Advances in Economics, Business and Management Research, volume 138
2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)

Peculiarities of the Investigation of Crimes and Administrative Offenses Committed in the Digital Environment

Sultanov K.A.[1,*] Shevtsov A.V.[2] Nikolaev A.G.[2]

[1] *Department of civil and labor law, civil procedure, Moscow University of the ministry of internal affairs of the Russian Federation named after V.Ya.Kikot, Moscow, Russia*
[2] *Department of Management of Public Order Service in Protection's Provision (Center for Command Staff Trainings) Management Academy of the Ministry of the Interior of Russia, Moscow, Russia*
[*] *Corresponding author. Email: mpkr@mail.ru*

ABSTRACT
With the development of Internet technologies, both the positive aspects of the Internet space and the adverse ones did not rest. The development of online fraud has become one of the main threats to the safe use of Internet resources. People who do not have sufficient Internet security skills are increasingly falling into the "digital traps" of scammers. However, the existing domestic legislation of Russia does not always manage to respond to new trends arising in modern crime. Therefore, new dangerous actions committed in the digital environment often remain beyond the scope of the law, and attackers remain unpunished. First of all, the point is in petty offenses committed in the digital environment (with damage up to 2,500 rubles), which, in principle, cannot be solved. This circumstance determines the relevance of the research topic. The relevance of the study is provided by the fact that the amount of damage caused by crimes in the virtual space in recent years has grown many times. The scientific novelty of this paper lies in the fact that, taking into account available research and existing legislation, questions about the causes and characteristics of crimes and delinquencies in the digital environment are revealed more than ever before.
Keywords: *Internet, cybercrime, digitalization, fraud, administrative offense, digital environment, digital rights*

1. INTRODUCTION

A comprehensive analysis of the state of crime in the Russian Federation over the past five years shows us a significant increase in crimes and administrative offenses committed in the digital environment. A similar situation can be seen in other foreign countries. The digitalization of social life has led to the emergence of previously unknown so-called digital rights. The need to recognize and protect digital rights is proclaimed in a number of international legal acts. Thus, the Charter of the Global Information Society [1] adopted by representatives of eight leading world powers, including Russia, proclaims the need to strengthen relevant policies and regulatory frameworks that promote cooperation to optimize global networks, to combat abuses that undermine the integrity of the network, to reduce the gap in digital technology, to invest in people, and to ensure global access and participation in this process. The Charter also reaffirmed the obligation of states to coordinate their actions in the creation of safe cyberspace, the security of information systems protected from crime, including transnational organized one.

It should be noted that the imperfection of statistical accounting allows tracing the dynamics of only a part of cybercrime, moreover, not the most significant one, and does not give an objective picture of the state of crime in this area (Table 1) [2]. In addition, administrative offenses committed in the digital environment are not accountable. If crimes are taken into account, then offenses are not divided into "digital" or "non-digital." For example, the offender stole 10 dollars (about 800 rubles) from the victim by deception and abuse of trust on the Internet. This action will be qualified as an administrative offense under Part 1 of Article 7.27 of the Code of Administrative Offenses of the Russian Federation and will most likely be never solved. In statistics, it also will not appear as committed in the digital environment by a cybercriminal [3].

Copyright © 2020 The Authors. Published by Atlantis Press SARL.
This is an open access article distributed under the CC BY-NC 4.0 license -http://creativecommons.org/licenses/by-nc/4.0/.

Table 1 Crimes/Years

Crimes	Years				
	2015	**2016**	**2017**	**2018**	**2019**
Prescribed by Article 28 of the Criminal Code of the Russian Federation, including	2,378	2,570	1,883	2,253	2,678
Article 272 Article 273 Article 274	1,395 970 13	1,443 1,124 3	1,079 802 2	1,250 999 4	1,755 910 13
Article 159.6	5,442	5,380	2,195	3,450	4,569
Article 171.2	1,477	1,519	1,492	1,550	1,663
Article 187	-	234	239	254	289

Every day, dozens of citizens' complaints are received by law enforcement agencies of the Russian Federation on the fact of unlawful actions against them in the field of the digital economy and digital environment, particularly, criminals remotely steal citizens' funds from bank accounts. However, if the theft amount is less than 2,500 rubles, then this is not deemed as a criminal offense but it is considered only an administrative offense with a short term of administrative responsibility, 3 months (Article 7.27 of the Code of Administrative Offenses of the Russian Federation). Moreover, as part of the verification of the offense report, it is impossible to conduct a high-quality investigation, to send requests to specialized informational police units in order to identify the offender [4].

The solving rate of even this small part of the detected cybercrimes does not exceed 5%. At the same time, the development of information and telecommunication technologies has made it possible to commit cybercrimes in many respects with impunity since the existing criminal legislation is poorly adapted to new types of crimes in the field of information technology, although online trading and banking, high-speed data services, modern communication formats, electronic education, gaming, and entertainment portals have come into existence a long time ago The list is limited to departmental statistical accounting that does not allow obtaining information about other crimes committed using electronic or information and telecommunication networks, including the Internet. [5]. The increasing role of information and communication technologies has affected the current trends of cybercrime: crime organization is growing, expanding, the spheres of criminal interests are extending, criminal schemes and latentization are becoming more complicated; the most common actions are those related to online trading, credit card servicing and internet banking, including the use of mobile communications; extortion; in the field of gambling; piracy of digital content and software; cyber mercenariness, as well as organizing the spread of prostitution, illegal migration, pornography, drug and arms trafficking; cybercrimes are often committed in conjunction with other socially dangerous actions and are optional in nature [6]. This is due to the fact that using computer information as a means of committing a crime, criminals “turn” it into the subject of another socially dangerous action (for example, the theft of personal data for the purpose of subsequent extortion); its transformations are reflected in the characteristics of the subjects [7]. Given the public danger of cybercrime and its alleged real scale, it is obvious that the existing criminal law does not contain a sufficient regulatory framework for the protection of relevant public relations. There are no uniform explanations of the highest court regarding the criminal legal assessment of such crimes, which maintains the conditions for further criminalization of the virtual space. The level of digital (computer) literacy of network users, which is increasing annually, is the criminogenic and at the same time anti-criminogenic factor of cybercrime. A further increase in cybercrime is predicted [8].

2. RESEARCH METHODOLOGY

The methodological base of this study was compiled by general scientific methods of cognition, including the principle of objectivity, systematicity, induction, deduction, etc. Along with general scientific methods of cognition, private scientific methods, i.e. descriptive, linguistic, and comparative-legal, were used. The study topic is disclosed from the standpoint of general scientific methods (sociological, systemic, structural and functional, concrete historical, and statistical), general logical methods of theoretical analysis, and private scientific methods (comparative law, technical legal analysis, concretization, and interpretation). In connection with the foregoing, a comparative study of the state of Russian legislation on combating cybercrimes and administrative offenses under the continuous influence of information technology seems relevant. The use of the comparative-legal method is due to the universal phenomenon of the digitalization of law.

3. RESEARCH RESULTS

The analysis of laws and regulations revealed the main idea of the formation of the information society: first, the creation of an information basis (computerization and internetization of the country); second, the development or improvement of the "information presentation" of the activities of state authorities and public-owned companies [9]. Most likely, the mechanism for the formation of the state program of the Russian Federation “Information Society (2011-2020)” consisted in collecting proposals from individual government bodies and public-owned

companies for the implementation of the information society in their activities, followed by generalization into programs (“road maps”). The tool of protection of the information society in the criminal law field is the existing criminal law. Accordingly, the adequacy of countering information threats depends significantly on the quality of legislative regulation [10]. The notions of computer crimes in law and science are not ideal and have a number of challenges at various levels, which should be addressed.

The main difficulty lies in the delimitation of the criminal law concept found in most papers from the concepts of criminological, forensic, sociological, and technical nature [11]. The specifics of the criminal law concept of “computer crimes” is revealed through a socially dangerous action, which is regulated by criminal law. Thus, the three components of computer crimes (Articles 272, 273, and 274 of the Criminal Code of the Russian Federation) represent universal ways of influencing the information component of society [12]. The term “cybercrime” has been actively used in scientific literature along with the concept of “computer crime.” So, A.I. Khaliullin identifies two signs of cybercrime: 1) committed using information and telecommunication networks; 2) involves the simultaneous presence of two objects of abuse: both public relations in the field of security of the circulation of computer information and public relations related to it, interconnected with the real world (relations of property, life, health, etc.) [13]. We believe that these signs are not enough to outline the circle of “cyber actions” since virtually any crime from the Criminal Code of the Russian Federation committed on the Internet automatically becomes a cyber crime. We believe that for a clear delineation of the concept, a third mandatory feature is required, the use of special knowledge in the computer field or special software systems for committing criminal acts.

Thus, three signs of computer crimes can be distinguished: 1) committed using a computer (information and telecommunication network); 2) the object is public relations to ensure legitimate access to computer information and an additional optional object is public relations associated with them; 3) an informational method of encroaching on computer information involving the use of special knowledge or computer systems (technology) is used.

The term "киберпреступление" is actually a linguistic calque from the English word "cybercrime" and in content, it completely corresponds to the one proposed by A.L. Osipenko - "network computer crime" [14]. The concept of “computer crimes” is wider in scope and includes cybercrime as a part of crimes committed online along with offline crimes. Thus, the criminal legislation of Russia consistently criminalize actions committed on the Internet, which has already been reflected in 13 articles of the Criminal Code of the Russian Federation: as signs of the basic components (Articles 171.2, 185.3, 282 of the Criminal Code of the Russian Federation); as signs of a qualified component (Clause "д" of Part 2 of Article 110, Clause "д" of Part 3 of Article 110.1, Clause "в" of Part 2 of Article 151.2, Part 2 of Article 205.2, Clause "б" of Part 2 of Article 228.1, Clause "б" of Part 3 of Article 242, Clause "г" of Part 2 of Article 242.1, Clause "г" of Part 2 of Article 242.2, Part 2 Article 280, Part 2 of Article 280.1 of the Criminal Code of the Russian Federation). In such crimes, the use of information and telecommunication networks (including the Internet) is not an object of encroachment but is used as a more effective means of achieving criminal goals that lie beyond the framework of information technology [15].

The legislator, solving practical problems, used regulatory models that exist in foreign legislation, where such actions are qualified as computer fraud, however, taking into account the position of the Supreme Court of the Russian Federation, it excluded the concepts of fraud and breach of trust by replacing them with a method of “by entering, deleting, blocking, modification of computer information or other interference with the functioning of storage, processing, or transmission of computer information or information and telecommunication networks." Thus, formally, we received fraud without fraud, although implied. The pre-existing set of crimes was replaced by a single complex crime combining illegal access and theft.

4. DISCUSSING THE RESULTS

Thus, the misconception regarding deception was secured at the level of legislation, which became the basis for further scientific research. Thus, for example, developing the thought of the legislator, S.A. Filimonov proposes to supplement the Criminal Code of the Russian Federation with Art. 158.1 "Theft Using Payment Cards" [16]. So, V.M.Bykov and V.N.Cherkasov noted that scientific and technological progress in the field of information has led to the emergence of new ways of presenting information, biotechnological, laser, nanotechnological, which casts doubt on the identification of the concept "computer information" with the concept "electronic information" [17]. In addition, the definition is incorrect because it allows attributing a whole group of analog devices and networks to means containing computer information.

Thus, computer crimes are actions distinguished by the method of encroachment, providing for basic primitives of influence on the information infrastructure. During the commission of computer crimes, the impact on additional objects (life, health, property, etc.) is qualified in the aggregate for the corresponding components of the crimes. A clear definition of computer crimes, their scope, and correlation with satellite components allows combining stable criminal law with the required flexibility to respond to emerging threats.

5. CONCLUSION

Society today lives in a new digital reality created by information technology. Digital technologies have penetrated into all areas of human activity and today we are talking about creating a new reality that will have no analogs in the old world. The digitalization of society, its

political and economic components suggests that there is a need to fill the national legal systems with standards that will acquire a new degree of compatibility within the framework of the formation of a macroenvironment of legal regulation.

The state's task is to protect the digital rights of citizens from various violations, but the existing legislation does not fully meet contemporary realities. Therefore, legislation relating to the regulation of digital rights of citizens needs to be modernized and systematized, bringing its conceptual apparatus into a harmonious, consistent state.

An important problem of the relationship between the government and the citizen in a digital society is the determination of possible restrictions on digital rights by federal law, including the permissible limits for the control of the information environment by law enforcement services in order to ensure effective protection of the society from cybercrime. Therefore, it is necessary to search for the ideal legal compromise between the ability of law enforcement services to access computer information and the right of citizens to its confidentiality.

The methodological reference point and starting point here should be constitutional principles and rules. Regardless of the extent of development of digital reality today, it should be subject to the Constitution of the Russian Federation as a regulatory act with the highest legal force in the Russian legal system, including with respect to the laws governing the field of new relations under consideration.

All of the above suggests that today it is required to search for the ideal legal compromise between the possibility of access of special services and law enforcement agencies to computer information and the right of citizens to its confidentiality:

- The total volume of crimes and offenses against constitutional human rights and freedoms committed in the Russian Federation in the field of digital technologies is increasing from year to year.

- The relevance of the issue of protecting human rights in the course of development of the information society lies, first of all, in the absence of a holistic concept of legal measures to counter human rights abuses and insufficient legislative regulation and a uniform understanding of rules of law in doctrine and law enforcement practice.

- Administrative offenses committed in the digital environment should be isolated in a separate statistical category. At present, their absence in statistics leads to the appearance of distorted figures on the state of crime in the Russian Federation. Actual petty digital offenses are excluded from it and they are not subject to accounting and control.

REFERENCES

[1] "Okinavskaya khartiya global'nogo informatsionnogo obshchestva" (Prinyata na o. Okinava 22.07.2000) // Diplomaticheskiy vestnik N 8, 2000 god.

[2] Korobeyev A.I., Dremlyuga R.I., Kuchina YA.O. Kiberprestupnost' v Rossiyskoy Federatsii: Kriminologicheskiy i ugolovno-pravovoy analiz situatsii // Vserossiyskiy kriminologicheskiy zhurnal. 2019. T. 13. No. 3. S. 416-425.

[3] Kompleksnyy analiz sostoyaniya prestupnosti v Rossiyskoy Federatsii i raschetnyye varianty yeye razvitiya // Analiticheskiy obzor. VNII MVD. M.: 2019.

[4] K.A. Sultanov, E.V. Kashkina, P.V. Ustinov Legal regulation of counteraction to administrative offenses in the conditions of digitalization // Advances in Economics, Business and Management Research, volume 105, Available Online December 2019. https://doi.org/10.2991/iscde-19.2019.161

[5] Volevodz A. G. Counteraction to Cyber Crimes: Legal Foundation of International Cooperation, 2002. Jurlitinform, 88 p.

[6] Federal Criminal Code and Rules: Title 18. Crime and Criminal Procedure. §1030 Fraud and related activity in connection with computers (amendment received to 15 February 1999). West Group, St. Paul, Minn. 1999

[7] USA Patriot Act of 2001, in the sphere of computer criminality and electronic evidence. http://www.crime-research.ru/articles/PatriotAct/4.

[8] United States Code Title 18, Part 1, Chapter 47, §1030 Computer Fraud and Abuse Act (CFAA). http://www.law.cornell.edu/uscode/text/18/1030

[9] Roose K. Here Come the Fake Videos, Too [Electronic resource] / K. Roose. — Mode of access: https://www.nytimes. com/2018/03/04/technology/fake-videos-deepfakes.html.

[10] Stover D. Garlin Gilchrist: Fighting Fake News and the Information Apocalypse / D. Stover // Bulletin of the Atomic Scientists. — 2018. — Vol. 74, iss. 4. — P. 283–288.

[11] Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities / A. Solodov [et al.] // Security Journal. — 2018. — Vol. 31, iss. 1. — P. 305–324.

[12] Digital Poly-Victimization: The Increasing Importance of Online Crime and Harassment to the Burden of Victimization / S. Hamby [et al.] // Journal of Trauma & Dissociation. — 2018. — Vol. 19, No. 3. — R. 383–384.

[13] Khaliullin A.I. Podkhody k opredeleniyu kiberprestupleniya // Rossiyskiy sledovatel'. 2015. N 1.

[14] Osipenko A.L. Setevaya komp'yuternaya prestupnost': teoriya i praktika bor'by: Monografiya. Omsk: Omskaya akademiya MVD Rossii, 2009. S. 103.

[15] Turyshev A.A. Informatsiya kak priznak sostavov prestupleniy v sfere ekonomicheskoy deyatel'nosti: Dis. ... kand. yurid. nauk. Omsk, 2006. S. 97.

[16] Filimonov S.A. Problemy bor'by s kiberprestupleniyami, sovershayemymi s ispol'zovaniyem bankovskikh kart // Sovremennoye pravo. 2015. N 3. S. 124.

[17] Bykov V.M., Cherkasov V.N. Ponyatiye komp'yuternoy informatsii kak ob"yekta prestupleniy // Zakonnost'. 2013. N 12. S. 37 - 40.