Pressing Issues of Unlawful Application of Artificial Intelligence

Alexandra Yuryevna Bokovnya[1,*], Ildar Rustamovich Begishev[2], Zarina Ilduzovna Khisamova[3], Igor Izmailovich Bikeev[4], Elina Leonidovna Sidorenko[5] and Diana Davletovna Bersei[6]

[1]*Faculty of Law, Department of Criminal Law, Kazan Federal University, Kazan, Russia*

[2]*Kazan Innovative University named after V.G. Timiryasov, Kazan, Russia*

[3]*Department of Planning and Coordination of Research Activities, Head, Research Department, Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Krasnodar, Russia*

[4]*Department of Criminal Law and Procedure, Kazan Innovative University named after V.G. Timiryasov, Kazan, Russia*

[5]*Department of Criminal Law, Criminal Procedure, and Criminalistics, Moscow State Institute of International Relations (University), Moscow, Russia*

[6]*Department of Legal and Special Disciplines. Stavropol branch of RANEPA, Stavropol, Russia*

Abstract: The article discusses the problematic aspects of the implementation and application of artificial intelligence technology at the present stage of its development. The authors provide definitions of this technology, with its essential properties revealed based on their analysis. Criminological forecasting helps identify groups of crimes most likely to be committed through the use of artificial intelligence. The authors believe that at present there are not sufficient grounds for distancing ourselves from the issue of the subject of criminal liability in case of damage to public relations directly by the AI, but there are no circumstances due to which its resolution would not be delayed. The system of criminal law relations must be built based on scientifically developed provisions. The problems of criminal legal regulation, in terms of the impossibility of criminalizing and penalizing socially dangerous acts committed by artificial intelligence, are revealed. The legislator is asked to develop and adopt legal acts regulating the creation, operation, and use of artificial intelligence.

Keywords: Artificial intelligence, intelligent systems, criminological risk, criminology, responsibility, legal regulation, subject of crime, criminal liability, criminal law, technological singularity.

INTRODUCTION

Digital technologies are widely used in all areas of public life, being introduced, and becoming an indispensable attribute of most social practices (Khisamova 2017). Considering the current state of technological development, it seems possible to state that digital information has significantly grown in its importance as a valuable resource, which determines the increase in the number of criminal attacks committed against it (Latypova, Nechaeva, Gilmanov, & Aleksandrova, 2019). Besides, criminal attacks on critical information infrastructure (Begishev, Khisamova, & Mazitova, 2019). are constantly being carried out, computer attacks (Begishev, Khisamova, Bokovnya 2019) and other digital crimes (Bokovnya, Khisamova, Begishev 2019) are being committed. Digitalization of various processes makes it possible to remotely commit socially dangerous acts, to create manipulation tools, and to evade responsibility (Begishev, Bikeev, 2020). The aforementioned circumstances actualize the need for analysis and development of state policy and criminal law regulation of public relations to ensure their reliable protection from the risks associated with digitalization. Especially in terms of implementing the most advanced technology - artificial intelligence (hereinafter - AI). It should be noted that in this article, the understanding of artificial intelligence was carried out as it is provided under the Decree of the President of the Russian Federation, which establishes priority areas of activity in this area. Thus, the term “artificial intelligence” means “a set of technological solutions that mimic human cognitive functions (including self-learning and search) decisions without a predetermined algorithm) and to obtain results when performing specific tasks that are comparable, at least, with the results of human intellectual activity” (Decree of the President of the Russian Federation No. 490 of October 10, 2019).

MATERIAL AND METHODS

The materials for the work were the provisions of the Russian criminal law, as well as legal acts in the creation and use of AI.

*Address correspondence to this author at the Faculty of Law, Department of Criminal Law, Kazan Federal University, Kazan, Russia; Tel: ????????????; Fax: ????????????????; E-mail: kafedra.ksu@yandex.ru

E-ISSN: 1929-4409/20

The methodological basis of the study is a combination of methods of scientific knowledge, including abstract logic, comparison, and correlation analysis.

RESULTS AND DISCUSSION

We are right with the arguments of the researchers, who insist that the uncontrolled development of AI technology poses certain threats to the safe development of society and the state, determined by the lack of adapted, following the specifics of AI technologies, criminal law mechanisms for the protection of public relations, the presence of legal uncertainty in the subject of criminal liability in case of causing harm directly by AI (Begishev, Khisamova, 2018).

In this context, it is necessary to clarify that the complex of AI technologies has an incomparably greater potential for speed, quality, and limits of storage, processing, and transmission of digital data than a person (Sukhodolov, Bychkov, & Bychkova, 2020). even if its activity is mediated by the computing power of computer technology (Bikeev, Kabanov, Begishev, & Khisamova, 2019, December). Having considered that the main functioning area of AI is information and telecommunication devices, their systems and networks it is possible to reasonably assume that the information circulating in them can be intercepted by AI with sufficient efficiency and used depending on the discretion of the creator or user of the technology. Articles 272-274.1 of the Criminal Code of the Russian Federation, which provide criminal liability for crimes in the field of computer information, do not cover these threats.

To ensure the validity of the reasoning, we should provide explanations of the concept of AI (Shestak, Volevodz, Alizade 2019) and design a further presentation on its basis. Of course, the fundamental document in this area is the above-mentioned Decree of the President of the Russian Federation and the Concept of the Russian Federation for the development of regulation of relations in the field of artificial intelligence and robotics technologies until 2024 (Decree of the Government of the Russian Federation No. 2129-R of August 19, 2020). The documents contain a significant observation that the complex of technological solutions includes information and telecommunication infrastructure, software (including that using machine learning methods), processes, and services for data processing.

The scientific literature provides a similar definition of AI (Sukhodolov, Bychkova, 2018. Begishev, Latypova, & Kirpichnikov, 2020, Shestak, & Volevodz, 2019. Stepanenko, Bakhteev, Evstratova 2020).

Analysis of the definitions allows us to identify the following essential AI properties:

1. simulation of human cognitive functions;
2. self-education;
3. search for solutions without a given algorithm;
4. comparability of the results of the intellectual activity of AI and humans.

Being in sync with the form of the previous definitions, we want to expand the ones. It is hardly possible to limit the material expression of AI only to its units, that is, objects of the material world that have an objective expression in it and are intended to realize its intellectual potential. As correctly noted in the provisions of the above-mentioned Decree of the President of the Russian Federation, AI can also be expressed in the information infrastructure, that is, by its physical nature, is a medium for transmitting digital information.

Based on a generalization of the above definitions, we can ascertain the consensus reached regarding the ability of AI to self-education, act without the algorithm-predetermined autonomy in decision-making (Khisamova, Begishev, & Sidorenko, 2019).

The stated properties significantly increase the criminological potential for committing certain types of crimes, the common property of which is digital information acting as a sign characterizing the subject of a crime. The greatest danger arises concerning attacks on the critical information infrastructure of the Russian Federation, that is, critically important and potentially dangerous facilities, the means of which is digital information.

We should also explain that at present, the activity of these digital objects is provided by automated control systems in which, firstly, digital information circulates, and secondly, systems and complexes of its protection are implemented that use various technical and cryptographic means of security.

However, the use of AI (for example, to create a malicious computer program for unauthorized

destruction, blocking, modification, copying of digital information or neutralizing of its means of protection) will significantly increase their ability to violate security systems, destabilize the functioning of security information systems, which naturally can lead to significant negative changes in the activities of critical information infrastructure facilities and cause a crisis to occur on various scales.

Along with the above, AI as a cross-cutting digital technology can be used with equal effectiveness to attack digital information (Khisamova, Begishev, 2019). The above demonstrates the significant criminological risks of the unlawful use of AI by hacker communities (Begishev, Khisamova, Nikitin, 2020).

Based on the above reasoning, we can state that one of the main urgent tasks of criminal law is to develop legal models for the prevention and penalization of acts of AI (or acts committed with its use) that harm public relations protected by criminal law. This activity has certain difficulties. For example, as previously demonstrated that AI technology can learn and act without a predefined algorithm. This creates legal uncertainty regarding the criminal prosecution of AI for acts committed by it.

In the scientific literature, a discourse has formed regarding the considered issue. The foreign scientific community is developing positions on the need to review the status of the subject of crime and establish, as such, AI, as well as authors, justifying the given position, intelligence and sanity are not caused solely by biological processes (Simmler, Markwalder, 2019).

Finding this opinion partially justified, we note that giving AI the status of a crime subject is premature in our opinion since these technologies are at an insufficient level of development that does not allow us to state fully the technological singularity and absolute autonomy of activity. In accordance with the provisions of article 19, article 20, article 21 of the Criminal code of the Russian Federation, the subject of a crime can be a sane individual who has reached the age of 16 at the time of committing criminal acts, so artificial intelligence can not be recognized as a subject.

However, the relevance of developing measures to resolve this question will only increase in the future, including when determining the methods of legal regulation of AI, both in Russia (Khisamova, Begishev 2019). and in the world (Khisamova, Begishev, & Gaifutdinov, 2019).

We note as well that some of the scientists argue that it is necessary to apply measures of coercion to AI even if it does not have the whole set of signs that classify it as a subject of a crime, citing its argument that any act prohibited by criminal law should be prevented, and the source of public danger must be addressed promptly (Hallevy, 2015). However, it is hardly possible to apply the measures applied to AI as punishment. Scientists are true asserting that it is impossible to correct the personal orientation of AI and form a respectful attitude towards law and society with the legal force, and the only measure to protect public relations from AI is to eliminate it (Uzhov, 2017). At the same time, the existing definition of criminal punishment is provided in Art. 43 of the Criminal Code avoids the inclusion of liquidation in the list of types of punishment since it is irrelevant for correction of a convicted person. Also, questions about the ability of AI to understand the nature and significance of enforcement measures applied to it were not clarified in legal science and legislation.

SUMMARY

We believe that at present there are not sufficient grounds for distancing ourselves from the issue of the subject of criminal liability in case of damage to public relations directly by the AI, but there are no circumstances due to which its resolution would not be delayed. We are convinced that the system of criminal law relations must be built based on scientifically developed provisions.

We share several scientific recommendations regarding the application of criminal law if AI causes harm to public relations:

1. evaluate the degree of independence of the act committed by AI;
2. consider the initial algorithms of actions the AI during its programming, design, and refinement was based on;
3. consider the amount of knowledge AI could get in the process of self-education;
4. establish the nature and degree of participation of the user (owner, proprietor) of AI in the commission of the crime.

CONCLUSION

To order the activities on the creation, operation, and use of AI, it seems necessary to publish a series of legal acts that regulate:

1. AI programming conditions and procedure;

2. the establishment of technical requirements for the AI creation (production);

3. the AI application procedure, considering the most typical and dangerous, in terms of criminology, situations of its use.

ACKNOWLEDGEMENTS

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

REFERENCES

Begishev I.R., Bikeev I.I.(2020). Crimes in the sphere of Digital Information Circulation. Kazan: Publishing House "Cognition" of Kazan Innovation University. 300 p.

Begishev I.R., Khisamova Z.I. (2018).Criminological Risks of Using Artificial Intelligence // Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology. Vol. 12, No 6. Pp. 767-775. https://doi.org/10.17150/2500-4255.2018.12(6).767-775

Begishev I.R., Khisamova Z.I., Bokovnya A.Y. (2019). Information Infrastructure of Safe Computer Attack // Helix. Vol. 9, No 5. Pp. 5639-5642. https://doi.org/10.29042/2019-5639-5642

Begishev I.R., Khisamova Z.I., Nikitin S.G. (2020). The Organization of Hacking Community: Criminological and Criminal Law Aspects // Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology. Vol. 14, No 1. Pp. 96-105.

Begishev, I. R., Khisamova, Z. I., & Mazitova, G. I. (2019). Criminal legal ensuring of security of critical information infrastructure of the Russian Federation. *Revista Gênero & Direito*, *8*(6), 283-292. https://doi.org/10.22478/ufpb.2179-7137.2019v8n6.49193

Begishev, I. R., Latypova, E. Y., & Kirpichnikov, D. V. (2020). Artificial Intelligence as a Legal Category: Doctrinal Approach to Formulating a Definition. Actual Probs. Econ. & L., 79. https://doi.org/10.21202/1993-047X.14.2020.1.79-91

Bikeev, I., Kabanov, P., Begishev, I., & Khisamova, Z. (2019, December). Criminological risks and legal aspects of artificial intelligence implementation. In Proceedings of the International Conference on Artificial Intelligence, Information Processing and Cloud Computing (pp. 1-7). https://doi.org/10.1145/3371425.3371476

Bokovnya A.Y., Khisamova Z.I., Begishev I.R. (2019). Study of Russia and the UK Legislations in Combating Digital Crimes // Helix. Vol. 9, No 5. Pp. 5458-5461. https://doi.org/10.29042/2019-5458-5461

Decree of the Government of the Russian Federation No. 2129-R of August 19, 2020 “On approval of the Concept of development of regulation of relations in the field of artificial intelligence and robotics technologies for the period up to 2024”. URL: https://www.garant.ru/products/ipo/prime/doc/74460628/#0

Decree of the President of the Russian Federation No. 490 of October 10, 2019 “On the Development of Artificial Intelligence in the Russian Federation” // Collection of laws of the Russian Federation. 2019. No 41. Article 5700. https://doi.org/10.4324/9780429057922-4

Hallevy, G. (2015). Liability for crimes involving artificial intelligence systems. Springer International Publishing. https://doi.org/10.1007/978-3-319-10124-8

Khisamova Z.I. (2017).Criminal Liability for Crimes Committed in the Financial sphere using Information and Telecommunications Technologies. Moscow: Yurlitinform, 160 p.

Khisamova Z.I., Begishev I.R. (2019). Criminal Liability and Artificial Intelligence: Theoretical and Applied Aspects // Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology. Vol. 13, No 4. Pp. 564-574. https://doi.org/10.17150/2500-4255.2019.13(4).564-574

Khisamova Z.I., Begishev I.R. (2019). Legal Regulation of Artificial Intelligence // Baikal Research Journal. Vol. 10, № 2.

Khisamova, Z. I., Begishev, I. R., & Sidorenko, E. L. (2019). Artificial Intelligence and Problems of Ensuring Cyber Security. International Journal of Cyber Criminology, 13(2), 564-577. https://doi.org/10.17150/2500-4255.2019.13(4).564-574

Khisamova, Z., Begishev, I., & Gaifutdinov, R. (2019). On methods to legal regulation of artificial intelligence in the world. SCOPUS-2019-9-1-SID85075304864.

Latypova, E. Y., Nechaeva, E. V., Gilmanov, E. M., & Aleksandrova, N. V. (2019). Infringements on Digital Information: Modern State of the Problem. In *SHS Web of Conferences* (Vol. 62, p. 10004). EDP Sciences. https://doi.org/10.1051/shsconf/20196210004

Shestak V.A., Volevodz A.G., Alizade V.A. (2019). On the Possibility of Doctrinal Perception of Artificial Intelligence as the Subject of Crime in the System of Common Law: using the Example of the U.S. Criminal Legislation // Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology. Vol. 13, No 4. Pp. 547-554. https://doi.org/10.17150/2500-4255.2019.13(4).547-554

Shestak, V. A., & Volevodz, A. G. (2019). Modern requirements of the legal support of artificial intelligence: a view from Russia. Russian Journal of Criminology, 13(2), 197-206. https://doi.org/10.17150/2500-4255.2019.13(2).197-206

Simmler M., Markwalder N. (2019).Guilty Robots? – Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence // Criminal Law Forum. Vol. 30, No 1. Pp. 1-31. https://doi.org/10.1007/s10609-018-9360-0

Stepanenko D.A., Bakhteev D.V., Evstratova Yu.A.(2020). The use of Artificial Intelligence Systems in Law Enforcement // Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology. Vol. 14, No 2. Pp. 206-214.

Sukhodolov A.P., Bychkova A.M. (2018).Artificial Intelligence in Crime Counteraction, Prediction, Prevention and Evolution // Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology. Vol. 12, No 6. Pp. 753-766. https://doi.org/10.17150/2500-4255.2018.12(6).753-766

Sukhodolov, A. P., Bychkov, A. V., & Bychkova, A. M. (2020). Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects. https://doi.org/10.17516/1997-1370-0542

Uzhov, F. V. (2017). Artificial intelligence as a subject of law. Probely v rossiiskom zakonodatel'stve, (3), 357-360.