ANALYSIS OF RUSSIAN JUDICIAL PRACTICE IN CASES OF INFORMATION SECURITY

[a]ALEXANDRA YURYEVNA BOKOVNYA, [b]ILDAR RUSTAMOVICH BEGISHEV, [c]IGOR IZMAILOVICH BIKEEV, [d]ILHAMIYA RUSLANOVNA ALMUHAMEDOVA, [e]DIANA DAVLETOVNA BERSEI, [f]NATALIA BORISOVNA NECHAEVA

[a]Ph. D. in Law Faculty of Law, Department of Criminal Law Kazan Federal University Kazan, Russia
[b]Ph. D. in Law Senior Researcher Kazan Innovative University named after V.G. Timiryasov Kazan, Russia
[c]Doctor of Law Department of Criminal Law and Procedure Kazan Innovative University named after V.G. Timiryasov Kazan, Russia
[d]Master of Law Department of Civil and Business Law Kazan Innovative University named after V.G. Timiryasov Kazan, Russia
[e]Ph. D. in Law Department of Legal and Special Disciplines Stavropol branch of RANEPA Stavropol, Russia
[f]Ph. D. in Law Department of Constitutional and International Law Stavropol Institute of Cooperation (branch of Belgorod University of Cooperation, Economics and Law) Stavropol, Russia
E-mail: [a]kafedra.ksu@yandex.ru, [b]bikeev@ieml.ru, [c]bikeev@ieml.ru, [d]airilya7@gmail.com, [e]di.bersej2012@yandex.ru, [f]natalyanechaeva18@gmail.com

Abstract: The article discusses the main trends in information security, reflected in the judicial practice of the Russian Federation in the last period. The authors made a conclusion that modern judicial practice today considers various aspects of cases related to information security. These are cases related to violation of confidentiality of information, disclosure of personal data, falsification of electronic documents, unauthorized access to computer information, distribution of malicious computer programs, violation of information protection rules, illegal activities in the field of information protection, disclosure of information with limited access, violation of order posting information, etc. Every year the number of such cases pending before the courts is growing. This confirms the relevance of the considered problem and indicates the need to return to its consideration in the near future.

Key words: court, judicial practice, offense, crime, cybersecurity, information security, digital technologies, information protection, cybercrime, secrecy, confidentiality.

1 Introduction

Information security involves the protection of information from theft or change, either accidental or intentional. The organization's information security system is an effective tool to protect the interests of information owners and users. It should be noted that damage can be caused not only by unauthorized access to digital information. It can be obtained as a result of a breakdown in telecommunication equipment. Effective organization of ensuring information security of banking systems and government institutions is especially relevant.

In this regard, knowledge of ways to protect the information infrastructure from criminal assaults is increasingly gaining its relevance (Begishev et al., 2019). Computer attacks (Begishev et al., 2019) and other information security incidents negatively affect the organization's productivity (Malik & Islam, 2019) and its cybersecurity status (Khisamova et al., 2019) in the context of digital crimes (Bokovnya et al., 2019), including by hacker communities (Begishev, 2020).

Thus, the analysis of judicial practice is a study in the field of law enforcement, which analyzes and systematizes judicial cases of information security, highlights the persistent differences in the application of legislation by the courts, as well as identify the causes and conditions that contribute to this, and develops suggestions and recommendations. The generalization of judicial practice makes it possible to identify cases of the adoption of various judicial acts relating to the same issues of law, to analyze different interpretations of the law, errors in the application of substantive and procedural law, and also to determine the reasons and conditions for their formation.

2 Materials and methods

The research materials were judicial practice in cases of information security in the Russian Federation.

A sample analysis of the indicated judicial practice over the past few years has been carried out. We examined a number of Russian laws that provide for liability for violations of information security. These are Articles 138.1, 159.6, 183, 185.6, 272-274.1, 283-284 and 310 of the Criminal Code, Articles 5.53, 13.11-13.14, 13.27.1, 13.33-13.34, 14.30, 15.21, 17.13, 20.23 and 20.24 of the Administrative Code of the Russian Federation.

To search for judicial decisions, we used the largest database of judicial acts, court decisions and regulatory documents in the Russian segment of the Internet - the Internet resource "Judicial and regulatory acts of the Russian Federation" (sudact.ru).
To find a judicial decision on the specified site, we used the number and name of a specific article of codes and the time period. In addition, the search for court decisions was carried out on thematic and industry sites.

3 Results and Discussion

The complexity of the search for judicial practice covering cases of information security is due to the fact that the volume of such practice is relatively small, the articles themselves are rather fragmented, and it is very difficult to compare and generalize the data of such rules.

Judicial practice indicates that a very important aspect is the need to comply with formal rules, organizing a trade secret regime. In particular, the Kolomna City Court considered the petition regarding the reinstatement of a plant employee who was charged with violating the trade secret regime. The personnel were allowed to enter the enterprise according to the rules governing official and commercial secrets, and also had to be guided by the Regulation on commercial secrets, where its regime was established, and the List of information that was included in the category of "commercial secrets". At the time of the disputed relationship between the employee and the employer, all the documents were valid, and together with other employees the plaintiff was acquainted with them, as evidenced by his signature on the List of reviewed documents.

After a while, the management of the enterprise limited the employee's access to trade secrets, but after a certain time working materials with the "CS" (commercial secret) signature stamp were found on his desk. The disciplinary action was confirmed by the management of the company, an act was drawn up on the fact of the audit, and photography was also conducted. The employee could not explain the reason for the presence of the indicated documents on his desk. Since the employee had previously been subject to disciplinary sanctions for violating commercial secrets (copying information, taking drawings out of the organization's territory, etc.), the court recognized the dismissal as legal, since the employee did not make the proper conclusions, and he did not comply with the requirements of the management.

Part of the court decisions is devoted to the problems of interaction between bank management and customers. In particular, an administrative fine was imposed on the head of the department for working with distressed assets of a branch of one of the banks. The reason for the punishment was that his subordinate decided to find out where the debtor was by contacting the employer of the latter. According to the court, there were actions to disseminate information about the presence of debt on credit obligations to the bank. Also, a bank employee collected information using unacceptable methods.

A quite large number of court cases examined are devoted to claims for the protection of personal data. In particular, a client

of one of the banks applied to the prosecutor's office with a statement that her rights to protect personal data were violated. The audit materials showed that one of the borrowers informed the bank of her personal data, presenting the applicant as a contact person. According to the court decision, the established procedure for processing personal data was violated - an indefinite number of persons received access to personal data, while the subject of personal data did not give his consent. This offense is not continuing; the date of the offense event can be considered the moment of acceptance of the relevant data from the borrower. This offense entails punishment under part 1 Article. 4.5 Administrative Code of the Russian Federation, but the presence of a three-month period of prosecution should be considered. Given that the expiration has already taken place, no punishment is prescribed by law.

A significant part of the disputes regarding the problem of the dissemination of personal data is disputes with the media that publish information regarding the personal lives of citizens. The Supreme Court passed a resolution that Roskomnadzor received the right to decide on the closure of a particular media if it was charged with regularly disseminating information about the personal lives of citizens or otherwise violating personal data laws. For example, one of the newspapers in the Krasnodar Territory included information about a minor in her publication: her first name, surname and even her school number. A written warning of the department was sent to the publication, but the newspaper continued to publish personal data of minors. The regional court, by its decision, terminated the activities of the newspaper, and the materiality of the case and the legality of its decision was confirmed by the Supreme Court of the Russian Federation (Decision of the investigative committee on Administrative Cases of the Supreme Court of the Russian Federation of June 24, 2015).

Along with the closure of the publication, the court may also require it to pay compensation for non-pecuniary damage. So, according to the court in St. Petersburg and the Leningrad Region, it was defined as a violation of the publication of a photograph of a citizen, as well as his information, while the citizen did not give consent to the distribution of personal data. The court recovered from the A. newspaper in favor of the aforementioned citizen moral damage because his personal data were published.

Another issue submitted to the courts is the provision of personal data at the request of state authorities. The law expressly prohibits their distribution, respectively, the operators, not wanting to risk receiving an order from Roskomnadzor, responds by refusing requests from government agencies, including the FAS, related to personal data of citizens. In particular, one of the requests of the FAS concerned information about the owner of the telephone number, regularly used to send numerous advertising messages. After refusing to provide such data, the organization was fined. The court concluded that the actions of the FAS Russia are legal in nature, as the telecom operator had to provide the personal data requested.

An analysis of the practice also revealed typical problems of medical or educational institutions that provide various services to the population, but at the same time they do not ask for consent not to process personal data from clients. In particular, the specialists of the clinic in the Samara region, conducting medical examinations, entered personal data of citizens into outpatient cards without obtaining the consent of patients. This violation has led to the prosecution of the director of a medical organization under Article 13.1 Administrative Code of the Russian Federation.

“Ignoring issues of embezzlement of property of another or acquisition of the right to another's property in electronic information circulation seems unacceptable. Many people mistakenly believe that digital technology is reliably protected from fraud. Such a postulate is false, which is proved by a large number of practical examples” (Begishev, 2016).

According to Article 159.6 of the Criminal Code of the Russian Federation, interference with the functioning of means of storage, processing or transmission of electronic information or the information and telecommunication networks is recognized as the targeted impact of software and/or software and hardware on servers, computer equipment (computers), including portable laptops, tablet computers, smartphones equipped with appropriate software, or to information and telecommunication networks, which violates the established process of processing, storage, transmission of computer information, which allows the guilty person or another person to illegally seize other people's property or acquire the right thereto (Resolution of the Plenum of the Supreme Court of the Russian Federation of November 30, 2017 No. 48, 2017).

Electronic information fraud committed through unauthorized access to computer information or through the creation, use and distribution of malicious computer programs requires additional qualifications under Articles 272, 273 or 274.1 of the Criminal Code of the Russian Federation (Resolution of the Plenum of the Supreme Court of the Russian Federation of November 30, 2017 No. 48, 2017).
For example, embezzlement of funds from an "electronic wallet", requires first to obtain an access code for this wallet. If a person breaks it with the help of technical means and steals money, actions will be qualified according to Articles 159.6 and 272 of the Criminal Code. The practice follows the same way if property theft occurs using malicious computer programs (Article 273 of the Criminal Code of the Russian Federation) (Saushkin et al., 2019).

Judicial practice is faced with another problem when applying Article 273 of the Criminal Code. The previous version of this rule provided only such malicious programs that could obviously lead to criminal consequences. The criminal law has fought against illegal activities of a fairly limited circle of people (hackers, computer fraudsters, etc.) (Korobeev et al., 2019).

Speaking about legal tools as means of information security, it should be noted that the potential of criminal law means (Efremova, 2017; Efremova, 2015) and modern Russian criminal policy (Rogova et al., 2016; Efremova et al., 2019; Khisamova et al., 2020) is least used.

One of the most common disputes in judicial practice are disputes with copyright holders. The number of claims increases every year. This category of cases is the most expensive. Thus, defendants in this category of cases are people who publicly post information that is owned by other citizens. At the same time, if the disseminated disputed information object is distributed at the request of the site owner by its users, the site owner is also responsible.

An important aspect of judicial practice is disputes related to theft of funds through remote banking channels. These cases are resonant in nature, while the courts now not only blame the client of the bank for concluding an agreement and taking all the risks of electronic payments, but they also evaluate the safety of bank payments directly. According to court decisions, a number of cases had inconsistency of the bank’s actions revealed, which allowed the client of such a bank receive the right to reimburse the entire stolen amount, as well as to pay the costs of the examination. Accordingly, today the courts impose increased requirements on the safety of banks.
Just a while ago, Russian judicial practice had practically no examples of criminal prosecution for the falsification of electronic documents. But modern judicial practice testifies to the fact that today there are a number of court decisions where financial data, certificates of income of individuals and various agreements are recognized as the subject of a crime.

Courts expressly indicate that the electronic form of compilation, storage and submission of documents does not exclude the presence of corpus delicti in the actions of the subject. Thus, in accordance with Article 327 of the Criminal Code, these documents correspond to the characteristics of an official

document, but the form of its submission to the court does not matter.

4 Summary

Judicial practice in cases of information security is determined by its specific features and moments. As a rule, similar court decisions on the considered category of cases in different constituent entities of the Russian Federation are similar. This state of affairs greatly facilitated the analysis of Russian judicial practice in cases of information security. We should note that the scope of this research is not enough to analyze the entire volume of judicial practice in cases in the field of information security. Perhaps a detailed analysis of each category of cases will be carried out in subsequent studies.

5 Conclusion

Thus, we may summarize that modern judicial practice today considers various aspects of cases related to information security. These are cases related to violation of confidentiality of information, disclosure of personal data, falsification of electronic documents, unauthorized access to computer information, distribution of malicious computer programs, etc. Every year the number of such cases pending before the Russian courts is growing. This confirms the relevance of the considered problem and indicates the need to return to its consideration in the near future.

Acknowledgments

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

Literature:

1. Decision of the investigative committee on Administrative Cases of the Supreme Court of the Russian Federation of June 24, 18-APG15-7. 2015. The text of the decision has not been officially published.
2. Resolution of the Plenum of the Supreme Court of the Russian Federation of November 30, 2017 No. 48 “On judicial practice in cases of fraud, misappropriation, and embezzlement”. 2017. Rossiiskaia Gazeta, 280.
3. Begishev, I. R.: Organization of the hacker community: criminological and criminal law aspects. *All-Russian Criminological Journal*, *14*(1), 2020. 96-105.
4. Begishev, I.R.: Some issues of combating fraud in the field of computer information. *Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*, 3(25), 2016. 112-117.
5. Begishev, I.R., Khisamova, Z.I., Bokovnya, A.Y.: Information Infrastructure of Safe Computer Attack. *Helix*, 9(5), 2019. 5639-5642.
6. Begishev, I.R., Khisamova, Z.I., Mazitova, G.I.: Criminal Legal Ensuring of Security of Critical Information Infrastructure of the Russian Federation. *Revista Gênero & Direito*, 8(6), 2019. 283-292.
7. Bokovnya, A.Y., Khisamova, Z.I., Begishev, I.R.: Study of Russia and the UK legislations in combating digital crimes. *Helix*, 9(5), 2019. 5458-5461.
8. Efremova, M.A.: The protection of information constituting commercial, tax and banking secrecy by means of criminal law. *Vestnik Permskogo universiteta. Juridicheskie nauki = Perm University Herald. Yuridical Sciences*, 1(27), 2015. 124-132.
9. Efremova, M.A.: Social Conditionality of Criminal Law Protection of Information Security in the Russian Federation. *Vestnik Permskogo Universiteta. Juridicheskie Nauki = Perm University Herald. Juridical Sciences*, 36, 2017. 222-230.
10. Efremova, M.A., Rogova, E.V. et al.: Trends of Modern Russian Criminal Policy in the Russian Federation. *Journal of Advanced Research in Law and Economics*, 10(1(39)), 2019. 144-154.
11. Khisamova, Z.I., Begishev, I.R., Latypova, E.Yu.: Digital crime in the context of a pandemic: main trends. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 14(3), 2020. 96-105.
12. Khisamova, Z.I., Begishev, I.R., Sidorenko, E.L.: Artificial Intelligence and Problems of Ensuring Cyber Security. *International Journal of Cyber Criminology*, 13(2), 2019. 564-577.
13. Korobeev, A.I., Dremlyuga, R.I., & Kuchina, Ya.O.: Cybercrimes in the Russian Federation: criminological and criminal law analysis of the situation. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 13(3), 2019. 416-425.
14. Luneyev, V.: *Crime of the 20th century. World, regional and Russian trends*. Moscow, 1997. 309-325.
15. Luneyev, V.: *Crime of the 20th century. World Criminological Analysis*. 1999. Moscow.
16. Malik, M.S., & Islam, U.: Cybercrime: an emerging threat to the banking sector of Pakistan. *Journal of Financial Crime*, 26(1), 2019. 50-60.
17. Rogova, E.V., Karnovich, S.A., Ivushkina, O.V., Laikova, E.A., Efremova, M.A.: State of the Contemporary Criminal Law Policy of Russia. *Journal of Advanced Research in Law and Economics*, 7(1), 2016. 93-99.
18. Rose-Ackerman, S., & Palifka, B. J.: *Corruption and government: Causes, consequences, and reform*. 2016. Cambridge university press.
19. Saushkin, D.V., Shulgina, D.D., & Korchagina, M.A.: *Rights and obligations of an entrepreneur in relations with law enforcement agencies: law and practice*. M.: Editorial office of “Rossiiskaia Gazeta", 2019. 160 p.
20. Starkov, O.: The model of causes and conditions of transnational crime. In *New criminal realities and the response to them*. 2005. Moscow.

Primary Paper Section: A

Secondary Paper Section: AD, AG