Code to protect the integrity and quality of data directed. This norm applies to the system of processing electronic information intentionally and without appropriate authority entering information, deleting or changing information stored in this system, system orcriminal prosecution of a person working with the method of data transmission is mentioned.According to Article 524 of the Luxembourg Penal Code, any telecommunications serviceinterference is a crime punishable by a fine or imprisonment from 1 month to 3 yearsis considered US computer crime legislation is unique and permanent differs in that it is updated. The United States Computer Crime Act of 1986 was developed in 2010 and is called "Computer Fraud and Abuse". Later, the "crime of computer fraud" was included in the US code of laws. Code section 1030(a)(4) defines computer fraud as any crime of value from 5 thousand US dollars during the year using a computer for the purpose of owning something excessive, illegal use of the computer system, that is, the computer server and connection system liability is set for free use.

In the USA, in 2002, the Federal Information Security Management Act (FISMA) security act has been adopted. According to this law, three organizations: health organizations, that financial institutions and federal organizations must protect their systems and information defined. In 2003, California passed the Security Breach Act, which Strengthened protection of personal data of California citizens.

In 1993, the adoption of a special law "On computer crimes" in the Netherlands strengthened the fight against crimes in the field of information technologies. Netherlands. The Criminal Code is filled with a normative base based on this law. of the Dutch Criminal Code One of the most important features of the legislator in the field of computer crime in explaining the terms. In particular, in Article 80 of the Dutch Criminal Code, "information", The meaning of terms such as "computer devices and systems" is disclosed.

If we dwell on the legislation of the Russian Federation on crimes in the field of computers, in order to regulate this field, the Russian Federation "Legal protection of electronic programs on" law was adopted. Also, "On Information" No. 24 of February 20, 1995 federal law was adopted.

Chapter XII of the Criminal Code of Tajikistan "Offenses against information security" named, and in its articles 298-304, it is criminal for crimes against information security responsibilities are defined. In particular, Article 298 of the Civil Code of Tajikistan states that "it is illegal to access computer information access to the information stored in the computer systems entry - a fine in the amount of two hundred to four hundred times the minimum monthly salary or two with deprivation of liberty up to 10 years, as well as damage to information systems, its operation obstruction - a fine of three hundred to five hundred times the minimum wage or two with correctional work for up to 10 years or with deprivation of liberty for the same period, from this in addition, if the actions seen in the above two cases are caused by carelessness and have serious consequences when brought - a fine in the amount of four hundred to seven hundred times the minimum monthly salary or shall be punished by imprisonment for up to three years. Seeing as it stands, computer information is illegal in all CIS countriesuse is not sanctioned as a separate norm. Only Russia, Azerbaijan, Georgia, such crimes are sanctioned separately in Tajikistan, Ukraine and Uzbekistan.

REFERENCES

1. Constitution of the Republic of Uzbekistan. - T., 2018. - 74 p.
2. Criminal Code of the Republic of Uzbekistan. - Tashkent: Adolat, 201. - 480 p.
3.Law of the Republic of Uzbekistan dated December 11, 2003 No. 560-II "On Information".
4. Law of the Republic of Uzbekistan No. 371 dated May 14, 2014 "Crime Prevention on" Law.
5. The President of the Republic of Uzbekistan on February 7, 2017 "More the Republic of Uzbekistan
"Decree on the Strategy of Actions for Development" // People's word. – 2017. – February 8.
6. Council of Europe "Convention on combating cybercrime" 23.11. 2001.
7. "On cooperation in the fight against crime in the field of computer information" of the CIS Agreement". Minsk. 1.06.2001.
8. SCO Agreement "On Ensuring International Information Security" dated June 16, 2009.
9. Rasulev A.K. "The crime of combating crimes in the field of information technology security improvement of legal criminological measures" Diss. Aftoreferat. T-2018.