Infringements on Digital Information: Modern State of the Problem

E.Yu. Latypova[1], *E.V.* Nechaeva[2,*], *E.M.* Gilmanov[1] and *N.V.* Aleksandrova[2]
[*]Corresponding author: nechaeva_ev@mail.ru

[1]Kazan innovative University named after V.G. Timiryasov, Kazan, Russia.
[2]Chuvash State University named after I.N. Ulyanov, Cheboksary, Russia.

Abstract. Continuous expansion of the scope of network information technologies application permanently create the background for the appearance of new threats to the security of individuals, society and the state, including information security. Especially dangerous are terrorist acts potential threats by using information resources in the appropriate infrastructure of society and the state individual institutions. The current state of the problem of criminal liability for trespass to digital information, their dynamics and impact on Russia's technological and industrial potential, as well as the negative consequences of committing crimes in the sphere of digital information are considered in the article. A wide use of information and communication technologies (ICT) is an integral requirement of time representing an indicator of the development of a modern economy, both private and national, i.e. state. However, an increase in the share of information crime interferes with the progressive development of ICT. When using the methodological approach in science, measures of general prevention, as well as measures of special prevention aimed at digital crime countering are singled out. The most effective of them are special preventive measures, such as the current criminal, criminal procedure and information legislation improvement; the judicial practice improvement; the creation of new and improvement of existing methods of investigation and prevention of digital security crimes; the qualified personnel training in the field of information security (including specialized research institutes and government agencies of the relevant areas); as well as the need to keep within the necessary information security limits by the users themselves, both in the workplace and in everyday communication. This article is devoted to discussing some of these special preventive measures.

Keywords: “Digital information”, “computer information crimes”, “malware”, “information”, “illegal access to computer information”.

1 Introduction

Strengthening of the country's defence capacity and its national security largely depends on the active development of the informative society, both globally and nationally. Contemporary information and telecommunication devices have a truly large potential, but the process of their active use in all spheres of society has inevitably entailed a number of negative phenomena, such as a steady increase in the number of digital information offences.

2 Problem Statement

It seems necessary to analyze the current state of the problem of criminal liability for offences against digital information. In addition, the related issues of criminal responsibility for committing crimes with the use of computer and telecommunication technologies require consideration as well.

3 Research Questions

We consider it expedient to research social relations evolving in the sphere of criminal legal regulation of offences against digital information. Study the practice of rules applying on criminal liability for crimes in the sphere of digital information and on the basis of the data obtained, to determine the effectiveness of mentioned standards.

4 Purpose of the study

The purpose of the research is to clarify the criminal legal nature of infringements on digital information. Furthermore, it is necessary to provide rationale for proposals for improvement and enhancement of penal legislation efficiency in the field of criminal liability regulation for separate types of crimes in the sphere of digital information and practice of application of punishment for the crimes of this kind.

5 Research methods

Research methods are traditional for works of this kind. They cover both general scientific methods - dialectical, formal logic, analysis and synthesis and specific scientific ones - comparatively legal, logically legal, analysis of the documents, printed and electronic publications, as well as statistical methods.

6 Findings

The Criminal Code of the Russian Federation uses the term "crimes in the field of computer information", but it seems to us that this definition is excessively narrow due to the fact that modern development of science and technology has resulted in the widespread use of digital rather than computer information. One can support I.R. Begishev's opinion that "digital information refers to information (messages, data) circulating in informative and telecommunication devices, their systems and networks" [1]. It should be noted that regulatory legal acts of the Russian Federation contain synonymous terms, such as "computer information", "digital information" and "electronic information", that inevitably leads to certain confusion in terminology. We should also have in mind that the content of these concepts, despite their undoubted similarity, is different. At the same time, the most complete of these terms is exactly the "digital information" we use, since eventually all the information used in data and telecommunication networks comes down to the use of zeros and ones specific sequence.

There is a similar instability in interpreting this concept in criminology, where the terms "computer crimes", "high technologies crimes", "computer information crimes" are used [2]. One can state that at present the concept of "information security" goes through only its development stage [3], and the concept itself is only being formed and filled with specific content.

In our opinion, the acts provided for in Art. 138.1 ("Illegal circulation of special technical tools intended for secret receipt of information"), 159.6 ("Computer information fraud"), 272 ("Illegal access to computer information"), 273 ("Creation, use and distribution of harmful computer programs"), 274 (Violation of the operating rules of the means of storing, processing or transmitting computer information and data and telecommunication networks") and 274.1 ("Illegal impact on the critical informative infrastructure of the Russian Federation") of the Criminal Code of the Russian Federation should be attributed to infringements on digital information. It should be noted that the last of these offences (Art. 274.1 of the Criminal Code of the Russian Federation) was introduced into the Criminal Code of the Russian Federation only on July 26, 2017 (Federal Law No. 194 - FL) [4]. It should also be borne in mind that digital information can be used for committing crimes of other kinds as well [5], for example, bringing to suicide [6, 7], sexual harassment against minors or other persons [8, 9, 10] and some others. In particular, insurance fraud can also be committed by means of information and telecommunication technologies [11], Illegal drug trafficking has become widespread through information and telecommunication networks [12]. The use of ICT for the purpose of the ideology of terrorism, xenophobia, extremism propaganda, distribution of the ideas of national exclusivity, destabilization of the social political situation in the country, etc. can be referred to infringements on digital information as well.

Even the Doctrine of Information Security of the Russian Federation indicates the sophisticated methods, manners and means of committing digital information infringements, that is confirmed by statistical data [13]. Thus, only 23 computer information crimes were registered in Russia as of 1997, whereas in 2016 there were 1,748 of them, however, the actual figures far exceed the official statistics data [1].

According to the official data, in 2017, 90 587 computers and telecommunication technologies crimes were committed, 20424 of which were solved, meanwhile, 62404 obligatory preliminary investigation crimes were registered among them, but only 15 986 of which were solved. The crime detection was only 28,1%, which confirms our conclusion about the significant latency of the researched infringements. Were committed 1 883 crimes connected with computer information, 726 of which were revealed. As to non-obligatory preliminary investigation crimes, 28183 of which were committed connected with computer and telecommunication technologies, 98,2% of which were solved (27680 crimes), i.e. almost all acts committed in this way.

For the first eight months of 2018 (January-August), 107980 computer and telecommunication technologies crimes were committed, 20075 of which were solved. During this period were committed 80419 obligatory preliminary investigation crimes, 21081 of which were revealed. Directly in the sphere of computer information 1 653 crimes were committed, 383 of which were revealed, i.e. the detection rate was 28,1%. As to the non-obligatory preliminary investigation crimes, were committed 27561 crimes related to computer and telecommunication technologies, 27126 of which were solved, i.e. 98,4%, which is consistent with the data for 2017.

To predict digital information crime, one can use mathematical formulas proposed by some authors, who fairly notes that mathematical prediction methods enjoy objectivity, reliability and accuracy of the results obtained, provided that the mathematical model is chosen correctly [14].

An infringement on digital information should be understood as a required by criminal law, guilty committed socially dangerous act, violating the confidentiality, integrity, reliability and availability of protected by law digital information. This provision is supported by I.R. Begishev, who reasonably indicates that the protected properties of limited access digital information are its confidentiality, integrity and reliability, and publicly available information - its integrity, reliability and availability [1].

In particular, AVIRA, the producer of antivirus software, claims that more than 4,4 million web attacks are being committed daily in the world, therefore every Internet user needs reliable security and offers a new software antivirus product Internet Security Suite.

The use of forced, corrective or compulsory work in relation to persons who commit encroachment on digital information is interesting and promising. Note that forced labor has proven itself as a means of effective correctional impact not only in Russia, but in foreign countries as well [15, 16]. The use of the denial to engage in specified activities as an additional punishment seems to be also efficient [17], as well as compulsory labor [18], which, unfortunately, have not found practical application yet. With regard to public servants who have committed offenses against digital information, it is necessary to provide for a procedure of bringing to disciplinary liability [19].

At the same time, it is essential to avoid bringing persons who may have committed an infringement on digital information by chance, i.e. innocently, to criminal responsibility, as long as frequently the person committed such an offense does not acknowledge the very possibility of committing it [20], however, due to elementary imprudence, still creates such a delict. For example, this may relate to downloading a program or application from GooglePlay or the AppStore.

Unfortunately, the user, unaware of anything, quite often downloads malicious software when he acquires the necessary one in the AppStore or Google Play. Such software application can, for example, activate the speakers and listen to the sounds around, transmitting the received information to interested persons, for example, advertisers; either remove the user's data about his online cards, passwords, logins, etc., wherewith dishonest persons can attack the user's phone, or withdraw money from his electronic cards. Applications can collect fairly detailed information about the user, right up to the browser history or the user's home address and location, that, in principle, can be used to offer the client the so-called targeted advertising.

Certain problems arise in relation to metadata that are collected by separate messengers (for example, WhatsApp, Google and others) and then transfer these data in a generalized form to publicity companies. SEO - experts consider it to be a standard practice, which the user is informed of when reading these messengers privacy policies, only with the consent of which the user is able to continue working with a specific messenger. During operation a search engine analyzes the text sent by the user.

WhatsApp, for example, explains: "We collaborate with third-party organizations that help us to provide work, make available, improve, analyze, configure, maintain and promote our services. Providing information to these organizations, we require them to use your data in accordance with our instructions."

An obligatory requirement is the need to impersonalize the transmitted information, that excludes the possibility of obtaining information about a specific addressee, however, it should be noted there is some intersection between the use of digital information and the user's personal security [21], as well as the potential commission of religious, extremist [22] and terrorist crimes by using digital information [23-26].

Note that despite the fact that developers transmit data in an impersonal and encoded form on a server, wrongdoers can intercept the necessary information and decipher it. Such attacks are referred to as MITM (Man in the middle), and in order to counteract them, the developers have to check their applications to prevent wrongdoers' possible attacks.

7 Conclusion

The dominant factor of the development of information and telecommunication technologies is the current legislation of the country, including criminal laws, which reflects both the state policy in this area and the rules of conduct for legal entities and individuals in Russia. We believe that the whole complex of public relations connected with production of information proper, its distribution, use and access, both free and limited (confidentiality of information), can be attributed to information computer technologies legislation.

We consider it necessary to change the name of art. 159.6 "Fraud in the field of computer information" into "Fraud with the use of digital information", more appropriate to its content. This proposal has been expressed by theoretical scientists more than once (for example, by I.R. Begishev [1]), but legislators have not accepted it yet.

It is necessary to work out a mathematical model to prevent infringements on digital information to realize the possibility of determining the future and predict the results of social, economic and political changes. This provision is supported by the conclusions of S.V. Maksimov, Yu.G. Vasin and K.A. Utarov [27]. The growing ICT potential of foreign states and as a result arising challenges and threats to the science, state authorities, industrial complex, etc. prove this.

References

1. I.R. Begishev, *The concept and types of crimes in the sphere of circulation of digital information*. Extended abstract of PhD dissertation. Kazan: Kazan Federal University. Retrieved from: https://kpfu.ru/dis_card?p_id=2404 (2017). [in Rus.].

2. I.A. Mochalov, O.B. Shalaginova, Crime in the field of information and telecommunication technologies as a threat to the national security of the country. *Crime in the Field of Information and Telecommunication Technologys: Problems of Prevention, Detection and Investigation of Crimes*, **1**, 131-136 (2016). [in Rus.].
3. A. Shobodoeva, Development of the concept of "information security" in the scientific and legal field of Russia. *Bulletin of Baikal State University*, **27**(1), 73-78. DOI: 10.17150 / 2500-2759.2017(1).73-78 (2017).
4. *Federal Law "Criminal Code of the Russian Federation"* from 13.06 1996 N 63 –FZ. Retrieved from: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=315095&fld=134&dst=1000000001,0&rnd=0.7147173970765794#05396867035252704. Accessed: 26.11.2018 (1996). [in Rus.].
5. K.N. Evdokimov, N.N. Taskaev, Problems of Qualifying Crimes Under Article 273 of the Criminal Code of the Russian Federation at the Stage of Initiating Criminal Proceeding. *Russian Journal of Criminology*, **12**(4), 590-600. DOI: 10.17150/2500-4255.2018.12(4),590-600 (2018).
6. A.I. Bastrykin, Online crimes against minors: to the issue of victimological prevention and criminal law assessment. *Russian Journal of Criminology*, **11**(1). 5-12. DOI: 10.17150/2500-4255.2017.11(1).5-12 (2017). [in Rus.].
7. A.M. Bychkova, E.L. Radnaeva, Incitement to suicide with the use of internet technologies: socio-psychological, criminological and criminal law aspects. *Russian Journal of Criminology*, **12**(1), 101-115. DOI: 10.17150/2500-4255.2018.12(1) 101-115 (2018). [in Rus.].
8. D. DeHart, G. Dwyer, M.C. Seto, R. Moran, E. Letourneau, D. Schwarz-Watts, Internet sexual solicitation of children: A proposed typology of offenders based on their chats, e-mails, and social network posts. *Journal of Sexual Aggression*, **23**(1), 77-89 (2017).
9. E. Lievens, Bullying and sexting in social networks: Protecting minors from criminal acts or empowering minors to cope with risky behaviour? *International Journal of Law, Crime and Justice*. **42**(3), 251-270. DOI: 10.1016/j.ijlcj.2014.02.001 (2014).
10. E. Quayle, E. Newman, An exploratory study of public reports to investigate patterns and themes of requests for sexual images of minors online. *Crime Science*. **5**(1), 21. DOI: 10.1186/s40163-016-0050-0 (2016).
11. E.Yu. Latypova, Insurance fraud as a trespass on consumers' rights: problems and prospects. In G.P. Kuleshov and I.G. Garaev (Eds.), *Actual problems of legal regulation and law enforcement practice in the field of protection of the consumers. Materials of the All-Russian scientific and practical conference*(pp. 78-81). Kazan: LLP "JurExPraktik" (2017). [in Rus.].
12. M.R. Umarov, E.V. Nechaeva, Drug trafficking in the Internet. In A.Yu. Alexandrov (Ed.), *Criminal legal prevention in the sphere of drug trafficking or psychotropic substances, alcoholic and spirit-containing products (regional aspect)* (pp. 349-353). Cheboksary, Russia: Chuvash State University (2015). [in Rus.].
13. *Decree of the President of the Russian Federation "On the Doctrine of Information Security of the Russian Federation approval"* from 05.12.2016. N 646- FZ. Retrieved from: http://www.consultant.ru/document/cons_doc_LAW_208191/. Accessed: 07.11.18 (2016). [in Rus.].
14. A. Sukhodolov, S. Ivantsov, T. Molchanova, B. Spasennikov, Digital criminology: Mathematical methods of prediction (part 2). *Russian Journal of Criminology*, **12**(2), 230-236. DOI: 10.17150/2500-4255.2018.12(2).230-236 (2018).
15. A.A. Krymov, A.V. Rodionov, A.P. Skiba, Certain aspects of the interbranch regulation of the convictis' labor organization in France. *Journal of Advanced Research in Law and Economics*, **8**:1(23), 97-102. DOI: 10/14505/jarle.v8.1(23).11 URL: https://journals.aserspublishing.eu/jarle/article/view/1134 (2017).
16. A.A. Krymov, A.V. Rodionov, A.P. Skiba, Legal regulation of the convicts' labor organization in penitentiary institutions of Germany. *Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, **1**(37), 41-46 (2017). [in Rus.].
17. E.M. Gilmanov, E.Y. Latypova, Some problems of punishment for illegal search and (or) withdrawal of archaeological objects out of the places of occurrence. In F.M. Editor (Ed.), *Legal and moral aspects of ensuring of the individual and state's security at the present stage of political and economic sanctions*. *Collection of materials of the All-Russian scientific and practical conference: in 2 books* (pp. 361 – 363). Cheboksary, Russia: Chuvash State University (2016). [in Rus.].
18. E.V. Nechaeva, Prospects for transformation of punishment in the form of compulsory labor. *Criminal and Executive Law*, **13**(1), 45-49 (2018).
19. O. Lutsenko, Bringing civil servants to liability for disciplinary misconduct in judicial practice of Ukraine, Poland, Bulgaria and Czech Republic. *Journal of Advanced Research in Law and Economics*, **8:***1*(23), 103-112. DOI: 10/14505/jarle.v8.1(23).12 (2017).
20. I.V. Makeeva, S.V. Tasakov, A.V. Mishin, Y.G. Sled, A.Y. Epikin, L.M. Zeinalova, Protection of the witnesses and victims: International legal acts, legislation of some states and the modern Russian legislation. *Journal of Advanced Research in Law and Economics*, **7**(2), 313-322 (2016).
21. O.A. Zaytsev, A.V. Grinenko, I.V. Makeeva, L.M. Zeinalova, S.V., Tasakov, Y.G., Sled, … A.V. Mishin, Problem of definition of personal security in the modern Russian criminal procedure. *Journal of Advanced Research in Law and Economics*, **7**(6), 1533-1539. DOI: 10.14505/jarle.v7.6(20).35 (2016).
22. A.G. Nikitin, Types and classifications of extremist behavior: General theoretical and legal problems. *Topical Problems of Economics and Law*, **1**(29), 186-194. DOI: 10.21202/1993-047X.08.2014.1.186-194 (2014). [in Rus.].

23. T.Y. Khabrieva, Counteraction to the legalization (laundering) of proceeds from crime and the financing of terrorism in the context of the digitization of economy: Strategic objectives and legal solutions. *Russian Journal of Criminology*, **12**(4), 459-467. DOI:10.17150/2500-4255.2018.12(4).459-467 (2018).
24. V.P. Kirilenko, G.V. Alekseev, Actual problems of extremism crime counteraction. *Russian Journal of Criminology*. **12**(4), 561-571. DOI: 10.17150/2500-4255.2018.12(4).561-571 (2018).
25. E.K. Kuzmina, E.Yu. Latypova, Criminal and legal control of terrorist activities. *National Security and Strategic Planning*, **4**(12), 56-58 (2015). [in Rus.].
26. A.S. Yarusova, E.Yu. Latypova, The motive of national or religious hatred or hostility as a terrorist crimes element In N.V. Huraskina (Ed.), *Legal and moral aspects of ensuring of the individual and state's security at the present stage of political and economic sanctions. Collection of material of the All-Russian scientific practical conference: in 2 books* (pp. 593-597). Cheboksary, Russia: Chuvash State University. Retrieved from: https://elibrary.ru/item.asp?id=26041791 (2016). [in Rus.].
27. S.V., Maksimov, Yu.G. Vasin, K.A. Utarov, Digital criminology as a tool for combating organized crime. *Russian Journal of Criminology*, **12**(4), 476-484. DOI: 10.17150/2500-4255.2018.12(4).476-484 (2018).