World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-29, December -2023
ISSN: 2749-3601

PROBLEMATIC ISSUES IN THE CRIMINAL LEGAL CHARACTERISTICS OF CYBERSTALKING

Kharatishvili Anton Georgievich
Candidate of Legal Sciences, Associate Professor of the Department of Criminal Procedure and Criminalistics, St. Petersburg State University.
Zokirov Sardorjon Karimjon ugli
Lecturer of the Criminal Procedure Law Department of the Tashkent State Law University

Article history:

Received: October 17th 2023
Accepted: November 14th 2023
Published: December 20th 2023

Abstract:

The article examines the specifics of cybercrime and high technology offences, as well as methods and technologies for their detection and investigation. The focus is on the need for co-operation between different countries and law enforcement agencies to effectively combat these threats.

Keywords: Cybercrime, high technology offences, detection, investigation, cooperation, blockchain

The study of the criminalistic characterization of crime is preceded by an analysis of its criminal law aspect. To a certain extent, the latter is an element in the development of the foundations of the criminalistic characterization and investigation techniques of unlawful acts. Criminal-legal characterization largely determines the direction and nature of the activities of law enforcement agencies. L.D. Gaukhman, considering the criminal-legal characterization, includes in it exclusively the issues of the concept and qualification of a crime[1]. The content of this characteristic is the information revealing a specific crime composition, represented by a set of features characterizing it, enshrined in the disposition of articles of the special part of the Criminal Code of the Republic of Uzbekistan and the Russian Federation. The features of the crime are united in groups, forming such elements as object, objective side, subject, and subjective side, which constitute a single system. The absence of at least one of them in this system leads to the absence of the crime itself. V.N. Kudryavtsev noted the following: "the composition is an information model of a crime of a certain type, enshrined in the criminal law. This model is formed because of generalization of signs of all crimes of this type. As a result, we get an economical, concise, and sufficiently clear description of their basic properties"[2]. Thus, the criminal-legal characteristic of a crime is a scientific category, which includes systematized information about the totality of signs of elements of a particular type of crime, obtained by the researcher and allowing him to correctly solve the issues of qualification of a crime.

To analyze the criminalistic characteristic of cyber theft, it is necessary to determine the criminal-legal differentiation of various forms of theft using information and telecommunications networks.

The most difficult question arising in practice is related to the distinction between Article 159.3 of the Criminal Code, paragraph "g" of Part 3 of Article 158 and Article 159.6 of the Criminal Code of the RF. Let us pay attention to the wording of p. "d" part 3 of article 158 of the Criminal Code of the RF, according to which the crime is theft from bank accounts, as well as in relation to electronic money. Many modern researchers concluded that the line separating one crime from another is rather thin, and sometimes it is extremely difficult to determine it. First, this is because the object and subject in these crimes are related. It should be noted that fraud and stealing are varieties of theft, that is, they have some common features. By stealing is meant a secret theft, in the commission of which the perpetrator does not enter direct contact with the victim. In the case of fraud, the perpetrator interacts with the victim, influencing him/her through deception or breach of trust, i.e. there is always an addressee of information perception.

Thus, the way of committing the crime is a factor that allows to separate these components. According to the Resolution of the Plenum of the Supreme Court of the Russian Federation of November 30, 2017, № 48: "The theft of other people's money through the use of a previously stolen or counterfeit payment card, if cash withdrawal was made through an ATM without the participation of an authorized employee of the credit

[1] Гаухман Л.Д. Расследование по делам о телесных повреждениях и хулиганстве. М., 1975. 80 с.

[2] Кудрявцев В.Н. Общая теория квалификации преступлений. М., 1972. 352 с.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-29, December -2023
ISSN: 2749-3601

organization does not form the crime of fraud. In this case the deed should be qualified as theft.

In cases when a person has stolen non-cash funds using confidential information of the payment card holder (for example, personal data of the owner, payment card data, control information, passwords), necessary for gaining access to them, given to the attacker by the payment card holder under the influence of deceit or breach of trust, the actions of the perpetrator shall be qualified as theft". It is assumed that this explanation does not fully correspond to the modern regulation of cash and settlement relations. There are situations when bank employees help clients with settlements, but do not check their identity (for example, when they ask a consultant to help them operate an ATM located in the bank's office). How should the actions of the guilty person be qualified in such cases? Modern practice does not give an answer to this question, from the point of view of doctrine there are arguments to justify both positions. On the one hand, in such a situation the deception is expressed in the default about the belonging of the bank card. On the other hand, the bank employee does not certify anything, does not confirm the belonging of the card to a particular person. In this regard, it is difficult to answer the question unambiguously.

Often the problem of differentiation of these offenses arises in cases of theft using a contactless bank card when paying for purchases at the cash register of a store. The Supreme Court of the Russian Federation states that the actions of a person should be qualified under Article 159.3 of the Criminal Code of the Russian Federation in cases when the theft of property was carried out by reporting to an authorized employee of a credit, trade or other organization knowingly false information about the belonging of such a card to the specified person on legal grounds or by omission of the illegal possession of the payment card. This explanation does not fully correspond to the modern civil turnover, because there are systems of contactless payment, PayPass, ApplePay, etc., when the guilty person does not tell anyone anything, but only mechanically puts the card or phone to the machine and the money is debited. Let us refer to one of the decisions of the Trans-Baikal Territorial Court[3]. In the appeal submission, the deputy prosecutor points out that the court sentence should be changed due to the incorrect application of criminal law by the court, believes that the actions of N. are subject to qualification under part 2 of article 159.3 of the Criminal Code of the RF, because "N. stole a bank card belonging to LNV and then in various trade organizations made payment from the card, causing significant material damage to the victim, without disclosing that he used the bank card illegally, that is, by deceiving sellers and abusing their trust. In the given example, the deception by defaulting about the true owner of the bank card is directed at the person who performs the functions of cash service for customers of the sales area. The doctrine has developed the following criteria of inaction: informational, energetic, and unlawful. M. D. Shargorodsky noted that the question should be solved not "when inaction is the cause of the result, but only about when the subject is responsible for inaction"[4]. Due to the blanket nature of the norms on fraud, the legal nature of passive deception will be revealed in the presence of a person's obligation to follow the established rules. In the above situation - to verify the identity of the cardholder. In some clarifications, the Ministry of Finance of the Russian Federation explains that a bank card is inserted into a payment terminal that has a connection with the issuer. After that it is checked, its belonging to a particular person is established by transferring the owner's account number, and the solvency of the person is confirmed. After that the card is returned by the cashier to the owner. Consequently, verification of users and verification of their solvency is performed by the payment card operator through the terminal. In this case, the cashier performs only the role of a service link that does not affect the process of debiting funds, the seller has no obligation to identify the person. In such a case it is appropriate to speak about the presence of signs of the crime provided by p. "g" part 3 of article 158 of the Criminal Code of the Russian Federation.

As part of the solution to this issue, let us turn to the practice of the Supreme Court of the Russian Federation. Quite recently, the Criminal Cases Collegium decided [5], according to which "within the meaning of

[3] Апелляционное определение Забайкальского краевого суда от 27.06.2019 по делу № 22-1753/2019 // Доступ из СПС «КонсультантПлюс»

[4] Шаргородский М. Д. Вопросы уголовного права в практике Верховного Суда СССР // Социалистическая законность. 1945. № 9. С. 47.

[5] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6 // Доступ из СПС «КонсультантПлюс»

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-29, December -2023
ISSN: 2749-3601

the criminal law, theft of money, committed with the use of electronic means of payment by the perpetrator, forms the component of this crime in those cases where the seizure of money was carried out by deception or abuse of trust of its owner or another person. However, as follows from the materials of the criminal case, Kaktan Y.Y., having found the victim's bank card, paid for goods with it by contactless method. Employees of trade organizations did not take part in the implementation of operations to write off funds from the bank account as a result of payment for goods. Accordingly, Kaktan Y.Y. did not give false information about the belonging of the card to the employees of trade organizations and did not mislead them. The current normative acts do not impose on the authorized employees of trade organizations carrying out payment transactions with bank cards the obligation to identify the cardholder by his identity documents". Also, the Supreme Court points out that in paragraph 17 of the Resolution of the Plenum of the Supreme Court of the Russian Federation No. 48 of November 30, 2017, explanations were given in relation to the earlier version of Article 159.3 of the Criminal Code of the Russian Federation. However, Federal Law No. 111-FZ of April 23, 2018 "On Amendments to the Criminal Code of the Russian Federation" amended Article 159.3 of the Criminal Code of the Russian Federation. Therefore, it is incorrect to apply such clarification in the case at hand.

Based on all of the above, we can distinguish the following main differences between stealing and fraud: in the case of fraud, the perpetrator acts openly, in the case of stealing - secretly; in fraud, the perpetrator through deception or breach of trust forces the victim to commit actions that will lead to the withdrawal of funds, in the case of stealing deception is not aimed directly at taking possession of another's property, but is used only to facilitate access to it.

Of great actuality in view of the development of information technologies is fraud in the sphere of computer information (Article 159.6 of the Criminal Code of the Russian Federation): stealing other people's property or acquiring the right to other people's property by entering, deleting, blocking, modifying computer information or otherwise interfering with the functioning of means of storing, processing or transmitting computer information or information and telecommunication networks. The mentioned article is designed to protect property relations, as well as relations ensuring the security of information and telecommunication networks and computer information. In this situation, the seizure of property is associated with penetration into the information environment, in which various kinds of information operations are carried out, the legal significance of which consists in the acquisition by participants of turnover of property (rights to it) in the form of cash, non-cash funds, other property rights.

Computer information means information (messages, data) presented in the form of electrical signals, regardless of the means of their storage, processing, and transmission (note to Article 272 of the Criminal Code of the Russian Federation). According to the clarification of the Supreme Court, interference in the functioning of means of storage, processing or transmission of computer information or information and telecommunication networks is recognized as a purposeful impact of software and (or) software and hardware on servers, means of computer technology (computers), including portable (portable) - laptops, tablet computers, smartphones equipped with the appropriate software, or on information and telecommunication networks, which violates the established procedure.

In cases when stealing is committed by using the credentials of the owner or other owner of the property regardless of the method of gaining access to such data (secretly or through deceit he used the victim's phone connected to the "mobile bank" service, authorized in the Internet payment system under the data of another person known to him, etc.), such actions are subject to qualification as stealing if the perpetrator did not illegally influence the software of servers, computers or the information and telecommunication technologies themselves At the same time, the change of data on the state of the bank account and (or) on the movement of funds, which occurred as a result of the use by the perpetrator of the victim's accounting data, cannot be recognized as such influence. If the theft of another person's property or acquisition of the right to another person's property is carried out by disseminating knowingly false information in information and telecommunication networks, including the Internet (for example, creation of fake websites of charitable organizations, online stores, use of e-mail), such fraud should be qualified under Article 159, not 159.6 of the Criminal Code of the RF.

Analyzing the disposition of Article 159.3 of the Criminal Code of the Russian Federation above it was stated that this component is characterized by a certain method: deception or breach of trust. This is a classic feature of the objective side of fraud, with the help of which it is possible to distinguish this component of the crime from other forms of theft. However, in Article 159.6 of the Criminal Code of the RF there is no indication of the method. To qualify a deed under this article it is

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-29, December -2023
ISSN: 2749-3601

necessary to establish the presence of interference in the functioning of information and telecommunication resources. This way of committing a crime does not provide for personal contact between the guilty person and the victim, there are only manipulations that are carried out by the subject with the help of technical and software tools. Some scientists concluded that fraud in the sphere of computer information is an independent form of theft, has a specific method that is not characteristic of classical fraud, in this regard is not special in relation to Art. 159 of the Criminal Code of the RF.

Thus, the main legal distinction between Art. 159.3 and Art. 159.6 of the Criminal Code of the RF lies in the method of committing theft of property. There is a position in the doctrine of criminal law, according to which it is necessary to exclude Art. 159.6 from the Criminal Code of the RF, because its presence in the criminal legislation is superfluous. The act can be qualified in this case under Art. 158 and Art. 272 of the Criminal Code of the RF. On the other hand, it can be assumed that the legislator by such an innovation wanted to facilitate the application of norms and combine into one compound several of them. However, the Supreme Court by its interpretation narrows the scope of application of Article 159.6 of the Criminal Code of the RF.

Based on all the above, we can conclude that in the modern world new methods of theft using information and telecommunication networks will be constantly invented. In this regard, it is necessary to interpret the rules of criminal law, explanations of the Supreme Court and doctrinal positions considering the existing scientific and technological changes to eliminate problems with the qualification of acts of guilty persons, to create more universal mechanisms for resolving conflicts.

Difficulties arising in practice in determining the criminal legal characterization of a crime are reflected in the criminalistic characterization of the unlawful act. Thus, the connection of these aspects is extremely important for the organization of an effective investigation.

LIST OF REFERENCES

1. Gauxman L.D. Rassledovanie po delam o telesnыx povrejdeniyax i xuliganstve. M., 1975.
2. Kudryavtsev V.N. Общaya teoriya kvalifikatsii prestupleniy. M., 1972.
3. Apellyatsionnoe opredelenie Zabaykalskogo kraevogo suda ot 27.06.2019 po delu № 22-1753/2019 // Dostup iz SPS «KonsultantPlyus»
4. Shargorodskiy M. D. Voprosы ugolovnogo prava v praktike Verxovnogo Suda SSSR // Sotsialisticheskaya zakonnost. 1945. № 9.
5. Opredelenie Sudebnoy kollegii po ugolovnыm delam Verxovnogo Suda Rossiyskoy Federatsii ot 29.09.2020 № 12-UDP20-5-K6 // Dostup iz SPS «KonsultantPlyus»
6. «Osobennosti vыyavleniya i rassledovaniya kiberprestupleniy i prestupleniy v sfere vыsokix texnologiy», https://humoscience.com/index.php/lfas/article/view/1617
7. «Specifics of detection and investigation of cybercrime and high technology offences», https://www.scholarexpress.net/index.php/wbml/article/view/3113
8. Zokirov Sardorjon Karimjon ogli, & Toxtabakiyev Kamronbek Abdukarim ogli. (2023). ON PROOF AND EVIDENCE IN CRIMINAL PROCEEDINGS - EXPERIENCE OF UZBEKISTAN. American Journal of Research in Humanities and Social Sciences, 18, 27–30. ON PROOF AND EVIDENCE IN CRIMINAL PROCEEDINGS - EXPERIENCE OF UZBEKISTAN | American Journal of Research in Humanities and Social Sciences