Правоприменение
2025. Т. 9, № 4. С. 36–46

ISSN 2542-1514 (Print)

THE LAW ENFORCEMENT BY THE PUBLIC AUTHORITIES

DOI 10.52468/2542-1514.2025.9(4).36-46

LEGAL ASPECTS OF ARTIFICIAL INTELLIGENCE IN ENSURING NATIONAL SECURITY: CHALLENGES AND THREATS**

Anna K. Zharova
Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia

Article info
Received –
2025 March 9
Accepted –
2025 September 20
Available online
– 2025
December 20

Keywords
Trusted technologies, artificial intelligence, principles, national security, information security, non-discrimination, objectivity, ethical standards, conformity assessment system

The subject. Artificial intelligence (AI) opens up wide opportunities for strengthening national security, but also raises a number of legal and ethical issues that need to be carefully analyzed and resolved. The implementation of a government strategy aimed at improving tools and approaches to information protection using AI is a key aspect of ensuring national security and maintaining law and order.

The aim of the article was to confirm the hypothesis that ensuring national security depends on algorithms implemented in artificial intelligence (AI) technologies.

Methodology. The criteria formulated in the President Decree of the Russian Federation No. 124 are fundamental on the basis of which trusted AI systems are developed. The analysis of legal acts, acts of technical regulation and scientific literature was made.

Main results. In areas where there is a threat to national security, the use of trusted AI technologies is becoming mandatory. In accordance with Presidential Decree No. 124, trusted AI technologies are defined as meeting safety standards and developed based on the principles of objectivity, non-discrimination and ethics. Their use should exclude the possibility of harming a person, violating his rights and freedoms, as well as harming the interests of society and the state. Only two principles formulated in that Decree are disclosed – this is the principle of non-discrimination and objectivity. Despite the use of the term "ethics of norms", "ethics" in the legislation in the field of AI, ethics is not defined as an independent principle. Ethics in the field of AI can be understood as a system of views and principles aimed at protecting the moral and social consequences associated with the use of various data processing models contained in AI technologies. The principle of objectivity or impartiality is related to the ability of the system to inspire confidence and exclude unjustified bias of the formed estimates. The principle of objectivity is closely intertwined with the principles of transparency of AI systems and data protection and security. To achieve the objectivity of data processing by AI systems, it is necessary to use high-quality and representative datasets obtained from reliable sources. The implementation of the principle of non-discrimination contains certain contradictions that manifest themselves in the conditions of ensuring national security. Since, despite the fact that it is intended to exclude the possibility of using AI algorithms for processing and analyzing data containing discriminatory criteria, if necessary, the state can apply other criteria to ensure the national security.

Conclusions. The implementation of the above principles, the creation of a trusted environment for the use of AI technologies, and the development of trusted AI technologies all ensure information security, the effectiveness of the system for protecting the interests of citizens, society, information, and information infrastructure, thereby ensuring national security.

** The publication was prepared within the framework of the scientific project "Creating a Russian historiographical model of political and legal knowledge and its application to develop prospecting means of countering ideological distortions of Russia's civilizational development", implemented by the Federal State Budgetary Institution of Science “Institute of State and Law of the Russian Academy of Sciences”, with financial support from the Ministry of Science and Higher Education of the Russian Federation (Agreement dated July 12, 2024 No. 075-15-2024-639).

ISSN 2658-4050 (Online)

1. Introduction

Artificial intelligence (AI) is actively being implemented in all areas of our lives, opening up great prospects for strengthening national security (NB). However, its use raises new legal and ethical issues that need to be understood and addressed. The idea expressed more than ten years ago by I.L. Bachilo[**Error! Reference source not found.**] that not only citizens and the state need protection from information but also information itself requires protection is also relevant in relation to the use of AI technology. It is not only necessary to ensure the information security (IS) of AI users but also to protect AI itself from illegal use[**Error! Reference source not found.**], as it has huge potential. For example, standards have been developed to ensure data security when processing with AI technologies[**Error! Reference source not found.**, **Error! Reference source not found.**].. Additionally, policies and requirements have been formulated for AI to ensure responsible use[**Error! Reference source not found.**, **Error! Reference source not found.**]..

The key goal of improving legislation on the development and application of AI technologies for the period up to 2030 is to create favorable legal conditions in Russia for the development, implementation, and use of these technologies. Therefore, from July 1st, 2020, an experiment was conducted in Moscow to establish an experimental legal regime to create the necessary conditions for the development and implementation of AI technology for five years. At the same time, the development of AI must be carried out in accordance with legal principles that protect human rights and freedoms, as well as ensuring the security of the Russian Federation. However, there is a question: how does the development phase relate to ensuring national security?

2. National Security and AI

In 2019, at his big press conference, Vladimir Putin said that the development of AI is a matter of national[1]security. AI is "a set of technological solutions that mimics human cognitive functions (including self-learning and search for solutions without a pre-defined algorithm) and allows you to achieve results that are at least comparable to the results of human intellectual activity when performing tasks[2]." Since AI is a complex of technological solutions, the link between AI and NB lies in the stages of AI development and application, that is, throughout the entire life cycle of AI technological solutions." Issues of ensuring the security of individuals, society, and the state from internal and external information threats are handled by information security[3]. Accordingly, AI technologies are associated with ensuring NB through providing information security, which is a key aspect of ensuring NB. This thesis is supported by numerous scientific studies, such as [9, 10, 11], and practices (which suggest combining these concepts and form the concept of "national information security"). Thus, practitioners emphasize the importance of ensuring information security to achieve national security[4]). Thus, practitioners emphasize the importance of ensuring information security in order to achieve national security.

In 2021, according to the National Security Strategy of the Russian Federation, information security has been classified as a national priority. Moreover, this strategy indicates that the implementation of state policy aimed at improving the means and methods of ensuring information security through the use of artificial intelligence technologies is one of the goals that will help achieve information security. The Decree of the President of the Russian Federation № 124 of February 15, 2004, entitled "On Amendments to Decree № 490 of October 10, 1999" (referred to as the "Decree on Development of Artificial Intelligence in Russia")5, defines not only the need for legislation regulating human interaction with AI technologies to promote their development and use

1 Vladimir Putin: "Artificial intelligence is a matter of national security" // https://www.garant.ru/news/1310389/

2 Roadmap for the development of the "end-to-end" digital technology "Neurotechnology and artificial intelligence" (The document was not published)

3 Decree of the President of the Russian Federation No. 646 dated December 5, 2016 "On Approval of the Information Security Doctrine of the Russian Federation"

4 Information security in the national security system // https://falcongaze.com/ru/pressroom/publications/informacionnaya-bezopasnost-v-otraslyah/informacionnaya-bezopasnost-v-sisteme-nacionalnoj-bezopasnosti.html

5 Decree of the President of the Russian Federation No. 124 dated February 15, 2024 "On Amendments to Decree of the President of the Russian Federation No. 490 dated October 10, 2019 "On the Development of Artificial Intelligence in the Russian Federation" and to the National Strategy approved by this Decree"

ISSN 2542-1514 (Print)

but also the creation of a list of areas where AI may damage state security.

Thus, based on the analysis of the provisions of legislation, it is obvious that implementing state policy aimed at improving means and methods for ensuring information security through AI technologies is a key goal for ensuring national security and law and order. Furthermore, the state has identified areas where the use of AI technology may be dangerous, such as for the National Bank, and regulations have been developed for compensation for damage caused by AI in experimental legal regimes approved by Order No. 752, dated November 26, 2014[6].

Based on the analysis of the provisions of Order No. 752 of the Ministry of Economic Development of the Russian Federation, we can conclude that the most vulnerable areas of public life to AI are personal life, health, and property of individuals, as well as property of legal entities. If any harm is caused to the life, health or property of an individual or to property of a legal entity while implementing the experimental legal regime due to using solutions developed with AI technologies, these situations will be discussed at a meeting of a commission to determine the circumstances under which the use of such technologies caused harm during the implementation of experimental regulations in the field of digital innovation[7].

Thus, the analysis of legal acts leads us to the conclusion that the level of vulnerability of various spheres of public life and, as a result, national security and the rule of law directly depend on who owns AI technologies and what data processing methods are used in these technologies. Presidential Decree No. 124 states that disseminating relevant ethical standards is necessary to achieve the goal of creating favourable regulatory and legal conditions for developing, implementing, and using AI technologies in the Russian Federation, while taking into account the protection of human rights, freedoms and security.

Although the use of the term "ethical standards" in the application of AI technologies is controversial, Vasilevskaya L. Yu. believes that some authors' point of view on the possibility of ethical rules for human interaction with AI is legally incorrect. On the one hand, we agree with Vasilevs'ka's point, as AI is a set of technologies. However, on the other hand, if we consider ethics as a philosophical science that studies morality, then ethical norms can be seen as a link between morality and technology development. The article notes that this relationship is not straightforward, and ethics is often interpreted in terms of how science and technology create new values and transform old ones.

So, taking into account the use of the term "ethical norms" in Presidential Decree No. 124, we will consider ethics as a process of forming public values among developers and users of AI technologies throughout the entire life cycle of AI systems and technologies. The life cycle of an AI system, in accordance with GOST R 71476-2024, can be presented as follows:[8]

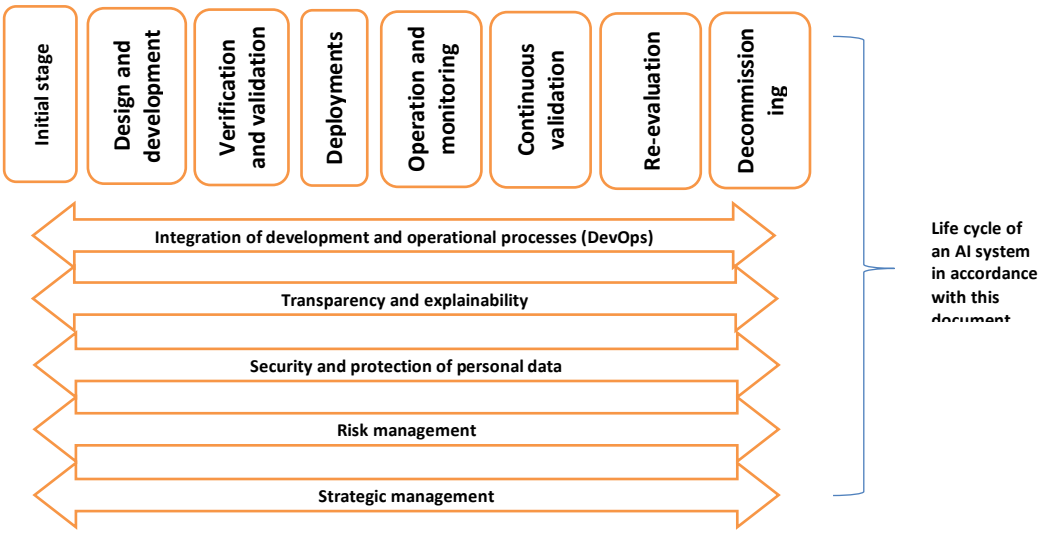
6 Order of the Ministry of Economic Development of Russia dated November 26, 2024 No. 752 "On Approval of the Procedure for Forming a commission to Establish the Circumstances in which, during the Implementation of an Experimental Legal Regime in the field of digital innovations, as a result of the Use of Solutions Developed using AI Technologies, Harm was caused to Human Life, Health or Property, or to the Property of a Legal Entity, the Procedure for Consideration by the commission of cases of harm to human life, health or Property, or property of a legal entity in the implementation of an experimental legal regime in the field of digital innovation as a result of the use of solutions, developed using AI technologies, the procedure for preparing the commission's conclusion based on the results of establishing circumstances in which, as a result of the implementation of an experimental legal regime in the field of digital innovations, when using solutions developed using AI technologies, harm was caused to the life, health or property of a person or a legal entity, the form of such conclusion". Official Internet-legal information portal http://pravo.gov.ru , 12/27/2024.

7 Order of the Ministry of Economic Development of Russia No. 752.

8 GOST R 71476-2024 (ISO/IEC 22989:2022). The national standard of the Russian Federation. Artificial intelligence. Concepts and terminology of AI (approved and put into effect by Rosstandart Order No. 1550-st dated 10/28/2024). Moscow: Federal State Budgetary Institution "Institute of Standardization", 2024.

ISSN 2658-4050 (Online)

allows the development of trustworthy AI technologies. Trust in AI technologies is primarily aimed at creating a trusting attitude towards these technologies among users, and it is inextricably linked to trust in the data processing models used in these technologies.



Presidential Decree No. 124, in addition to the "dissemination of relevant ethical standards", notes the following main directions for creating a comprehensive system of regulatory regulation of public relations in the development and use of AI technologies and ensuring the safety of their use: "formation of a mechanism for assessing the risks of violation of ethical standards when implementing AI technologies in economic and social spheres; development of requirements for information security of AI technologies; creation of a system to assess compliance of AI technology with the requirements of Russian legislation, including in the field of information security (paragraphs "g" - "l" of paragraph 51(11)).[9].

Moreover, for those areas of application of AI technologies where the NB can be violated, the development of AI technology must be carried out in accordance with the requirements for information security for trusted AI technologies (Clause "a" of subclause 51 (10) of Decree No. 124 of the President of the Russian Federation)[10].

The creation of a system for assessing the compliance of AI technologies with information security requirements is linked to the system of standardization and certification of AI technologies, which ultimately

Users' understanding of the data processing process is important because a technology that mimics human cognitive functions can create an illusion of understanding its decisions. [**Error! Reference source not found.**,**Error! Reference source not found.**].

However, this is not the case. AI technologies at this stage of development cannot explain the logic behind their decisions, so that people can understand the logic of obtaining a solution. This illusion can lead people to misinterpret AI technology and use it for wrong purposes. Not only is ignorance of AI functionality dangerous, but understanding its potential and capabilities can also lead to negative consequences if attackers gain access to these systems. [**Error! Reference source not found.**].

3. Trusted AI technologies

From 2021 to the present, significant changes have taken place in the field of artificial intelligence, related to the creation of a list of standards. By the end of February 2025, 61 AI standards had been published on the Rosstandart website, of which 32 were adopted in 2022. Based on the key objectives defined by Presidential Decree No. 124, including the mandatory use of trustworthy AI technologies in areas with a threat of NB, we will examine the criteria and methods for evaluating the compliance of AI technologies with Russian legislation.

9 Decree of the President of the Russian Federation No. 124
10 Decree of the President of the Russian Federation No. 124

ISSN 2542-1514 (Print)

Trusted AI technologies are defined as those that meet security standards based on principles of objectivity, nondiscrimination, ethics, and exclude the possibility of harm to individuals or violation of their fundamental rights or freedoms, or harm to societal or state interests (subsection "c")[11].

For the development of trusted AI systems, a special platform has been created that allows automating the processes of identifying and eliminating threats that may arise at all stages of the life cycle of machine learning model creation. 12.

In this case, a natural question arises: Do the standards in the field of AI reflect the principles of objectivity, non-discrimination, and ethics, as well as other important principles? For example, the Russian Federation is developing a Code of Ethics for Artificial Intelligence in 2022 (hereinafter referred to as the "AI Code")[13]. However, the AI code itself does not define ethics as a principle.

Apparently, by including "ethics" in its name, the developers wanted to emphasize that ethics should be fundamental at all stages of AI technology and system development. However, we have already pointed out that the use of this term in relation to AI is controversial.

Despite the fact that Presidential Decree No. 124 links the development of trustworthy technologies to the principle of ethics, we do not agree with this statement. In order to achieve this goal, it is necessary to clearly define what is meant by the principle of ethical behavior in AI. Ethics in the field of artificial intelligence can be considered a system of views and principles aimed at protecting moral and social consequences arising from the use of AI technologies, including liability for damages caused by AI, exclusion of bias in data processing algorithms and transparency, and addressing the fine line between privacy and information security. We believe that the concept of socially responsible AI best represents these relationships.

The authors of the AI Code revealed the principles of socially responsible behavior in the field of AI applications, regarding only one area: the use of AI technologies. Ethics in this field affects, among other things, the relationships in the development of AI technology. According to the AI Code14, the principle of social responsibility in AI applications requires participants to be responsible for the impact of their systems on society and individuals. This includes protecting privacy, using ethical and secure data, and responsibly selecting and using hardware and software at different stages of AI system development (Section 1, Paragraph 2.2, Part 2).

Thus, we believe that the requirement for socially responsible behavior in the field of AI applications is aimed at creating a trusted user environment for AI systems. It is assumed that market participants involved in AI should be aware of all possible risks when choosing a particular technology and should do everything in their power to prevent these risks from being implemented[20, **Error! Reference source not found.**]..

Returning to the other two principles - objectivity and non-discrimination, we also want to note that, in the AI code, the principle of objectivity does not have an independent definition, like the principle of ethics. In scientific literature, this principle is associated with stages of the AI lifecycle, such as its development and use, and the importance of protecting data processed by AI technologies[**Error! Reference source not found.**,**Error! Reference source not found.**]. The ethical consequences of letting AI make decisions and values and principles needed to ensure AI development are also mentioned[24], but there is no clear definition of this principle in the literature [25, 26].

Foreign researchers emphasize the need to systematize existing research and categorize concepts [27].

In GOST R 59276-2020, objectivity is defined as impartiality, and it is linked to the ability to trust in system functioning, avoiding unfair biases in estimates[15].

Closely related to the principle of objectivity is the principle of transparency in AI technology. This is defined, for example, in GOST R ISO 26000 and the Preliminary National Standard 963-2024 (ISO/IEC

11 Decree of the President of the Russian Federation No. 124
12 Trusted Artificial Intelligence (AI) Platform // https://www.ispras.ru/technologies/tai/
13 Code of Ethics in the field of artificial intelligence (The document was not published)
14 Code of Ethics in the field of artificial intelligence
15 GOST R 59276-2020. The national standard of the Russian Federation. Artificial intelligence systems. Ways to ensure trust. General provisions (approved and put into effect by Rosstandart Order No. 1371-st dated 12/23/2020). Moscow: Standartinform, 2021.

5339:2024).[16]. " Transparency allows stakeholders to get information about what the AI system was designed for, how it was developed, and how it was put into operation[17]. This includes information about goals, constraints, definitions, assumptions, algorithms, data sources and collection, security, privacy, and privacy protection, as well as the level of automation. Traceability is attributed to transparency as a potential source of ethical concerns."

As we can see, the principle of transparency covers such an element of the life cycle of an AI system as its development. In other words, users of AI technology can get information about the principles of data processing by AI systems and methods of making decisions from the manufacturer. The principle has been expanded and supplemented by the concept of explain ability of AI systems aimed at ensuring clarity and transparency in decisions made by AI systems when stakeholders interact with them. This interaction of principles leads to a more complete understanding of the work of AI by users.

And finally, the third feature defined in Presidential Decree No. 124 related to the development of trustworthy AI technologies is the principle of non-discrimination. In the AI code, this principle is called the "principle of equality and non- discrimination". This principle aims to prevent AI algorithms from processing and analyzing data containing discriminatory criteria, and it requires market participants (actors) to ensure that their algorithms do not discriminate against individuals or groups in their processing information for machine learning purposes. However, explicit rules of operation for AI systems stated by actors may be considered discriminatory if they are applied differently to different groups based on specific characteristics[18].

However, it should be noted that the implementation of the principle of non-discrimination leads to certain contradictions in ensuring national security. On the one hand, the State is obliged to ensure the safety of all its citizens, regardless of race, ethnicity, religion, gender or sexual orientation. On the other hand, in order to counter threats to national security, it may be necessary to apply criteria for data processing that may be discriminatory and violate the principle of equality. However, when faced with a choice between national security and equality, the state always chooses national security.

4. Conclusions

So, summing up the research, we can draw the following conclusions: In areas where there is a threat to national security, the use of trustworthy AI technologies becomes mandatory. According to Presidential Decree No. 124, trustworthy AI is defined as meeting security standards and being developed based on principles of objectivity, non-discrimination, and ethics. Its application should exclude any possibility of harm to individuals, violation of their rights and freedoms, or damage to the interests of society or the state. Analysis of the provisions of legislation and technical regulations allows us to conclude that the two principles formulated in Presidential Decrees 1 and 2 are disclosed - these are the principles of a non-discriminatory and objective approach. Despite the use of the phrase "ethical norms", ethics is not defined as a separate principle in legislation on AI.

The analysis of scientific literature allowed us to conclude that ethics in the field of AI can be understood as a system of views and principles aimed at protecting the moral and social consequences associated with the use of various data processing models contained in AI technologies. The principle of objectivity or non-bias is related to a system's ability to inspire confidence and eliminate unjustified biases in estimates. This principle is closely intertwined with transparency and data protection principles in AI systems. To achieve objectivity in data processing by AI systems, high-quality, representative data sets from reliable sources must be used.

The implementation of the principle of non-discrimination contains certain contradictions that manifest themselves in the conditions of ensuring national security. Despite the fact that the principle is intended to exclude the possibility of using AI algorithms for processing and analyzing data containing discriminatory criteria, the state may apply other criteria if it is necessary to ensure national security. The implementation of these principles, the creation of a trusted environment for using AI

16 PNST 963-2024 (ISO/IEC 5339:2024). Preliminary national standard of the Russian Federation. Artificial intelligence. Guidelines for applications based on artificial intelligence (approved and put into effect by Rosstandart Order No. 70-pnst dated 10/25/2024). Moscow: Federal State Budgetary Institution "Institute of Standardization", 2024.
17 GOST R 71476-2024 (clause 5.15.8)
18 Code of Ethics in the field of artificial intelligence

ISSN 2542-1514 (Print)

technologies, and the development of trustworthy AI technologies ensure information security, the effectiveness of the system to protect the interests of citizens, society, information and information infrastructure, thus contributing to National Security.

REFERENCES

1. Bachilo I.L. *Legal provision of information security at a new stage in the development of the information society*. Available at: http://igpran.ru/public/articles/BachiloIL.2014.1..pdf. (In Russ.).

2. Strakhov A.A., Dubinina N.M. About data leakage and DLP systems. *Kriminologicheskii zhurnal = Criminolog- ical journal*, 2022, no. 4, pp. 226–232. DOI: 10.24412/2687-0185-2022-4-226-232. (In Russ.).

3. Gromov Yu.Yu., Drachev V.O., Vojtjuk V.V., Rodin V.V., Samkharadzce T.G. Analysis of existing methods of information protection in modern information systems. *Inzhenernaya fizika = Engineering physics*, 2008, no. 2, pp. 67–69. (In Russ.).

4. Zharova A.K., Elin V.M., Avetisyan B.R. Prevention of computer attacks such as man in the middle, committed using generative artificial intelligence. *Voprosy kiberbezopasnosti = Cybersecuriry issues*, 2024, no. 6 (64), pp. 28–41. DOI: 10.21681/2311-3456-2024-6-28-41. (In Russ.).

5. Denning P.J., Arquilla J. The context problem in artificial intelligence. *Communications of the ACM*, 2022, vol. 65, iss. 12, pp. 18–21. DOI: 10.1145/3567605.

6. Cheruvalath R. Artificial Intelligent Systems and Ethical Agency. *Journal of Human Values*, 2023, vol. 29, no. 1, pp. 33–47. DOI: 10.1177/09716858221119546.

7. Zharova A.K. The intelligent image and meaning recognition systems in the crime prevention system. *Trudy po intellektual'noi sobstvennosti = Works on Intellectual Property*, 2024, vol. 49, no. 2, pp. 16–23. DOI: 10.17323/tis.2024.21708. (In Russ.).

8. Zharova A.K. Intellectual systems of pattern and meaning recognition in the system of prevention of crimes committed using the Internet. *Russian Journal of Economics and Law*, 2024, vol. 18, no. 2, pp. 469–480. DOI: 10.21202/2782-2923.2024.2.469-480. (In Russ.).

9. Tsygichko V.N., Alekseeva I.Yu. *Information challenges to national and international security*, ed. by A.V. Fedorov and V.N. Tsygichko. Moscow, PIR Center for Political Studies Publ., 2001. 328 p. (In Russ.).

10. Gulabyan A.O., Smirnov V.M. The main directions of information protection and information systems resources. *Tendentsii razvitiya nauki i obrazovaniya*, 2022, no. 88-1, pp. 45–46. DOI: 10.18411/trnio-08-2022-13. (In Russ.).

11. Ruzanova E.A. Means of information protection in LAN, in: *Theory and practice of modern science: the view of youth*, Proceeding of the III All-Russian Scientific and Practical Conference in English (St. Petersburg, November 30, 2023), in 2 parts, St. Petersburg, Saint Petersburg State University of Industrial Technologies and Design Publ., 2024, pt. 2, pp. 166–169.

12. Roizenson G.V. Modern approaches of formalization of the concept of ethics in artificial intelligence, in: *Proceedings of the International Conference on Computational and Cognitive Linguistics TEL-2018* (Kazan, October 31 – November 03, 2018), in 2 volumes, Kazan, Academy of Sciences of the Republic of Tatarstan Publ., 2018, vol. 1, pp. 306–331. (In Russ.).

13. Gallese Nobile C. Regulating Smart Robots and Artificial Intelligence in the European Union. *Journal of Digital Technologies and Law*, 2023, vol. 1, no. 1, pp. 33–61. DOI: 10.21202/jdtl.2023.2.

14. Kharitonova Yu.S. Legal Means of Providing the Principle of Transparency of the Artificial Intelligence. *Journal of Digital Technologies and Law*, 2023, vol., 1, no. 2, pp. 337–358. DOI: 10.21202/jdtl.2023.14.

15. Vasilevskaya L.Yu. The code of ethics for artificial intelligence: a legal myth and reality. *Grazhdanskoe pravo = Civil law*, 2023, no. 2, pp. 19–22. (In Russ.).

16. Laruel F. Two ethical principles in the technological world, transl. by E. Rudneva. *Filosofskaya antropologiya*, 2015, vol. 1, no. 1, pp. 49–61. (In Russ.).

17. Zharova A.K. Achieving Algorithmic Transparency and Managing Risks of Data Security when Making Decisions without Human Interference: Legal Approaches. *Journal of Digital Technologies and Law*, 2023, vol. 1, no. 4, pp. 973–993. DOI: 10.21202/jdtl.2023.42.

18. Begishev I.R., Zharova A.K., Zaloilo M.V., Filipova I.A., Shutova A.A. Digital and Nature-like Technologies: Features of Legal Regulation. *Journal of Digital Technologies and Law*, 2024, vol. 2, no. 3, pp. 493–499. DOI: 10.21202/jdtl.2024.25.

19. Begishev I.R., Khisamova Z.I. *Artificial intelligence and criminal law*. Moscow, Prospekt Publ., 2024. 192 p. (In Russ.).

20. Zharova A.K. Informational and psychological violence in criminal law. *Informatsionnoe obshchestvo*, 2024, no. 2, pp. 103–111. (In Russ.).

21. Halezov S.A. Ethics of artificial intelligence, in: *Nauka. Tekhnika. Chelovek: istoricheskie, mirovozzrencheskie i metodologicheskie problemy*, Interuniversity collection of scientific papers, iss. 13, Moscow, Moscow State Technical University of Civil Aviation Publ., pp. 240–246. (In Russ.).

22. Sushchin M.A. Taddeo M. Three ethical challenges of artificial intelligence applications in the field of cybersecurity (Abstract), in: Bulavinov M.P. (ed. & comp.). *Etika nauki*, Collection of reviews and abstracts, Moscow, Institute of Scientific Information on Social Sciences of the Russian Academy of Sciences Publ., 2022, pp. 175–178. (In Russ.).

23. Perevozchikova D.A., Zaripova M.Y. Ethics of artificial intelligence. *Nanotekhnologii: nauka i proizvodstvo*, 2024, no. 3, pp. 26–30. (In Russ.).

24. Lizikova M.S. Ethical and legal issues of artificial intelligence development. *Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk = Proceedings of the Institute of State and Law of the RAS*, 2022, vol. 17, no. 1, pp. 177–194. DOI: 10.35427/2073-4522-2022-17-1-lizikova. (In Russ.).

25. Dodonova V., Dodonov R., Gorbenko K. Ethical Aspects of Artificial Intelligence Functioning in the XXIst Century. *Studia Universitatis Babeş-Bolyai. Philosophia*, 2023, vol. 68, no. 1, pp. 161–173.

26. Giarmoleo F.V., Ferrero I., Rocchi M., Pellegrini M.M. What ethics can say on artificial intelligence: Insights from a systematic literature review. *Business and Society Review*, 2024, vol. 129, iss. 2, pp. 258–292. DOI: 10.1111/basr.12336.

INFORMATION ABOUT AUTHOR

Anna K. Zharova – Doctor of Law, Associate Professor, Leading Researcher
Institute of State and Law of the Russian Academy of Sciences
10, Znamenka ul., Moscow, 119019, Russia
E-mail: anna_jarova@mail.ru
ORCID: 0000-0002-2981-3369
ResearcherID: H-4012-2015
RSCI SPIN-code: 2240-1467

BIBLIOGRAPHIC DESCRIPTION

Zharova A.K. Legal aspects of artificial intelligence in ensuring national security: challenges and threats. *Pravoprimenenie = Law Enforcement Review*, 2025, vol. 9, no. 4, pp. 36–46. DOI: 10.52468/2542-1514.2025.9(4).36-46. (In Russ.).