European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.05.213

ISCKMC 2020

International Scientific Congress «KNOWLEDGE, MAN AND CIVILIZATION»

CORPUS DELICTI CHARACTERISTICS PROVIDED BY THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

Gilyana Vladimirovna Tsebekova (a)*, Vladimir Vasilyevich Basanov (b)
*Corresponding author

(a) Kalmyk State University named after B.B. Gorodovikov, 11, Pushkina str., Elista, Republic of Kalmykia, Russia, tsebekova_gv@mail.ru,
(b) Kalmyk State University named after B.B. Gorodovikov, 11, Pushkina str., Elista, Republic of Kalmykia, Russia, kafedra_pd@bk.ru

Abstract

The elements of such corpus delicti as cyber fraud (Article 159.6 of the Criminal Code of the Russian Federation) were studied in detail and key features were considered in the paper. The reasons for identifying a special type of fraud, as well as the presence of classification problems were analyzed. The paper considers the possible existence of an objective need to delineate the method of theft of the property of another or acquisition of the right to someone's property by entering computer information from other methods of cyber fraud as a separate method of theft, or it is an integral part of one of the already known methods. The disposition of Article 159.6 of the Criminal Code of the Russian Federation presents methods of cyber fraud, which are mandatory signs of this crime, provided for in the considered article. It is important to note that we face a new form of stealing when dealing with cyber frauds, but without the direct fraud as such related to fraud or abuse of trust. To date, actions and concepts that are related to distortion, introduction or other processes that will change the conditions for information storage facilities, or will be related to changes in the procedure for processing or transmitting computer information through information communication means, have not yet been regulated and explained at the legislative level.

Keywords: Fraud, types of fraud, computer information

https://doi.org/10.15405/epsbs.2021.05.213
Corresponding Author: Gilyana Vladimirovna Tsebekova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Many scientific works in legal literature and Internet resources are devoted to the analysis of criminal and legal characteristics of economic crime in the Russian Federation (hereinafter – Russia, RF), including crimes against property and some of its types, which include fraud.

Such interest is not accidental, since in our time the relevance of the fight against fraud crimes does not decrease, but instead only increases, as evidenced by the official statistics and the increasing diversity, dynamism and continuous updating, as well as the modernization of fraud methods depending on the scale of their distribution. According to Article 159.6 of the Criminal Code of the Russian Federation, cyber fraud means "theft of the property of another or acquisition of the right to the property of another by entering, removing, blocking, modifying computer information or other interference in the functioning of the means of storing, processing or transmitting computer information or information and telecommunication networks".

This crime is included in chapter 21 of the Criminal Code of the Russian Federation, which implies that its direct object is the property of another or rights to this property. At the same time, for more than 10 years, namely, since 2008, information has been excluded from the list of civil legal relations, which was caused by the fact that it does not have inherent property features, it does not have an owner.

2. Problem Statement

The unsuccessfully formulated legislative norm of Article 159.6 of the Criminal Code contradicts the classical understanding of fraud and creates a lot of practical problems starting from the search for signs of deception in cyber fraud to the differentiation of these elements of crime from the elements of computer crimes. A continuous study of the Article 159.6 leads to the idea of its unnecessary nature in the Criminal Code of the Russian Federation.

3. Research Questions

It should be noted that in the disposition of Article 159.6 there is no reference to the commitment of a fraud or abuse of someone's trust, which is a consequence of the fact that the considered actions are aimed at computers, i.e. a soulless machine, a thing that does not have a psyche, which also makes the fraud as such it impossible.

In the disposition of the 6th paragraph of the analyzed article, the legislator does not indicate either fraud or abuse of trust as methods of committing cyber fraud.

The main modus operandi, which are provided for in Article 159.6 include entering, blocking, deleting information, or other interference.

Traditional fraud is based on direct or virtual contact with a person against whom the act is directed, but a prerequisite is that the person must be animate, which is irrelevant to the rule proposed by the legislator.

https://doi.org/10.15405/epsbs.2021.05.213
Corresponding Author: Gilyana Vladimirovna Tsebekova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

4. Purpose of the Study

In order to understand the nature of the considered crime, it is necessary to assess and disclose the basic concepts mentioned earlier.

The entry of computer information means the following process characterized by the actions on the input of information to computer devices for their further processing or their storage on given computer devices.

The removal of computer information consists in performing actions on media or devices that ensure access to such information, as a result of which it will be impossible to restore information stored on these devices, or the destruction of the media itself, which store information so as to be irrecoverable.

5. Research Methods

In most cases, the judicial practice does not use a set of methods, the input of information is delimited as an independent method of committing fraud and the input, which is an integral part of other methods (for example, modification, blocking, etc.).

Blocking or information blocking means performing artificial, targeted actions that lead to the fact that the user begins to experience difficulties in accessing the necessary information, information resources, or this access is completely closed to him, but this information, which legitimate users are persons with difficulties in accessing or with its termination, is not destroyed.

At the same time, it should be borne in mind that access blocking to information or to software resources is inherently different from direct failure of a computer program, i.e. violation of the integrity of files, its components, which lead to the impossibility of its functioning without the intervention of specialists, or, in most cases, the creators of this program, i.e. its resetting from the media or from the network.

In case of computer program failure, we refer to such actions that make it impossible to work with this program or in it, but the files of its components remain intact, but do not function in the appropriate way that would ensure full interaction with the legitimate user of this program.

Besides, when describing the necessary concepts related to the peculiarities of cyber fraud it is necessary to note such a phenomenon as intentional modification of computer information associated with changes to this information or to the parameters of this information.

At the same time, it should be noted that the following types of information modification are allowed by the current legislation (if this is carried out by persons who legally own this information):

- correction of obvious errors;
- “maintenance” of software, information tools, which is carried out on the user equipment;
- partial transformation of programs to increase their capabilities for interaction with other software tools.

https://doi.org/10.15405/epsbs.2021.05.213
Corresponding Author: Gilyana Vladimirovna Tsebekova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

6. Findings

The interference with storage, processing, as well as information and telecommunication networks, as well as means of transmitting information storage, is understood to mean targeted unlawful actions that distort or completely stop access to information, as well as violate the ability to store and process computer information.

According to Khilyuta (2013), the legislation shall include a norm that will not be associated with fraudulent actions caused by distortion or modification of information on information storage devices.

An example is the position described in the UK Fraud Act 2006, which refers to any form of misleading that may be carried out against any device or system that is designed for transmission, processing or human interaction even without the user involvement (Ladenburg, 2007).

It is important to note that in law enforcement and judicial practice, significant difficulties arise in reflecting the methods of committing fraudulent acts in the field of computer information in the prosecution, as evidenced by the significant number of studied materials of judicial practice on these crimes.

Here we refer to the fact that the attackers take possession of property by taking actions to gain access to information resources or the information environment, manipulating which they get the opportunity to gain access to, use property funds, take away these funds (cash, cashless funds or property rights) belonging to the owners of information or means of storing and processing information.

As has already been noted, the considered article does not specify such a method of committing a crime as fraud or abuse of trust, this corpus delicti does not relate to classical fraud, it is a separate form of theft.

It is necessary to present the features of cyber fraud:

- criminal actions are not performed in relation to the victim's consciousness, but are aimed at computer information or the means of its storage and processing;
- there is no direct influence on the victim's psyche through fraud or abuse of trust;
- there is no direct transfer of property or documents confirming the right to any property by the victim himself;
- in this case not false information that is transmitted directly to a person as part of fraud or abuse of his trust, but the information itself, the means of storing, transmitting and processing this computer information, with the help of which fraudulent actions are carried out, shall be considered as a crime instrument.

The legislator also does not mention such a fraud method as purposeful and intentional copying of computer information, with the help of which, or when it is modified in the future, embezzlement or acquisition of rights to property, the fixation of which was guaranteed by copied information, can be carried out.

The limits of Article 159.6 of the Criminal Code of the Russian Federation are established within the terms that describe the objective side of the considered crime.

At the same time, most of the definitions specified in the norm are almost not disclosed by the legislator, or their characteristics are incomplete and often inaccurate.

https://doi.org/10.15405/epsbs.2021.05.213
Corresponding Author: Gilyana Vladimirovna Tsebekova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

An example of such inaccuracies indicated by the legislator is the concept of "computer information" defined in note 1 to Article 272 of the Criminal Code of the Russian Federation, which states that computer information should be understood as data that are presented in the form of electrical signals that do not depend on their means of storage, processing and transmission.

Continuing the analysis of Article 159.6 of the Criminal Code of the Russian Federation, it should be noted that it does not specify the concept of "other interference with the functioning of the storage facility...", although the wording itself is given in the considered article.

Such unspecified concepts and formulations presented by the legislator in the rules give rise to incorrect, often too narrow or, conversely, too broad interpretations of the studied concepts. The legislative gap described above is noted in the works of many specialists, in particular, Stepanov (2016) says that "other interference..." can be understood as any way of committing a crime, which in turn characterizes this wording as unspecified, thus giving rise to incorrect interpretation.

As part of the analysis of the crime under investigation, it is necessary to reveal the subject and the subjective side of this crime.

According to Article 159.6 of the Criminal Code of the Russian Federation, the subject of crime is a capable person who has reached the age of 16, but also in accordance with Part 3 and Part 4 of Article 159.6 of the Criminal Code of the Russian Federation, a special subject is also provided for specially classified crimes, which means a person with a certain official position.

The main difficulty of establishing the identity of a person who committed a crime in accordance with Article 159.6 of the Criminal Code of the Russian Federation refers to the anonymity of the person who committed this act, which often entails the suspension of criminal cases under this article due to the impossibility of establishing the person who committed it.

The form of direct intent is an expression of the subjective side of fraud in the field of computer information, i.e. a guilty person is aware that he is acting with various forms of distortion and modification, etc. of information through information and telecommunication networks, with the help of special equipment that provides for the processing and transfer of information, in order to seize someone else's property or rights to it.

At the same time, it is necessary to stipulate that the circumstances presented above will not necessarily be signs of a crime under Article 159.6 of the Criminal Code of the Russian Federation, because in order to establish this, in each particular case it is necessary to objectively establish that the person intended to use the obtained access and information obtained in such ways for his selfish purposes.

The considered Article 159.6 of the Criminal Code has 4 parts, the first reveals the disposition of the crime, and the second, third and fourth parts of the article contain its classified elements:

- part 2 – a group of persons by prior agreement, equal with significant damage;
- part 3 – specially classified elements of crime – by a person in the use of his official position, equal to a large amount;
- part 4 – an organized group on an especially large scale.

Thus, by identifying the main signs and systematizing them, we can present the following classifying signs of the crime of cyber fraud:

https://doi.org/10.15405/epsbs.2021.05.213
Corresponding Author: Gilyana Vladimirovna Tsebekova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

- previous concert and a group of persons (Part 2 of Article 159.6 of the Criminal Code of the Russian Federation);
- causing considerable damage to a citizen (Part 2 of Article 159.6 of the Criminal Code of the Russian Federation);
- use of official position to perform a crime (Part 3 of Article 159.6 of the Criminal Code of the Russian Federation);
- especially big amount (Part 3 of Article 159.6 of the Criminal Code of the Russian Federation);
- organized group of persons (Part 4 of Article 159.6 of the Criminal Code of the Russian Federation);
- and especially big amount (Part 4 of Article 159.6 of the Criminal Code of the Russian Federation).

Further, within the framework of the carried out study it is necessary to elaborate more on the characteristics of the classifying signs of the considered crime.

The big amount in relation to the article under consideration is more than 50,000 rubles, especially big – 1 million rubles.

At the same time, in the note to Article 159.1 of the Criminal Code of the Russian Federation, in relation to property of a big amount in Article 159.6 of the Criminal Code of the Russian Federation – property worth more than 1.5 million rubles, and especially big amount – 6 million rubles.

An important characteristic is the ratio of big to especially big amount: 1 to 6, and in Article 159.6 of the Criminal Code of the Russian Federation and in Article 159 of the Criminal Code of the Russian Federation.

The next feature of the classified elements of crime considered in this paper will be the sanctions for this article established by law, as well as the sanctions that are established for “classic” fraud in accordance with Article 159 of the Criminal Code of the Russian Federation.

Under the second and third parts of Article 159.6 of the Criminal Code the sanctions include the deprivation of freedom, the punishment for which can be imposed for a period of up to 4 and 5 years, accordingly, under the second and third parts of Article 159 of the Criminal Code, the sanctions will be for a period of 5 and 6 years, respectively, which, according to Efremova (2013), confirms a less socially dangerous act, which consists in cyber fraud in relation to classic “fraud”, if to consider them in terms of the relevant sanctions established by the legislator.

Taking into account the above features of two types of crimes – cyber fraud and “classic” fraud –in relation to the sanctions of these elements, as well as the limits of stolen property, the question remains open whether these features confirm that the legislator considers cyber crimes less socially dangerous than “classic” fraud, and how objective this classification is in the modern conditions of the widespread penetration of information technologies into all spheres of life of people and society as a whole.

We believe that the opinion expressed by Lopashenko (2015) on this issue is correct: “the legislator took care more of fraudsters of certain groups providing them with more preferential conditions for criminal prosecution” (p. 303) rather than the injured party.

https://doi.org/10.15405/epsbs.2021.05.213
Corresponding Author: Gilyana Vladimirovna Tsebekova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

7. Conclusion

In summary, let us present some conclusions on the issues addressed in the study:

- in the light of the mentioned main methods of committing a crime under Article 159.6, it can be said that here the legislator indicates the elements of crimes under Article 272–274 of the Criminal Code of the Russian Federation;
- the elements of cyber fraud is independent and cannot be correlated with the composition of "classic" fraud, since the disposition of the considered article is not indicated as a way of committing a crime of fraud, or abuse of trust;
- the limits of Article 159.6 of the Criminal Code of the Russian Federation are determined by a significant number of specialized terms that describe the objective side of this crime, while they are not disclosed in full and in terms necessary for their understanding by the legislator. Many new forms of fraud, including in the field of computer information, are blanket. The legislator does not define all the characteristics of these forms of fraud, or many typical characteristics and definitions are given in other regulatory acts, but even in cases where the definitions are in other acts, their exact definitions do not meet the requirements necessary for their accurate understanding;
- in modern circumstances, the criminal legislation does not contain a single definition for crimes in the sphere and using computer equipment and the Internet. Reviewing the legislation, it was revealed that in a number of normative legal acts the legislator enshrined the following definition – "crimes carried out using information and telecommunication networks, including the Internet", but despite this, there is still no full definition and exhaustive definition of "cyber" crimes, which also indicates that the legislator has the right to improve the understanding and definition of computer-assisted crimes in order to achieve an exhaustive definition of such crimes;
- one of the difficulties in relation to the subject of crime under Article 159.6 of the Criminal Code is the anonymity of the perpetrator of this act, which often entails the suspension of criminal cases under this article due to the impossibility of identifying the person who committed it; the difficulties in the objective aspect of the considered crime relate to the use of constantly changing computer technologies, from the point of view of the subjective aspect, often difficulties also arise with the definition of the motive for such crimes and their purpose, which, in turn, is necessary to determine the guilt of suspects. Such situations do not solve and do not contribute to the problems that arise in the process of combating "cyber" crimes;
- difficulties and problems are connected with the fact that in Article 159.1 of the Criminal Code of the Russian Federation there is no specificity of the concept of "other interference with the functioning of the storage facility...", although the wording itself is given in the considered article. Such unspecified concepts and formulations presented by the legislator in the rules give rise to incorrect, often too narrow or, conversely, too broad interpretations of the studied concepts.

https://doi.org/10.15405/epsbs.2021.05.213
Corresponding Author: Gilyana Vladimirovna Tsebekova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

- another problem that the law enforcement officer will face is the use of the term “removal”, which is enshrined in Article 159.6 of the Criminal Code of the Russian Federation and is one of the methods of committing the above crime. The more specific and definite term “destruction” of computer information is used by the legislator in Article 272 of the Criminal Code of the Russian Federation. It is assumed that the use of such a term would also be preferable for Article 159.6 of the Criminal Code of the Russian Federation.

References

Efremova, M. A. (2013). Fraud using electronic information. *Inform. Law, 4*, 20.

Khilyuta, V. V. (2013). *Characterization of crimes against property*. *Textbook*. Yanka Kupala State University.

Ladenburg, G. (2007). *Blackstone's Guide to Fraud Act 2006*. Oxford press.

Lopashenko, N. A. (2015). Legislative reform of fraud: forced questions and forced answers. *Criminol. J. of Baikal State Univer. of Econ. and Law, 3*, 510.

Stepanov, M. V. (2016). Critical analysis of fraud in the field of computer information (Article 159.6 of the Criminal Code of the Russian Federation). *Bull. of Nizhny Novgorod Acad. of the Ministry of Internal Affairs of Russ.*, 175–177.