Cyber crimes against property in foreign and Russian criminal law

Vladimir Ilyich Tyunin[1*], *Anton Gennadievich* Antonov[1], *Tatyana Andreevna* Ogar[1], *Maria Vitalievna* Shkele[1], and *Elena Andreevna* Zorina[2]

[1]Saint Petersburg University of the Ministry of Internal Affairs of Russian Federation, Department of Criminal Law, Saint Petersburg, Russia
[2]Saint Petersburg University of the State Fire Service of the Ministry of the Russian Federation for Civil Defence, Emergencies and Elimination of Consequences of Natural Disasters of Russia, Department of Labour Law, Saint Petersburg, Russia

Abstract. The prerequisite for the study was a significant increase during a pandemic in the number of cyber crimes against property, caused by forced isolation, a reduction in the use of cash and an expansion of the scope of computer technology when concluding civil transactions. Purpose of the study: to identify trends in the criminalization of cyber crimes against property in foreign and Russian criminal law. To achieve the goal, the following methods were used: general scientific – analysis, synthesis, generalization, special scientific – statistical, formal logical, comparative legal, content analysis, the method of expert assessments. The results of the work were the classification of cyber crimes against property, the novelty is the definition of the most common type of these crimes – fraud, the identification of the growth of its individual forms during a pandemic. The issues related to the observed expansion of the scope of application of the liability for fraud, both in international law and in the national legislation of individual states, which are no longer limited to such traditional methods of committing it as deception and breach of trust. Cyber crimes in the Russian criminal legislation are investigated in their relation to crimes against property, recommendations are given for further optimization of the criminal legislation of the Russian Federation. In Russia, as in the rest of the world, during the period of the pandemic, an increase was recorded in crimes against property committed remotely, in relation to non-cash funds, using bank cards. When committing such acts, computer information, electronic data and programs are used as a method or means of committing them, which allows them to be classified as cyber crimes. Previously, cyber crimes were considered separately from traditional socially dangerous encroachments, but the massive use of information technology in the commission of certain types of crimes (in particular, crimes against property) requires a new approach to their description in national legislation.
Keywords: crimes against property, cyber crimes, fraud

* Corresponding author: v-tunin@rambler.ru

1 Introduction

A significant trend in the 21st century has become the transformation of crime as a result of the inclusion of information technologies in its arsenal. All over the world, cyber crimes are merging with certain types of traditional crimes that were previously committed without the use of computers. This is especially evident in the example of crimes against property, which are increasingly committed with the use of computer technology, information and telecommunication networks, electronic means of payment. This trend manifested itself most sharply during the pandemic in relation to crimes committed with non-cash funds using bank cards.

2 Methods

A content analysis of the works of Russian and foreign authors over the past 15 years, including during a pandemic, was carried out to identify the general dynamics and characteristics of cyber crimes against property. The conclusions are supported by expert assessments and statistics. Published documents of judicial practice, reports of domestic and foreign mass media, monographic studies in this area are analyzed.

3 Results

It was revealed that the most widespread crime against property, which is committed with the use of computer technology, in world practice is a fraud, while there is a transformation of the content of this crime, a departure from indicating its traditional methods towards an abstract description of its features in the criminal law. However, in Russian legislation, along with the expansion of the scope of the use of fraud, there is a tendency to casuistry, which has given rise to a number of law enforcement problems that require resolution.

4 Discussion

Quarantine measures have contributed to the growth of computer attacks against property Countries in Europe and the Americas: compared with last year, the volume of fraudulent transactions in dollars increased by 35% [1], the number of reports of fraud with new credit card accounts increased by 88% in 2020 [2]. A similar picture can be observed in the Russian Federation: the number of crimes using bank cards from January to June 2020 increased by almost 500% compared to the same period in 2019 [3].

In both foreign [4] and domestic [5] scientific literature, crimes in the field of computer information are subdivided into cyber crimes in a narrow sense and in a broad sense. In this work, we will use the term “cyber crimes” in a broad sense, that is, including in relation to crimes where information technology is used as a means of criminal encroachment. To determine the place of cyber crimes among traditional ones, it is advisable to refer to international regulatory legal acts and the national criminal legislation of individual foreign states, providing for liability for their commission, as well as scientific research in this area.

The Convention on Crime in the Field of Computer Information, concluded on November 23, 2001 in Budapest [6], provides only one thing as cyber crimes against property: “Computer fraud” (Art. 8). Note that this rule is formulated rather abstractly, among all the varieties and forms of theft, only one is indicated (fraud), and when it is implemented into the national legislation of a particular state, it should be included in the system of property crimes that already exists in it.

In modern monographic studies on cyber crimes against property, the latter are also associated with fraud in its various manifestations [7].

In the legislation of individual states, different approaches have been formed to establish responsibility for cyber crimes against property. Thus, in the 2006 UK Fraud Act, fraud becomes a crime of behavior, not a result, and is no longer associated only with deception (since the use of this concept is impossible, for example, when committing an action using computers), It introduces the concept of "dishonesty", which significantly expands the scope of this crime [8]. In German criminal law, along with the rule on liability for fraud (§263 of the Criminal Code of the Federal Republic of Germany), there was a provision on liability for computer fraud (§ 263a of the Criminal Code of the Federal Republic of Germany) [9].

Cyber crimes against property in Russian criminal law can include thefts committed using technical means that allow receiving or transmitting computer information, as well as crimes encroaching on non-cash or electronic money: theft from a bank account, as well as in relation to electronic money funds (clause "g" part 3 of Art. 158 of the Criminal Code of the Russian Federation), fraud using electronic means of payment (Art. 159.3 of the Criminal Code of the Russian Federation, fraud in the field of computer information (Art. 159 of the Criminal Code of the Russian Federation).

According to the Ministry of Internal Affairs of Russia, among the crimes committed using bank cards from January to June 2020, there is an increase in crimes such as theft (Art. 158 of the Criminal Code of the Russian Federation) and fraud using electronic means of payment (Art. 159.3 of the Criminal Code of the Russian Federation); however, the number of registered frauds in the field of computer information (Art. 159.6 of the Criminal Code of the Russian Federation), on the contrary, decreased by 21% [3].

This trend of law enforcement is explained by a number of circumstances, among which the following prevail: clarifications of the Supreme Court of the Russian Federation, given in the Resolution of the Plenum of 30.11.2017 No. 48 "On judicial practice in cases of fraud, misappropriation and embezzlement" [10]; criminalization of theft from a bank account, as well as in relation to electronic money, in combination with amending the edition of Art. 159.3 of the Criminal Code of the Russian Federation, which extremely narrowed the boundaries of its application (Federal Law of 23.04.2018 No. 111) [11]; appeal practice of regional courts and supervisory practice of the Supreme Court of the Russian Federation in cases of this category.

In the theory of criminal law, there have been no stable views on the rules for applying the rules on cyber crimes against property for a number of reasons:

1) the criminalization of acts falling under the action of special types of fraud, which differ in the features of the subject of the crime and the scope of their commission (Federal Law of November 29, 2012, No. 207);

2) recognition of non-cash funds in a bank account as a kind of someone else's property [12];

3) the imperfection of the legislative structure of the elements of cyber crimes requiring clarification of the Supreme Court of the Russian Federation [13];

4) the absolutization of the established doctrinal provisions of scientific criminologists in the context of the new criminal law and criminological reality.

In the design of computer fraud (Art. 159.6 of the Criminal Code of the Russian Federation), the legislator refused to indicate the traditional methods of classic fraud – deception and abuse of trust, which drew criticism from forensic scientists and practitioners [14]. The composition of the fraud enshrined in Art. 159.3 of the Criminal Code of the Russian Federation (until April 23, 2018) provided for deception in relation to persons on whom the use of a payment card by the guilty person depended as a means of committing a crime. This made it possible to apply the rule in case of illegal debiting of funds from the bank account of the injured persons when making payments for purchased goods and

rendered services, when receiving money from credit institutions on someone else's or counterfeit card. Subsequently, the clarifications of the Resolution of the Plenum of the Supreme Court of the Russian Federation of November 30, 2017 made it possible to apply Art. 159.3 of the Criminal Code in case of passive deception of persons providing the opportunity to use payment cards [10].

However, the legislator considered the presence of the specified offenses to be insufficient. The rationale for the criminalization of theft from a bank account was the idea that such a crime poses an increased public danger, since the perpetrator through remote access to a bank account using technical means, while remaining anonymous, is able to commit a crime from anywhere in the world, having only access to the network [15].

Such actions could be covered by the provision of Art. 159.6 of the Criminal Code of the Russian Federation, but at that time it did not provide for the subject of theft in the form of funds in a bank account. An updated version of paragraph "c" of part 3 of Art. 159.6 of the Criminal Code of the Russian Federation contains the aforementioned subject of the crime, but the article is not widely applied, since, according to the explanations of the Supreme Court of the Russian Federation [10], the methods of committing a crime should lead to interference in the operation of computer facilities, disrupt the process of processing, storing, transferring computer information, which ultimately should lead to theft.

After the addition of Art. 158 of the Criminal Code of the Russian Federation with clause "d" in part three and amendments to the main composition of Art. 159.3 of the Criminal Code of the Russian Federation, a judicial practice followed the path of using theft from a bank account in cases previously qualified under Art. 159.3 of the Criminal Code of the Russian Federation and Art. 159.6 of the Criminal Code of the Russian Federation. It is rather difficult to talk about the ratio of the acts currently falling under these articles, since judicial statistics do not reflect the number of crimes classified separately under paragraph "d" of Part 3 of Art. 158 of the Criminal Code of the Russian Federation. This circumstance does not allow us to fully assess the growth in the number of cyber crimes against property according to statistics, since a significant part of them in judicial and investigative practice refers to theft.

In the scientific community, discussions continue about the enforcement of articles on cyber crimes and their further fate [16].

The existing uncertainty in law enforcement practice regarding the delimitation of norms on cyber crimes can be eliminated either by introducing clarifications into the text of the current resolution of the Plenum of the Supreme Court of the Russian Federation of November 30, 2017 No. 29, or by introducing amendments to the articles on crimes against property committed by information methods.

5 Conclusion

In international and foreign criminal law, cyber crimes against property are associated mainly with fraud, and the content of this concept is significantly expanded and is no longer associated with deception in relation to a specific person.

To cyber crimes against property in a broad sense in the domestic Russian criminal legislation should include the acts provided for by paragraph "g" of Part 3 of Art. 158 of the Criminal Code of the Russian Federation, Art. 159.3 of the Criminal Code of the Russian Federation and Art. 159.6 of the Criminal Code of the Russian Federation. It is necessary to rethink the degree of public danger of the listed acts, which may require legislative intervention. Also, given the global trends in the criminalization of norms on liability for cyber crimes against property in a broad sense, legislation should more actively use an abstract way of formulating norms, without focusing on the criminalization of incidents, which currently gives rise to serious problems in the practice of applying the norms on cyber crimes against property in Russia.

References

1. A.M. Andriotis, O. McCaffrey, Borrower, Beware: Credit-Card Fraud Attempts Rise During the Coronavirus Crisis. Accessed on: March 22, 2021. [Online]. Available: https://www.wsj.com/articles/borrower-beware-credit-card-fraud-attempts-rise-during-the-coronavirus-crisis-11590571800
2. J. Steele, Credit card fraud and ID theft statistics. Accessed on: March 22, 2021. [Online]. Available:https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276
3. Brief description of the state of crime in the Russian Federation in January – June 2020. Accessed on: March 22, 2021. [Online]. Available: https://xn--b1aew.xn--p1ai/reports/item/20597695/
4. A. Dreißigacker, B. von Skarczinski, G.R. Wollinger, Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. Accessed on: March 22, 2021. [Online]. Available: http://www.krimg.de/drupal/files/9783964100191.pdf
5. A.S. Mironchik, A.V. Susloparov, Legal Research, **9**, 17-30 (2019). https://doi.org/10.25136/2409-7136.2019.9.30745
6. Konventsiya o prestupnosti v sfere kompyuternoi informatsii ETS N 185 (Budapesht, 23 noyabrya 2001 g.) Accessed on: March 22, 2021. [Online]. Available: http://base.garant.ru/4089723/#ixzz6cFkI64wE
7. B. Rajput, *Cyber Economic Crime Typology*, in: Cyber Economic Crime in India, 79-96 (2020). https://doi.org/10.1007/978-3-030-44655-0_5
8. J. Maureen, M.R. Kevin, Int. Rev. Law, Comput. & Tech. **21(3)**, 295-304 (2007). https://doi.org/10.1080/13600860701701553
9. A.E. Zhalinsky, Sovremennoe nemetskoe ugolovnoe pravo [Modern German Criminal Law] (TK Welby, Publishing house Prospect, Moscow, 2006)
10. Postanovlenie Plenuma Verkhovnogo Suda Rossiiskoi Federatsii "O sudebnoi praktike po delam o moshennichestve, prisvoenii i rastrate" ot 30.11.2017g. №48 [Resolution of the Plenum of the Supreme Court of the Russian Federation "On judicial practice in cases of fraud, misappropriation and embezzlement" dated 30.11.2017. No. 48], Bul. Supreme Court of the RF, **2**, 7-13 (2018)
11. Federalnyi zakon ot 23.04.2018 № 111-FZ "O vnesenii izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii" [Federal Law of 23.04.2018 No. 111-FZ "On Amendments to the Criminal Code of the Russian Federation"], Rossiyskaya Gazeta, **88(7551)** 2018
12. A.V. Arkhipov, Bul. Tomsk State Univ. **48,** 195-198 (2017). https://doi.org/10.17223/15617793/418/24
13. E.A. Russkevich, J. Rus. Law. **8(248)**, 73-80 (2017). https://doi.org/10.12737/article_597714e7c1b439.52593067
14. Yu.V. Gracheva, Crim. Law **5**, 28-33 (2019)
15. N.Yu. Skripchenko, Bank. Law **1**, 41-49 (2020)
16. A.K. Klimenko, Rus. Investig. **5**, 38-42 (2020). https://doi.org/10.18572/1812-3783-2020-5-38-42