Criminal Legal Support for Safeguarding the Citizens' Digital Rights

Ildar Begishev[1,*], *Danila* Kirpichnikov[1], *Elvira* Latypova[1], *Elena* Nechaeva[2], and *Sergei* Tasakov[2]

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

Abstract. The article discusses the active introduction of technologies based on the use of artificial intelligence, the activities of which entail the storage, transmission and processing of information circulating in information and telecommunication devices, their systems and networks. The article indicates that the amount of computing power of artificial intelligence technologies can significantly change the foundations of the functioning of information legal relations and, accordingly, the procedure and conditions for the implementation of digital rights of citizens. The inevitability of computer attacks on automated information systems using artificial intelligence, as well as the possibility of its misuse, create significant criminological risks of unauthorized access and use of citizens' digital rights by subjects through these technologies. The article examines the criminal law support for the protection of digital rights of citizens as a priority direction in the development of theory and practice of the application of criminal law institutions in the global, national and regional dimensions. The initial theses formulated in this study can be used in the future when building state policy and developing legal regulation of relations in the context of industrialization and digitalization.

1 Introduction

The President of the Russian Federation V.V. Putin in his Address to the Federal Assembly of the Russian Federation of 2019 has designated the scientific and technological development of the country as an absolute national priority and issued an order to develop a general scheme for the development of the digital economy infrastructure, which includes information and telecommunication systems and networks, as well as hardware and software systems for storing, processing, and transmitting digital data. Attention is drawn to the special role of digital technologies in the aforementioned document of state planning. This circumstance reflects the well-established and consistent state policy aimed at stimulating the digitization of public relations. In order to substantiate the above theses, let us turn to the provisions of the Strategy for the Development of the Information Society approved by the Decree of the President of the Russian Federation dated May 9, 2017, No. 203, which establishes as the basic principles of development—ensuring the rights of

* Corresponding author: begishev@mail.ru

citizens to access information, as well as legitimateness and reasonable sufficiency in the collection, accumulation information about citizens and organizations [1].

The recognition of these priorities at such a high level is not accidental. A tendency that does not require special confirmation has become the placement by citizens of significant amounts of data in information and telecommunication systems and networks, which, in the absence of adequate provision with systems for digital information protection, creates threats of illegal access to it, interception and registration from transmission channels.

The obvious dissonance between the recorded facts of illegal access and bringing to responsibility established by law indicates problems in the practice of detecting, preventing, suppressing, disclosing, and investigating crimes that encroach on digital information.

The development of digital technologies makes it possible to realize a significant part of the interests and needs of a person through the use of information and telecommunication devices, their systems and networks. The processing of large amounts of data by automated information infrastructure management systems has become widespread, and the practice of storing personal data and confidential information of commercial organizations in cloud-based information technology models of providing ubiquitous access has become established. Digital information forms the basis of the organization of modern information relations [2].

By transferring their own confidential data to counterparties in digital networks, users often neglect to ensure their protection against unlawful use, as a result of which current court practice is characterized by an increase in the number of claims for personal data protection. We also agree with the fears of an increase in the uncontrolled distribution of electronic messages containing illegally obtained digital data of citizens, which are used to exert undue influence on them in order to generate profit [3].

The above theses are confirmed by the data of official statistics, according to which there is a tendency towards an increase in the number of frauds using electronic means of payment and in the field of computer information, facts of illegal access to digital information, its destruction, blocking, modifying, and copying.

In this regard, the knowledge of ways to protect digital information from criminal encroachments is becoming increasingly important [4-8]. Computer attacks [9-10] and other information security incidents negatively affect the performance of the organization [11-14] and the state of its cybersecurity in the face of digital crimes [15], including in the context of a pandemic [16-17] and the development of artificial intelligence [18-29].

Indeed, due to its characteristics, digital information and, accordingly, the rights, arising in relation to it, is a profitable resource. The State needs to create legal models for the protection of public relations and the prevention of encroachments on digital rights. At the same time, scholars investigating the possibilities of the current legislation on information security reasonably come to the conclusion that the lack of systematization of the norms governing the entire set of information protected by law has a negative effect on the process of their application [30].

2 Materials and methods

The materials for the work have been papers posted in domestic and foreign academic journals and on websites on the Internet, as well as Russian legal acts.

The methodological basis of the research is a set of methods of scientific cognition, including methods of abstract logical, comparison, and correlation analysis.

3 Results and discussion

Modern resources of digital information circulation give rise to new types of acts prohibited by the criminal law aimed at seizing and manipulating it, which substantiates the claims of researchers that information security is a priority in the development of protective legal rules [31].

This thesis forms the basis for further reasoning that digital information is the subject matter of any subjective digital law.

Let us reconcile the reasoning with the fact that, according to the form of representation, digital information can be an electromagnetic signal, a documentary message, a file, a program for a computer, a database [32], from which it follows that the subject matters of digital rights are digital information; and by appearance, by a form, they can be presented as various objects of intellectual property, information of a confidential nature, materials of commercial negotiations, if they are carried out through digital channels.

Thus, it seems possible to state that computer programs created by citizens, apps for digital devices, messages transmitted by them over telecommunication networks containing acoustic or video information, information entered into electronic databases constituting personal data, transmitted information about private life, financial transactions made through computer apps are inherently digital information, from which it follows that these types of digital information constitute the subject matter of the citizens' digital rights, since they are what social relations arise about.

For example, the right of a citizen in relation to his/her funds transferred by means of electronic payment can be recognized as a digital right, since in this case, the subject matter of the legal relationship is the transmitted digital information.

We believe that the modern conditions for the functioning of the digital space form a significant number of criminological risks of illegal access to digital information, which is the object of the citizens' digital rights, which predetermines the need, on the one hand, to use more effective legal remedies for its protection, and, on the other hand, to work on drawing up a constructive criminal legal policy on the protection of the most significant public relations arising from digital information.

The increasing complexity of the procedure and methods of using modern information and telecommunication devices creates risks of illegal obtaining of information about the private life of users by third parties. At the same time, users often pose a threat of data leakage by their own victim behavior, neglecting considerations of the safe use of information and telecommunication devices. With the increase in the sphere of digital information circulation, there are new ways of committing acts that encroach on digital information circulating, for example, in mobile networks, satellite communications, as well as in wireless access networks.

Based on the foregoing, it seems possible to state that information, messages (data) circulating in information and telecommunication devices, their systems and networks are subject to the subjective digital rights of citizens, which allows us to give it the following definition: the subjective digital right of a citizen is the type and measure of possible behavior of an authorized person established by law regarding information belonging to him/her, on the right of ownership or other legal basis, circulating in information and telecommunication devices, their systems and networks.

4 Conclusions

Modern conditions for the development of information and telecommunication devices, their systems and networks, an increase in the flow of digital information and its mediocre protection against unlawful influence, especially interception and registration, necessitates the study of issues of protecting the citizens' digital rights by criminal legal remedies, since

it is a criminal law that acts as the guarantor and the most effective regulator of social stability, protecting the most significant social relations.

Development of digital data flows, digital storage of monetary assets, intellectual property items, personal data, implementation of telephone conversations through digital devices, including in the framework of entrepreneurial activities, as well as the emergence of significant criminological risks caused by these trends and the multiplication of forms of encroachment on digital information confirm the thoughtful, well-grounded, and motivated position of the President of the Russian Federation expressed in the Decree, which, as a national interest in the information sphere, envisages the provision and the protection of constitutional human and civil rights and freedoms in terms of obtaining and using information, personal privacy when using information technologies [33].

Furthermore, we note that technologies based on the use of artificial intelligence are actively being introduced into modern digital legal relations, the activity of which entails the storage, transmission, and processing of information circulating in information and telecommunication devices, their systems and networks. The thesis that the volume of the processing power of artificial intelligence technologies is capable of significantly changing the foundations of the functioning of information legal relations, and, accordingly, the procedure and conditions for the implementation of the citizens' digital rights, does not require special confirmation. The inevitability of computer attacks on automated data systems using artificial intelligence, as well as the possibility of its misuse, create significant criminological risks of unauthorized access and the use of subjects of the citizens' digital rights through these technologies [34].

The above reasoning gives grounds to regard criminal legal support for safeguarding the citizens' digital rights as a priority direction in the development of the theory and practice of applying criminal legal institutions in the global, national, and regional dimensions.

We express the hope that the initial theses formulated under this study will be used in the future when building state policy and developing legal regulation of relations in the context of industrialization and digitization.

References

1. Decree of the President of the Russian Federation dated May 9, 2017, No. 203 On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030, Collection of Legislation of the Russian Federation, 20, 2901 (2017)
2. I.R. Begishev, Current Problems of Economics and Law, **1**, 123 (2010)
3. E.Yu. Latypova, Economics and Law, **2**, 37 (2019)
4. A.Y. Bokovnya, Z.I. Khisamova, I.R. Begishev, Helix, **9(5)**, 5458 (2019)
5. I.R. Begishev, Z.I. Khisamova, S.G. Nikitin, Russian J. of Criminology, **14(1)**, 96 (2020)
6. A.I. Korobeev, R.I. Dremlyuga, Ya.O. Kuchina, Russian J. of Criminology, **13(3)**, 416 (2019)
7. M.A. Efremova, Perm University Herald. Yuridical Sciences, **1(27)**, 124 (2015)
8. E.V. Rogova, S.A. Karnovich, O.V. Ivushkina, E.A. Laikova, M.A. Efremova, Journal of Advanced Research in Law and Economics, **7(1)**, 93 (2016)
9. I.R. Begishev, Z.I. Khisamova, A.Y. Bokovnya, Helix, **9(5)**, 5639 (2019)
10. M.S. Malik, U. Islam, J. of Financial Crime, **26(1)**, 50 (2019)
11. A.Yu. Bokovnya, Z.I. Khisamova, V.F. Vasyukov, I.R. Begishev, Cuestiones Políticas, **38(66)**, 156 (2020)

12. M.A. Efremova, Perm University Herald. Juridical Sciences, **36**, 222 (2017)
13. I.R. Efremova, Z.I. Khisamova, G.I. Mazitova, Revista Gênero & Direito, **8(6)**, 283 (2019)
14. M.A. Efremova, E.V. Rogova, Journal of Advanced Research in Law and Economics, **10, 1(39),** 144 (2019)
15. Z.I. Khisamova, I.R. Begishev, E.Yu. Latypova, Russian Journal of Criminology, **14(6)**, 96 (2020)
16. A.Yu. Bokovnya, Z.I. Khisamova, I.R. Begishev, E.Yu. Latypova, E.V. Nechaeva, Cuestiones Políticas, **38(66)**, 463 (2020)
17. A.Yu. Bokovnya, Z.I. Khisamova, I.R. Begishev, E.L. Sidorenko, A.N. Ilyashenko, A.Yu. Morozov, Applied Linguistics Research Journal, **4(7)**, 91 (2020)
18. A.Yu. Bokovnya, I.R. Begishev, Z.I. Khisamova, I.I. Bikeev, E.L. Sidorenko, D.D. Bersei, International Journal of Criminology and Sociology, **9**, 1054 (2020)
19. Z.I. Khisamova, I.R. Begishev, E.L. Sidorenko, Int. J. of Cyber Criminology, **13(2)**, 564 (2019)
20. A.Yu. Bokovnya, I.R. Begishev, Z.I. Khisamova, N.R. Narimanova, L.M. Sherbakova, A.A. Minina, Revista San Gregorio, **41**, 115 (2020)
21. A.P. Sukhodolov, A.V. Bychkov, A.M. Bychkova, J. of Siberian Federal University. Humanities & Social Sciences, **13(1)**, 116 (2020)
22. I.R. Begishev, Z.I. Khisamova, Russian J. of Criminology, **12(6)**, 767 (2018)
23. A.P. Sukhodolov, A.M. Bychkova, Russian J. of Criminology, **12(6)**, 753 (2018)
24. I.R. Begishev, E.Yu. Latypova, D.V. Kirpichnikov, Actual Problems of Economics and Law, **14(1)**, 79 (2020)
25. V.A. Shestak, A.G. Volevodz, Russian J. of Criminology, **13(2)**, 197 (2019)
26. Z.I. Khisamova, I.R. Begishev, Russian J. of Criminology, **13(4)**, 564 (2019)
27. D.A. Stepanenko, D.V. Bakhteev, Yu.A. Evstratova, Russian J. of Criminology, **14(2)**,206 (2020)
28. Z.I. Khisamova, I.R. Begishev, R.R. Gaifutdinov, International J. of Innovative Technology and Exploring Engineering, **9(1)**, 5159 (2019)
29. G. Hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer International Publishing, 257 (2015)
30. L.A. Bukalerova, I*nformation Crimes in the Sphere of State and Municipal Administration: Legislative and Law-Enforcement Problems*, 50 (2007)
31. E.Yu. Latypova, E.M. Gilmanov, E.V. Nechaeva, Human: Crime and Punishment, **27(1-4), 1**, 81 (2019)
32. V.B. Vekhov, Criminal Law, **4**, 17 (2004)
33. Decree of the President of the Russian Federation dated December 5, 2016, No. 646 On Approval of the Doctrine of Information Security of the Russian Federation, Collection of Legislation of the Russian Federation, 50, 7074 (2017)
34. D. Kirpichnikov, A. Pavlyuk, Y. Grebneva, H. Okagbue, *E3S Web of Conferences* 159, 04025 (2020).