Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 06 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

TRENDS IN THE DEVELOPMENT OF CRIMINAL LIABILITY FOR CRIMES AGAINST THE SECURITY OF COMPUTER INFORMATION IN THE RUSSIAN FEDERATION

Mariya V. Talan[1]
Ramil R. Gayfutdinov[2]

Abstract: The development of modern computer technology and changes in federal legislation introduced in recent years, have caused the authors to identify the main trends in the development of criminal liability for crimes against the security of computer information: four areas that encourage the need to increase criminal liability for acts committed with computer technology. The paper also gives a historical overview devoted to the development of computer technologies and a general description of crimes in the field of computer information, taking into account changes introduced into criminal legislation by Federal Law No. 194-FZ dated July 26, 2017.

Keywords: crimes in the field of computer information, crimes against the security of computer information, cybercrime, the problems of crimes in the field of computer information

1. Introduction

The history of the development and spread of computer technology begins in the 1960s. Over the years, Ed Roberts has organised *MITS* (*Micro Instrumentation and Telemetry Systems*) as a small electronic company; in April 1974, he became interested in microprocessors manufactured by *Intel* Company, and at the end of 1974 a small company in Albuquerque (New Mexico) has created the first personal computer showing results and having much prospects [1]. Ed Roberts called it "*Altair*", it met the minimum definition of a microcomputer, and after assembly it represented from outside a metal box [2]. It had neither a keyboard nor a monitor; data input and output was carried out through the switch panel. The operation of the first computer was very complicated and required special knowledge of a programmer; when the

[1] Kazan Federal University, e-mail: gayfutdinov.r@yandex.ru. Tel.: 8 843 233 71 03.
[2] Kazan Federal University, e-mail: gayfutdinov.r@yandex.ru. Tel.: 8 843 233 71 03.

machine has been turning off, the program and data were lost, because the computer was equipped only with volatile RAM.

Computer diskettes for storing programs and data first appeared on the market in 1972 [3], then their size was 200x200x1 mm. These were simply smaller versions of the drives used on computers since 1956. Disk drives for new floppy disks were also cumbersome, but they were preferable to other data access devices, such as magnetic tape drives, tape readers, and tape recorders, because they allowed users to find the information they needed instead of doing fast-forward tapes first with other data.

Since the autumn of 1975, *MITS* has acquired the exclusive right to distribute a license for the first *Basic Microsoft* software. [4] However, a few months later, *Microsoft* found that its revenue was reduced to the limit. The reason for this was illegal copying. Bill Gates was directly involved in the development of the *BASIC language*. It was he who first declared the need for software protection, having addressed two open letters to the public. His actions contributed to the gradual introduction into the minds of the idea that the program is a product of creativity and therefore should be protected in the same way as musical compositions or a literary work.

Many years have passed since then. The problem of unauthorized interference is especially acute in countries with highly developed information networks. Developed as part of an initiative by the US Department of Defence in the US state of California, one of the first computer networks, ARPANET, in 1969 became the progenitor of the modern Internet network, which developed far beyond its original military and academic goals. Over the past decades, the Internet has become an exciting new public domain, which, because of its ability to circumvent geopolitical, economic and social boundaries, has traditionally not contained politics and no explicit social settlement [5, pp. 105-106]. Today, these milestones previously indicated in the literature are rapidly undergoing dramatic changes. The criminal codes of a number of countries have introduced rules providing for liability for illegal access to all or part of an automated data processing system, hindering the operation or violation of the correct

operation of such a system or entering information into it in a fraudulent manner, or destroying or modifying a database.

Computers have become an integral part of our lives and at the same time have generated a lot of problems of a socio-economic and legal nature. There are *four main areas* that need further development and improvement of the legal mechanism and encourage the need to strengthen legal responsibility for acts committed with and around computer technologies (so-called computer crimes).

2. Methods

Comparative legal and historical methods are chosen as the main research methods of the issues under consideration.

3. Results And Discussion

3.1 The first and most significant problem is the need to comprehensively counter the information threats faced by modern society and the state in the implementation of domestic and foreign policies. The course to digitalization has affected all socially significant and economic spheres of the state's development; the importance of electronic means of communication, and also receipt and dissemination of information is increasing. All this led to the approval in 2016 of the new Doctrine of Information Security of the Russian Federation and the Federal Law dated July 26, 2017, No. 187-FZ "On the Security of Critical Information Infrastructure". In Russia and in a number of foreign countries, laws have been enacted that increase criminal liability for attacks on state or critical computer information systems (for example, in France and in Kazakhstan).

3.2 Therefore, the *piracy problem* in the computer market and the Internet space has gradually faded *into the background*. Their common types are software piracy, audio piracy, video piracy, and piracy against literary works. In recent years, the way of distribution of the listed illegal products has undergone changes: if the circulation of such products was previously spread through the transfer of material data storage devices (CDs, DVDs), now they are actively distributed in all different peer-to-peer networks (e.g. torrents) or through cloud storage technologies

(cloud storages). Article 44 of the Constitution of the Russian Federation emphasizes the need to protect intellectual property. Any use of copyright objects without the consent of the author, including publication, reproduction, and distribution, is illegal. Software for computer technology is constantly replicated and distributed without the consent of the authors of such programs; it is offered to consumers at very low prices or completely free of charge. Apparently, this situation is partly due to the unavailability, high cost of genuine software for mass consumers and the lack of alternative offers, and, on the other hand, the growing needs of the domestic market for such products.

In such circumstances, it is undoubtedly necessary to ensure the implementation of the criminal law provisions on liability for violation of copyright and related rights.

3.3. As the *third situation,* one can identify an increase in the number of “traditional” crimes committed using computer technology. In recent years, theft of funds from electronic payment systems, bank accounts, plastic cards from individuals and in enterprises, institutions and organizations using remote banking services (Bank-Client systems) have become widespread among the mercenary crimes identified, using computer technology. The first crime of this kind was recorded in the former USSR in 1979 in Vilnius. Damage from such theft amounted to 78 584 roubles (at that time, embezzlement in an amount exceeding 10,000 roubles was recognized as large scale embezzlement). This fact was recorded in the international registry of offenses of this kind and was a kind of starting point in the development of a new type of crime in our country [6, p. 126].

Every year, such thefts were becoming increasingly common. From June to September 1994, a criminal group led by L., using an electronic computer telecommunication system *Internet* and overcoming several lines of protection against unauthorized access, and using a personal computer located in an office in St. Petersburg, entered false information into the cash management system "*City Bank of America* ". As a result of this crime, at least 49 money transfers totalling 1,010,952 US dollars were made from customer accounts of the named bank located in New York, to the accounts of persons belonging to

Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 06 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

their criminal group and living in six countries [7, p. 17].

According to Main Information and Analysis Center of the Russian Ministry of Internal Affairs, the number of crimes committed in the field of telecommunications and computer information, including crimes for which responsibility is provided for in Part 1 of Art. 138, Art. 138 [1], Article 272, Art. 273, Art. 274, Art. 146, Art. 158, Art. 159, Art. 165, p. 171 [2], Art. 183, art. 242, Art. 242 [1], Article 242 [2], is growing steadily. Such growth occurs mainly due to an increase in the number of thefts (Art.158 of the Criminal Code), committed using computer information and telecommunications, as well as fraud [8, pp. 93-94].

Table. Information on crimes committed in the field of telecommunications and computer information

Years	**2010**	**2011**	**2012**	**2013**
Number of recorded crimes	12698	7974	10227	11104
Years	**2014**	**2015**	**2016**	
Number of recorded crimes	10968	43816	65949	

Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 06 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

Undoubtedly, this state of affairs contributed to amendments by the Federal Law No. 111-FZ to the Criminal Code of the Russian Federation [9]. Part 3 of Art. 158, is supplemented by a new qualifying attribute: theft committed from a bank account, as well as in relation to electronic money (in the absence of signs of a crime under Article 159 [3] of the Criminal Code of the Russian Federation). The disposition of part 1 of Article 159 [3] is completely set forth in the new edition, which now provides liability for fraud using electronic payment methods, which expands the subject of this crime. Part 3 of Article 159 [6] is supplemented by a new qualifying attribute and strengthens the responsibility for computer information fraud committed from a bank account, as well as in relation to electronic money.

3.4 Fourth problem is the increase in cases of unauthorized access to computer information and the spread of malicious computer programs aimed at unlawfully affecting computer information, according to experts. In accordance with the Federal Law dated July 27, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection" [10], any documented information is subject to protection, the unlawful use of which may harm its owner, proprietor, user and other person.

As is known, the concept of computer crimes is broader than the definition of crimes in the field of computer information (crimes against the security of computer information). The legislator identifies a group of crimes against the security of computer information in the section of attacks on public safety and public order and does not indicate in any corpus delicti such qualifying feature as a crime using computer technology, although there is a narrower one: committing a crime using information and telecommunication networks (including the Internet). Given this position of the legislator, we can say that the term "computer crimes" has no criminal legal boundaries and can be used only in forensic or criminological aspects. Such a definition of computer crime from a criminalistic perspective is proposed by V. B. Vekhov. He understands computer crimes as socially dangerous acts provided for by criminal law committed using electronic computer equipment [7, p. 24]. The concept of "the use of computer

equipment" is singled out as the main classification criterion that a crime belongs to the category of computers, regardless of at what stage of the crime it was used: during its preparation, during the commission, or for concealment.

Interventions in the operation of a computer, the liability for which is established according to the offenses located in chapter 28 "Crimes in the field of computer information", are expressed in

- Unlawful access to computer information (Art.272);

- The creation, use and distribution of malicious computer programs (Art. 273);

- Violation of the rules for the operation of means used for storage, processing or transmission of computer information and information and telecommunication networks (Art. 274);

- Unlawful impact on the critical information infrastructure of the Russian Federation (Art. 274 [1]).

Computer information, a computer device, a computer system or a computer network, etc. can also act as an *object or means of committing crimes in the field of computer information*. Computer information may be contained in devices designed for its permanent storage and transfer. Today it's all different magnetic, optical and electronic data carriers: magnetic disks (hard drives, HDD), SSD disks, various memory cards (flash cards, USB flash drives, etc.), compact disks (CD, DVD, Blu-ray, etc.).

The generic object of crimes against the security of computer information is its security, i.e. a condition in which there is no harm or no threat of harm to the legitimate use of computer information. Therefore, for example, V.S. Komissarov offers the following definition: "computer information crimes are deliberate socially dangerous acts (actions or omissions) that cause harm or endanger the public relations governing the safe production, storage, use or dissemination of information and information resources or their protection "[11]. *A specific object of* the crimes *under* consideration is the security of the circulation of computer information, which is understood as the state of security (the absence of harm or its threat) to the processes of production, storage, use or dissemination of computer information.

Periódico do Núcleo de Estudos e Pesquisas sobre Gênero e Direito
Centro de Ciências Jurídicas - Universidade Federal da Paraíba
V. 8 - Nº 06 - Ano 2019 – Special Edition
ISSN | 2179-7137 | http://periodicos.ufpb.br/ojs2/index.php/ged/index

Crimes in the field of computer information can be divided into types based on the characteristics of the legislative *description of the act* on

- Unlawful access to computer information (Article 272, part 2 of Article274 [1]),

- The creation, use and distribution of malicious computer programs (Article 273, part 1 of Article 274 [1]) and

- Violation of the rules for the operation of means for storage, processing or transmission of computer information and information and telecommunication networks (Article 274, part 3 of Article274 [1]).

By the nature of the *focus of the* criminal act on the *main immediate* object of criminal protection can be divided into

1) Crimes encroaching on computer information of a general nature (Articles 272-274), and,

2) Encroaching in its narrower form - computer information contained in the critical information infrastructure of the Russian Federation. Criminal law provides for more severe penalties for attacks on the last specified type of information.

Unlike similar offenses in the legislation of other countries, the types of unlawful access to computer information and violation of the rules for operating storage facilities, processing or transmission of computer information and information and telecommunication networks are designed as material. Criminal liability is associated with the onset of certain consequences, and there are two types of consequences: a) destruction, blocking, modification or copying of information (Articles 272, 274); b) damage to the critical information infrastructure of the Russian Federation (parts 2 and 3 of art.274 [1]).

Many crimes against the security of computer information can be committed with various forms of guilt. According to the legislative structure of the corpus delicti, various types of intent and negligence may be inherent in them, but most often these are deliberate crimes.

Summary And Conclusions

Thus, *four* problems can be distinguished that affect the development and improvement of the legal mechanism of criminal liability for acts against the security of computer

information. This is the need for a comprehensive counteraction to the information threats faced by modern society and the state in the implementation of domestic and foreign policies, the problem of piracy in the computer market and the Internet space. In addition, there is the problem of increasing the number of "traditional" crimes committed using computer technology, the problem of increasing cases of unauthorized access to computer information and the spread of malicious computer programs aimed at unlawfully affecting computer information. They need further scientific development and require close attention from the legislative bodies and the scientific community.

Acknowledgments

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.

References

Rosa, Jerry "DR. H. EDWARD ROBERTS -- INVENTOR OF THE ALTAIR.(Technology Information)" // Computer Reseller News, Nov 13, 2000.

Goff, Leslie «Altair: Another PC Milestone. (Micro Instrumentation Telemetry Systems creates Altair, world's first computer kit, in 974) (Industry Trend or Event)» // Computerworld, June 28, 1999, p.83(1).

Wallis, Lawrence "The fading sound of cassette tape" // Printweek, May 24, 2007, p.24.

Watt, Peggy "No time for Gates to celebrate" // Network World, Oct 30, 1995, Vol.12(44), p.10.

D. Wall, "Cybercrimes: New Wine, No bottles?" // Invisible Crimes, Chapter 5, P. Davies et al. (eds), 1999. – pp. 105-106.

Baturin Yu.M. Computer law issues. - M. : Legal literature, 1991. - P. 126.

Vekhov V.B. Computer crimes: Methods of commission and disclosure / Edited by Academician V.P. Smagorinsky. - M.: Right and Law, 1996. - 182 p.

Efremova M.A. Criminal protection of information security. - M.: Yurlitinform, 2018. -- Pp. 93-94.

On Amending the Criminal Code of the Russian Federation: Federal Law of the Russian Federation dated April 23, 2018 No. 111-FZ: adopted by the State Duma of the Federal Assembly of the Russian Federation on April 10, 2018: approved by the Council of the Federation of the Federal Assembly of the Russian Federation on April 18, 2018// Collection of legislation of the Russian Federation. - 2018. - No. 18, article 2581.

On information, information technology and information protection: Federal Law of the Russian Federation dated July 27, 2006 No. 149-FZ: adopted by the State Duma of the Federal Assembly of the Russian Federation on July 08, 2006: approved by the Council of the Federation of the Federal Assembly of the Russian Federation on July 14, 2006// Collection of legislation of the Russian Federation. - 2006. - No. 31 (1 h.), Article 3448.

Komissarov V. S. Crimes in the field of computer security: concepts and responsibility // Legal World.1998. - No. 2