

# Artificial Intelligence and Information Security: Legal Regulation, Prospects, and Risks (Real and Perceived Threats)

Anna A. Chebotareva<sup>1</sup><sup>a</sup>, Natalia G. Kazantseva<sup>2</sup><sup>b</sup> and Ekaterina S. Vologdina<sup>2</sup><sup>c</sup>

<sup>1</sup>Russian university of transport (MIIT), Moscow, Russia

<sup>2</sup>Transbaikal state university (ZabGY), Chita, Russia


**Keywords:** Artificial Intelligence, Security, Cyber Threats, Authentication, Trust Space.


**Abstract:** At the turn of the second decade of the 21st century, the foundations of the importance of the information sector for humanity and the need to effectively ensure information security seems fairly obvious. The speed and dynamics of the implementation of cross-cutting digital technologies into public relations actualize the latest information challenges and threats, both real and perceived. The nature of the development of the modern information society specifies the awareness of the need for the development of artificial intelligence technologies and, clearly, lead to an understanding of the special role of legal support for information security. This makes it appropriate to study the experience of regulating artificial intelligence technologies in foreign countries, which will subsequently make it possible to assess the possibility of applying such experience in the Russian Federation. The result of such an assessment is the basis for determining further directions for the development and the content of information security measures. Assessment of the current state of public relations in the information sector, the degree of their resilience and formation intensify in the domestic legal science the problem of regulation of artificial intelligence systems, which is practically not studied. Obviously, this is related to the novelty of the studied public relations, as well as their influence on information security. Currently, in Russia and worldwide, some models of regulating artificial intelligence technologies have been developed. However, a unified information concept that would contribute, among other things, to ensure global security none yet exists. Overall, this issue assumes an interdisciplinary approach that takes into account both social, ethical, and political, economic factors, and, obviously, an effective legal mechanism. In order to establish the legal relevance of cross-cutting digital technologies and information security, based on the analysis and study of models for regulating artificial intelligence technologies in Russia and abroad, we can come up with a possible concept for ensuring information security in Russia, considering digital innovations.


## 1 INTRODUCTION

Extensive changes in the context of the development of cross-cutting digital technologies create preconditions for exacerbating national security problems, form challenges to the triad of the personal interests, society and the state and ensuring their security in the information sector. Digitalization processes, the digital economy are rapidly replacing the old way of working in modern society. Understanding that, on the one side, due to information technologies, the efficiency of most

sectors of the economy and public administration is increasing, the possibilities of interaction between subjects of legal relations through new cross-cutting digital technologies, artificial intelligence, and robotics, are expanding, the speed of development and adoption of managerial decisions is increasing. At the same time, from the opposite side, currently, there is a positive trend of growth in the number of cyberattacks. According to analytics, products from such programs as Kaspersky and Cisco detect more than 700 million online attacks per quarter all over the world and block about 20 billion network attacks per

<sup>a</sup> <https://orcid.org/0000-0001-7886-1685>

<sup>b</sup> <https://orcid.org/0000-0003-2400-3233>

<sup>c</sup> <https://orcid.org/0000-0002-3958-0941>

day. The above allows us to note the improvement and transformation of a new type of malicious activity by cybercriminals through the automation of cyberattacks, including the use of artificial intelligence technology and machine learning in order to bypass known information (data) protection tools. It also identifies possible areas of negative (malicious) use of artificial intelligence technologies that crack passwords or ignore the authentication process, the significance of which is speculated by many authors (Ratha, et al., 2001; Chebotareva et al., 2020; Sapuay et al., 2019). Using a large array of data sources in the darknet to form a system of stable knowledge of artificial intelligence, malefactors can attack on a personal data of the person. To counter new challenges and threats, existing protection systems are interested in the active implementation of cross-cutting digital technologies, including global ML / DL technologies, used to detect, anticipate possible cyber threats and effectively respond to them in real time. For this reason, the problems of ensuring information security are becoming especially urgent and acute.

The legal and organizational issues of cross-cutting information technologies increase the level of response to the latest risks and actualize the requirements for the level of information protection. In an emerging environment of an information and legal trust space, this issue is on the agenda as a priority. This study focuses on models (approaches) of legal support for artificial intelligence technologies.

Scientific interest in the problems of the building of a legal support system for artificial intelligence technologies, robotics and their impact on information security is seen in various humanities: philosophy, political science, cultural studies, psychology, pedagogy, economics, sociology, and others, and is also reflected in the study of trends in the development of the information environment. as a principal defining factor in the life of modern society.

In this study, this problem is considered in several aspects: social, ethical, political, economic, legal. Such interdisciplinary approach will justify a possible adequate mechanism for legal support of cross-cutting digital technologies through interaction with information security, and propose a possible concept for ensuring security in Russia, considering digital innovations.

## 1.1 Related Work

In accordance with the specifics of this study, we present an overview of the scientific and methodological basis.

1.1.1. The stated purpose of this study was achieved through the use of a complex of general scientific and special research methods. The methods of analysis and synthesis were used as the basic general scientific methods, the use of which made it possible to conceptualize the main sections of the research area, and also made it possible to create a line of the author's scientific concepts. The induction method led to identify the specific features of artificial intelligence within the framework of the general structure of the legal regulation of information technologies. The use of special methods, particularly, comparative legal method, led to summarize the world law enforcement experience and identify the specifics of existing approaches and assessments of the studied definitions based on foreign concepts.

1.1.2. Secondly, we note that the study addressed a serious issue that requires special assessments and consideration of the model of regulation of artificial intelligence technologies as the most relevant empirical area.

## 1.2 Our Contribution

The focus of researching technological features and the legal nature of not only artificial intelligence, but also other cross-cutting digital technologies (the Internet of Things, augmented reality, blockchain technology, etc.) is becoming a subject of active interest for specialists in all branches of knowledge. Nevertheless, in any case, all scientists recognize the problem of security as fundamental, requiring the close attention in the context of the most powerful development of all cross-cutting digital technologies. So, B.K.Mohanta, D.Jena, U.Satapathy, S.Patnaik, studying machine learning (ML), artificial intelligence (AI) and blockchain, indicate the importance of information security, privacy issues in the study of the Internet of Things, "one of the fastest-growing technologies in the last decade" in their opinion (Mohanta et al., 2020). In recent years, the number of studies of possible areas of application of artificial intelligence (in health care, education, mechanical engineering, etc.) has noticeably increased, while the authors, with their studies, confirm the possibilities of developing the latest technologies only under the condition of a parallel solution of the problems of organizational and legal

support of information security. Thus, the issue of ensuring safety in the use of artificial intelligence in medicine in general, in telemedicine, is widely discussed. J.P.Hlávka in Chapter 10 "Security, privacy, and information-sharing aspects of healthcare artificial intelligence" of the book "Artificial Intelligence in Healthcare" explores the issues of security and privacy, including the risks and opportunities associated with new technologies based on artificial intelligence in healthcare, and potential problems for its implementation due to regulatory interference (Hlávka, 2020). And the use of artificial intelligence in outer space activities, for example, according to A.-S.Martin and S.Freeland (Martin and Freeland, 2021), this is not only new opportunities, but also new problems for international space legislation, primarily due to the relevance of the issue of responsibility in the carrying out of space flights in the event of damage caused by advanced artificial intelligence. At the same time, it must be admitted the general concern about the problems of the impact on the development of artificial intelligence and on national security, as indicated regarding to the United States by the authors of the study "Artificial Scientific Intelligence and its Impact on National Security and Foreign Policy" E. Briscoe and J. Fairbanks (Briscoe and Fairbanks, 2020), and global security in general. In our study, we will further refer in greater detail to a number of developed foreign concepts (Calo, 2009; Kurzweil, 1990; Rissland, 1990).

### 1.3 Paper Structure

1.3.1. The study is structured and corresponds to the stated issues. Section 2 outlines the legal aspects of the development of cross-cutting digital technologies at this stage of the development of the information society and the key issues of ensuring information security. Section 3 presents foreign experience (approaches and concepts) of subject regulation of artificial intelligence technologies (on the example of some countries - China, France, South Korea, Japan). In Section 4 of this study, scientific conclusions are formulated.

## 2 BACKGROUND

The development of artificial intelligence technologies has been known for several decades. Primarily, the principle of artificial intelligence was based on a given set of rules. In the 70s, artificial intelligence technologies based on neural networks became widespread. In the early 2000s, there was an

active development of artificial intelligence for solving certain practical problems, for example, image, video, voice processing. In 2005-2008, the development of artificial intelligence was considered from the position of ensuring information security. And it was aimed at protecting highly attacked resources - web servers.

The ubiquitous processes of introducing artificial intelligence and robotics technologies into various areas of human life, their use in protecting against cyber attacks (cyber threats) is becoming one of the key issues in ensuring information security. In the current realities, this is a perspective, and in the near future, it is an actual reality. Some experts, for example, Elman Beibutov, rightly stated that "it is important not to collect as much information as possible, there is a lot of it around, but to understand how to structure and process it correctly so that automated protection tools work efficiently and safely" (Application of machine learning and artificial intelligence technologies in information security). It is obvious, since today IBM has created a number of information security products (cybersecurity products) that use the power of a supercomputer called Watson. The project was originally intended for the healthcare industry, but now the artificial intelligence of the Watson supercomputer has the ability to structure data regardless of the industry.

Exceptionally and unprecedented attention of the state to all the constituent processes of digitalization, which confirms the special significance of new public relations and the state's concern on the problem of digital data circulation, the implementation and exploitation of cross-cutting digital technologies, the creation of an effective system of legal regulation of information security that properly responds to contemporary security challenges and threats. As a result, the implementation of amendments to the Constitution of the Russian Federation, Article 71, clause "m", according to which the main issues of "ensuring the safety of the individual, society and the state when using information technologies, digital data circulation" are attributed to the jurisdiction of the Russian Federation, as well as traditionally the most important areas of government, such as defense, security.

An important direction in the development of regulation of the investigated cross-cutting digital technology was signified by the National Strategy for the Development of Artificial Intelligence for the period up to 2030. In the provisions of the Strategy, initially at the legislative level, definitions of some terms that were not previously mentioned in

regulatory legal acts were fixed. This is the wording of the dominant term of the Strategy, artificial intelligence as “a complex of technological solutions enabling to simulate human cognitive functions (including self-learning and search for solutions without a predetermined algorithm) and to obtain results comparable, at least, to the results of human intellectual activity when performing specific tasks. The complex of technological solutions includes information and communication infrastructure, software (including which uses machine learning methods), processes and services for data processing and finding solutions.” We consider it necessary to highlight that the essence of the stated term is interpreted exclusively for the purposes of the Strategy and is not considered as universal. In this regard, the legislator envisages the possibility of different formulations of the key term in relation to the scope of its use.

One of the defining factors of the National Strategy is expressed in “the creation of a comprehensive system for regulating public relations arising in connection with the development and employing of artificial intelligence technology.” Public relations related to information security are disclosed only through the basic principles set out in the Strategy, one of which is security, expressed in the prevention of the use of AI systems and technologies for the purpose of deliberately causing harm to subjects of public relations (citizens and legal entities), prevention and minimization of risks and threats of negative consequences. This principle has a clearly expressed legal character, since it will undoubtedly have an impact on the adopted regulations in the investigated area. Considering new challenges and threats, the provisions of the Strategy reflect the position of the legislator in the need to adapt normative regulation in terms of human interaction with artificial intelligence and the development of ethical standards. Therefore, for the successful implementation of the goals and objectives formulated in the investigated document, in the context of the further development of artificial intelligence technologies, there is a conscious need to form an integrated security system, including information system.

Thus, the Strategy has identified an obvious advanced model and the main directions for the development of artificial intelligence technologies. However, Russia is far from being the first to create strategic documents in the area under study.

3. In this regard, the approaches to subject regulation that have developed in a number of countries are indicative, for example, China, France,

South Korea, Japan, where national Strategies have been adopted, but individual acts of governance with norms of direct action are also perceived.

Summarizing the practical experience of China and France in the application of artificial intelligence technologies made it possible to identify an approach that distinguishes two levels of regulation - national and local. In particular, in China, at the national level, a Concept that includes a set of strategic documents and plans for the development of the robotics industry - the Global State Development Program “Made in China-2025” has been developed, as well as the 2017 New Generation Artificial Intelligence Technology Development Plan. In France, the provisions of the strategic planning document dated 2018 “National Strategy on Artificial Intelligence” are applied. This Strategy is based on the ideas of the scientist Cedric Villani. In the scientific report “Making sense of artificial intelligence as a European and national strategy” (Digital economy of France and Russia: forecast analysis) (Villani Report), the author pays attention to the mass adoption of artificial intelligence technologies in France. Villani Report describes the importance of introducing AI in four priority areas: health, mobility, environment and safety - all of which “represent a serious problem from a common interest point of view.” For example, Villani focuses on creating an advanced platform for “data consolidation for security innovation”. Note that in France, the cybersecurity pact concluded in 2019 is the basis for regulating the investigated technologies and their relationship with information security. The pact regulates confidence and security issues in cyberspace.

In some countries, increased attention is paid to the rules of direct action, which govern the use of specific types of artificial intelligence systems. Strategic planning documents are absent at all, or exist and are used as a “universal (complex) regulator”, but there are laws on specific types of artificial intelligence and robotics technologies. An outstanding example is South Korea, where acts of direct action are the Law “On the Promotion and Distribution of Smart Robots” No. 9014 dated March 28, 2008, acts of introduction of unmanned vehicles, unmanned aerial vehicles, the Memorandum “On the establishment of a joint venture for the development and production of new vertical landing strips for UAV”, Laws “On Aviation Security” and “On Aviation Business”, applied since 2017).

The experience of artificial intelligence technologies in Japan permits the conclusion that the goals and objectives of legal regulation are indicated in the Fifth basic scientific and technical plan, a

comprehensive Japanese model of the social and economic structure of Society 5.0 "Technological strategy for the AI development". Nevertheless, in each area of government, the legal basis is formed by its own (national) plans for the development of advanced areas, for example, the "Public/Private R&D Investment Strategic Expansion Program".

Based on the above, we believe that to this day a sufficient number of intelligent technological solutions have been developed in world practice, but there is no comprehensive formalization of the norms governing relations in relation to the use of AI technologies in all their diversity. Therefore, the authors of this study found it possible to highlight some approaches to legal regulation in countries with the highest level of production and implementation of artificial intelligence technologies.

Referring to foreign concepts of regulation of cross-cutting digital technologies, we can single out several fundamental approaches created by the scientific community of different countries (Calo, 2009; Kurzweil, 1990; Rissland, 1990). One of the remarkable concepts is the theory of externalities, proposed by the Belgian scientist Nicholas Petit in the scientific work "Law and Regulation of Artificial Intelligence and Robots - Conceptual Framework and Normative implications" (Petit, 2017). In this study, we consider it necessary to review a number of provisions described by this author, which are of interest to legal science from the position of establishing the relevance of the development of legislation on artificial intelligence technologies and information security in Russia. Thus, the author describes modern approaches to the AI regulation: legalistic and technological. The first approach identifies the most important legal institutions in the legislative system that are influenced by the activities of cross-cutting digital technologies. One of these institutions is security in general, information security, security in cyberspace, confidentiality of personal information, identification, and authentication. The essence of the second approach is to predict various problems that may arise in the framework of the use of innovative technologies and techniques, for example, unmanned vehicles, exoskeletons, robots, and others. According to the authors of this study, the complexity of the developing of a unified concept of information security lies in the choice of a specific direction of regulation, one of the regulatory models that should be implemented in the context of the development of new technology. In the investigated study, the author (N. Petit) describes the following regulatory measures (models) for establishing a system of legal

support for the investigated issue: limiting, instinctive, administrative rent model, regulatory model (providing opportunities). Analysis of the content of these measures allowed us to state that the issue of lagging regulation is one of the most advanced. A pattern that the regulatory process is unable to proceed at the same (or possibly outstripping) rates as the development of technologies is revealed. G.N. Mandel rightly points out, that new technologies leads to a legal dilemma: "opportunities and threats (risks) cannot be understood and assessed correctly from a legal position until these technologies are further developed". As a consequence, the regulatory process must be in constant synergy with technology. The authors identified that the problems revealed in the works of researchers, especially in the work of N. Petit, summarize the trends in ensuring global and Russian security.

### 3 CONCLUSION

In the context of the existence of artificial intelligence as a trend direction, it is necessary to state the validity of the existing judgments and approaches about the possibility of significant risks for citizens, society and the state in general, and information security in particular. The concepts reviewed in this study, particularly, the need to form a high-quality system of norms that provide a proper guaranteeing mechanism for protection against possible violations of rights, freedoms and legitimate interests using artificial intelligence.

Cross-sectoral issues regarding certain issues of using artificial intelligence technologies as special information systems deserve particular attention, since the tasks of ensuring information security, regulating access to such technologies, their integration with the external environment, become relevant both in science and in reality. Information and legal aspects will play a central role in resolving identification problems and establishing legal personality limits for artificial intelligence systems (Naumov, 2016).

Note that the Russian practice of improving artificial intelligence technologies and introducing new ones is in a state of intensification, and further successes in the development of this area are directly related to the results of approbation and the positive effect of the development of the corresponding regulatory framework - on the territory of the constituent entities of the Russian Federation. In this regard, it is possible to point out a tendency to

introduce experimental legal regimes to establish special regulation for creating the necessary conditions for the development and implementation of artificial intelligence technologies, for example, in the constituent entity of the Russian Federation - the city of federal importance Moscow, as evidenced by the adopted Federal Law dated April 2020. The purpose of its adoption is aimed at conducting a legal experiment on the territory of the city related to the development of artificial intelligence technologies. Carrying out the existing multi-component branched system of implementation - artificial intelligence technologies, machine learning, technological solutions, big data - is expensive from an economic point of view and seems premature (especially in the territories of such subjects of Russia, which are significantly lagging behind in information, communication and technical aspects).

Consequently, in the Russian Federation by 2030, it is expected to create a flexible, efficiently functioning, valid system of regulatory support in the field of artificial intelligence, which will guarantee the information security of the country's population and aimed at stimulating the development of new cross-cutting digital technologies.

## REFERENCES

- Application of machine learning and artificial intelligence technologies in information security. [https://www.antimalware.ru/analytics/Technology\\_Analysis/machine-learning-and-artificial-intelligence-in-is](https://www.antimalware.ru/analytics/Technology_Analysis/machine-learning-and-artificial-intelligence-in-is)
- Briscoe, E. and Fairbanks, J. (2020). Artificial Scientific Intelligence and its Impact on National Security and Foreign Policy. *Orbis*, 64(4): 544-554. Doi.org/10.1016/j.orbis.2020.08.004
- Chebotareva, A. A., Danilina, E. I. and Chebotarev, V. E. (2020). Electronic Passports of Citizens as a Personal Essential Attribute During the Pandemic. *Proceedings of the Research Technologies of Pandemic Coronavirus Impact (RTCOV 2020). Advances in Social Science, Education and Humanities Research*, volume 486. ISBN 978-94-6239-268-7. DOI: <https://doi.org/10.2991/assehrk.201105.083>.
- Digital economy of France and Russia: forecast analysis. <https://zen.yandex.ru/media/id/5d3d76f9ec575b00be402a52/cifrovaia-ekonomika-franciia-i-rossiia-prognozni-analiz-5ef228e1211879584d8d583f>
- Fifth basic scientific and technical plan. URL: <https://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf>.
- Hlávka, J.P. (2020). Security, privacy, and information-sharing aspects of healthcare artificial intelligence. *Artificial Intelligence in Healthcare*, Academic Press, pages 235-270, ISBN 9780128184387. Doi.org/10.1016/B978-0-12-818438-7.00010-1
- Kurzweil, R. (1990). *The Age of Intelligent Machines*. Cambridge, Mass., MIT Press.
- Martin, A-S. and Freeland, S. (2021). The Advent of Artificial Intelligence in Space Activities: New Legal Challenges. *Space Policy*, 55: 101408. Doi.org/10.1016/j.spacepol.2020.101408
- Mohanta, B.K., Jena, D., Satapathy, U. and Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, 11: 100227. Doi.org/10.1016/j.iot.2020.100227
- Naumov V. B. (2016). Scientific approaches to the classification of types of legal identification in information legal relations. *Proceedings of the Institute of State and Law of the Russian Academy of Sciences*, 3 (55): 104-115.
- Petit N. (2017). *Law and Regulation of Artificial Intelligence and Robots: Conceptual Framework and Normative Implications*, 31 p. <https://ssrn.com/abstract=2931339>
- Ratha, N. K., Connell, J. H. and Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *Ibm Systems Journal*, 40(3): 614-634. DOI: 10.1147/sj.403.0614
- Rissland, E.L. (1990). Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning. *The Yale Law Journal*, 99(8): 1957-1981.
- Calo, Ryan M. (2009). People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship. *Penn State Law Review*, 114(3): 809-855.
- Sapuy Sheena I., Gerardo Bobby D. and Hernandez Alexander A. (2019). Dynamic Third-Factor for Enhanced Authentication in Human Resource Information System. *IEEE 7th Conference on Systems, Process and Control (ICSPPC 2019)*, Melaka, Malaysia. DOI: 10.1109/ICSPPC471372019.9068077