JURNAL CITA HUKUM (Indonesian Law Journal)
FSH UIN Syarif Hidayatullah Jakarta
Vol.12 No. 3 (2024), pp. 505-516, DOI: 10.15408/jch.v12i3.42520

Artificial Intelligence and the Issue of Information Protection: Legal Aspect*

Vladislav Kudryavtsev[1], Mikhail Leontev[2], Aleksandr Riabchenko[3], Elman Akhyadov[4], Nataliia Panova[5], Vasily Sinyukov[6]

[1]St. Petersburg Institute (branch) of the All-Russian State University of Justice (RPA Russian Ministry of Justice), Russia

[2] Moscow State University of Civil Engineering (National Research University), Russia

[3] Kuban State Agrarian University named after I.T. Trubilin, Russia

[4] Chechen State University, Russia

[5] Moscow Polytechnic University, Russia

[6] Pacific National University, Russia

10.15408/jch.v12i3.42520

Abstract

The development and use of artificial intelligence (AI) brings new challenges related to information protection, which is an important concern in the legal context of today's digital era. This article aims to analyse the legal aspects of information protection in the development and application of AI. This research was conducted using qualitative methods through a literature approach and analysis of legislation, both at the national (Russian) and international levels. The analysis results show that the main objects of information protection in the context of AI include trade secrets, professional secrets, and personal data. Therefore, entities holding trade and professional secrets and processing personal data must handle this issue under the applicable legal framework. This article concludes that existing regulations need to evolve to accommodate information protection challenges in the dynamic AI ecosystem.

Keywords: Artificial Intelligence; Information Protection; Trade Secret; Professional Secrets; Personal Data.

* Received: July 25, 2024; revised: July 26, 2024; accepted: August 22, 2024; published December 29, 2024.

[1] **Vladislav Kudryavtsev**, St. Petersburg Institute (branch) of the All-Russian State University of Justice (RPA Russian Ministry of Justice), Russia. ORCID: https://orcid.org/0000-0003-3141-2676 E-mail: kudryavtsev@mymail.academy

[2] **Mikhail Leontev**, Moscow State University of Civil Engineering (National Research University), Russia. ORCID: https://orcid.org/0000-0001-8192-6523 E-mail: leontev@mymail.academy

[3] **Aleksandr Riabchenko**, Kuban State Agrarian University, named after I.T. Trubilin, Russia. ORCID: https://orcid.org/0009-0007-8848-612X E-mail: riabchenko@mymail.academy

[4] **Elman Akhyadov**, Chechen State University, Russia. ORCID: https://orcid.org/0000-0002-0793-1727 E-mail: akhyadov.e.s.m@mail.ru

[5] **Nataliia Panova**, Moscow Polytechnic University, Russia. ORCID: https://orcid.org/0000-0002-7752-8263 E-mail: panova@mymail.academy

[6] **Vasily Sinyukov**, Pacific National University, Russia. ORCID: https://orcid.org/0000-0001-6266-0088 E-mail: sinyukov.vas@yandex.ru

****Corresponding author**: e-mail kudryavtsev@mymail.academy

A. INTRODUCTION

Despite a breakthrough in artificial intelligence (hereinafter referred to as AI) with the introduction of the GPT language model by the American company OpenAI, discussions about AI date back to the mid-20th century (Bostrom, 2016). The continuous advancement of technology has led to the development of AI solutions used in everyday activities. Over time, AI has permeated various spheres of life, creating a revolution for many people. Some view this as developmental potential, while others consider it a threat (Russell & Norvig, 2015). Therefore, studying the fundamentals of the legal aspects of AI operations is relevant, particularly in information protection.

Currently, the prevailing reality of legal regulation does not match the breakthroughs achieved by AI. In the absence of regulatory acts specifically addressing AI, the resolution of existing issues must be found within the current regulatory framework, or at least an attempt must be made. The need to regulate many AI-related issues has become evident.

Recent years have shown that the continuous development of new technologies also demands closer attention to AI-related solutions. Given AI's potential in all fields, understanding its operations is essential to using AI skillfully, safely, and legally.

Literature Review

Modern legal scholars devote considerable attention to regulating various aspects of AI functioning. Research focuses on general legal issues of AI use (Kartskhiya & Makarenko, 2024; Morkhat, 2017; Yastrebov, 2018), issues of AI legal regulation (Kholodnaya, 2019; Minbaleev, 2020; Shestak & Volevodz, 2019), liability for unlawful AI application (Kibalnik & Volosyuk, 2018; Mosechkin, 2019), AI applications in jurisprudence (Balashova, 2022; Romanova & Vidova, 2023; Sokolova, 2021), the relationship between copyright and AI use (Abinov, 2022; Blednov, 2023), and AI's potential in judicial proceedings. (Amyants & Chemerinsky, 2019; Zaplatina, 2019)

However, the legal issues surrounding information protection in AI use require more in-depth research. As researchers in this field note, the reasonable use of AI solutions requires familiarity with key usage conditions, regulation of rights to AI products, and confidentiality conditions regarding input data. (Litvin, 2021)

According to M.B. Dobrobaba (2022), AI developers often shift responsibility to users, even though users may lack the ability to verify the data sources used to train AI and the process by which generated content is created. Users can influence the input data as commands, but this data may be inappropriate for various reasons. This makes it difficult to question user responsibility. Nevertheless, AI developers may use both input and output content to provide and support services.

The terms of AI use usually stipulate that services for processing personal data require information regarding privacy protection and obtaining necessary consent for data processing. Users assert that they process personal data in compliance with applicable laws. (Lipchanskaya & Zametina, 2020) This article analyses the legal aspects of information protection in developing and using artificial intelligence.

B. METHODS

This study explored the legal aspects of information protection in the development and use of artificial intelligence through a desk research methodology. The research involved a detailed analysis of information sources relevant to the topic, with the source base comprising two main categories. The first category included Russian and international regulatory frameworks, providing the foundational legal standards governing information protection in the AI domain. The second category consisted of academic articles and monographs, which analyzed the legal dimensions of information protection in AI development and application while also examining international legislation in this field. To process these sources, the study employed theoretical generalization, comparative analysis, and synthesis, enabling a comprehensive understanding of how existing legal frameworks address the challenges posed by AI technology. These methods facilitated the identification of gaps and opportunities for improving legal protections in this rapidly evolving area.

C. RESULTS AND DISCUSSION

The analysis of Russian and international regulatory frameworks regarding information protection in AI development and use identified the following objects of protection (Table 1).

Table 1. Objects of information protection in AI development and use

Objects of Information Protection	Sources
Trade Secrets	
Professional Secrets	
Personal Data	

Source: Author's research

Easy access to AI enables professionals such as lawyers, doctors, and others who may be legally required to maintain the confidentiality of the information in their possession to use AI in their daily work. Additionally, some corporate employees are prepared to incorporate the latest AI tools into their everyday tasks and may also be required to keep entrusted information confidential under non-disclosure agreements (NDAs).

According to Article 3 of the Federal Law "On Trade Secrets" (State Duma of the Federal Assembly of the Russian Federation, 2004), information constituting a trade secret is defined as "any kind of information (production, technical, economic, organisational, and other), including the results of intellectual activity in the scientific and technical sphere, as well as information on the methods of carrying out professional activities, which has actual or potential commercial value due to its confidentiality to third parties, which third parties cannot freely access on a legal basis, and for which the holder of such information has introduced a trade secret regime."

In the EU directive, a trade secret is understood as information that meets all the following requirements: (a) it is confidential in that it is not generally known or readily accessible to people within circles that usually handle such information in its entirety or the configuration and assembly of its components; (b) it has commercial value because it is confidential; (c) the person who legally controls it has taken reasonable steps under the circumstances to maintain its secrecy. (The European Parliament and the Council of the European Union, 2016b)

The broad definition of a trade secret means that it can encompass a large volume of information about a business and its operations. Its disclosure to third parties, who may be difficult or even impossible to identify, could result in significant losses for the company. The greatest threat is the leakage of confidential data.

Specific legal issues may arise regarding protecting trade secrets when using AI. For instance, when using GPT-4 or another language model, there may be cases where the content of requests includes information protected as a trade secret or confidential information under non-disclosure agreements (NDAs). Incorrectly formulated requests may result in AI developers gaining access to information that the business or its employees are prohibited from disclosing.

Most AI solutions store input data for a certain period, depending on the selected settings or product version. Some input content may become training data, allowing AI to improve its quality and accuracy. Additionally, these data originate from various sources, some of which may not align with the interests of the company or individual, not just the AI developer. Data leakage could weaken a business's market position, grant competitors access to confidential information, or result in other related losses. For an employee, it could mean the termination of employment and liability for the damage caused.

The legal challenges surrounding trade secrets and artificial intelligence (AI) remain unresolved, leaving businesses vulnerable to potential disclosure risks. To mitigate these risks, companies must establish comprehensive internal policies governing AI usage, clearly specifying permissible and strictly prohibited activities. These policies should outline precise procedures for employees in case of a confidentiality breach, ensuring swift and effective action to minimise potential damage. Additionally, the policies must identify and regulate access to sensitive information, specifying who is authorised to handle confidential data for AI-related tasks and general operations. By implementing such robust measures, businesses can create a secure environment that protects their trade secrets while fostering the responsible and ethical use of AI. This proactive approach is essential to navigating the uncertainties of current legal frameworks and ensuring long-term success in the evolving AI landscape.

When utilising language models in a business or organisational setting, taking proactive steps to mitigate the risk of trade secret disclosure is essential. A key approach is educating employees, collaborators, or partners about the potential legal risks of these advanced AI tools. Providing targeted training helps them understand how language models operate, the types of data they process, and the potential vulnerabilities associated with improper use. It is important to emphasise the relationship between the input data and the model's outputs, ensuring that sensitive or confidential information is handled cautiously. Businesses can significantly reduce the risk of accidental data leaks by fostering awareness and encouraging responsible usage practices. Moreover, this education empowers individuals to use AI tools effectively and ethically, aligning their usage with internal policies and broader legal obligations related to data security and confidentiality.

In unfair competition involving the disclosure, use, or acquisition of others' trade secret information, a business owner may demand, among other things, a declaration of relevant content and form or compensation for damages based on general principles. Furthermore, criminal liability applies to those who disclose or use trade secret information contrary to their obligations, causing serious harm to the business. However, violating a confidentiality agreement may lead to a contractual penalty for the disclosing party or liability for damages, depending on the agreement's terms.

Regarding protecting professional secrets, professionals such as legal consultants and attorneys must maintain the confidentiality of all information disclosed while providing legal assistance. Individuals bound by confidentiality obligations should exercise particular care when using AI to avoid disclosing confidential information. However, this does not exclude AI use for verifying specific questions or obtaining assistance in formulating appropriate responses, provided confidential information is not disclosed. Civil and disciplinary liability should be considered if individuals in these professions disclose a professional secret.

Recently, there have also been reports of judges using AI solutions and seeing potential in them. This is safe and effective if the obtained response can be precisely verified. Currently, AI supports human activity rather than replacing it, but it is conceivable that, shortly, court decision rationales may be written by AI tools adapted to the chosen sector. However, it is essential to control who oversees AI query results (Batchaeva et al., 2021). Similar observations apply to other sectors where AI could enhance or replace human labour.

Regarding personal data protection, adopting AI requires compliance with principles derived from data protection laws of various countries concerning the processing of personal data and the free movement of such data. Despite the breakthroughs by AI tools, developing clear personal data protection guidelines is still challenging, and data protection authorities also face this challenge.

AI users should pay attention to how each AI solution processes personal data, whether the input prompts and data are used for training, how long activity history is stored, and the methods used to secure the data. This is important for processing both the users' data and the data of other individuals that users may include in their queries. For example, ChatGPT Enterprise does not use user prompts and data for model training and provides data encryption, at least according to OpenAI's website. Terms of use and privacy policies for AI products are constantly updated, so users of specific AI versions are encouraged to monitor these changes. Caution when using these solutions requires familiarity with the service's terms. Careless use of such tools can lead to the unauthorised processing of personal data by users—and thus by AI products—and legal liability, including financial responsibility, in case of penalties.

Regarding OpenAI, its terms of use regulate situations in which users process others' data when using OpenAI services. Users must provide relevant privacy information and obtain the necessary consent for data processing. Additionally, they must state that they process personal data under applicable laws. For those using AI offered by OpenAI to process personal data, it is necessary to conclude a Data Processing Addendum. Thus, those using AI and processing personal data in AI products must ensure compliance with data protection obligations. Depending on the specific situation, they may act as data controllers, joint controllers, or processors.

First and foremost, it is essential for users employing AI to have a proper basis for processing the personal data of other individuals. They should also generally fulfil information obligations related to data processing and implement appropriate policies within their organisations. AI has also become a concern for data protection authorities that monitor the compliance of personal data processing with national laws. For example, the UK regulator overseeing data processing developed a set of obligations for users and developers employing such solutions.

In addition to citing the appropriate legal basis for personal data processing and defining the user's role, there is a need to publish information about data processing or, if disproportionate efforts are required, to provide such information directly to individuals. Users who are legal entities (businesses) must also determine how they will handle requests from individuals whose personal data they process, such as requests for correction, data access, or deletion. The literature highlights the need to foster public trust in data processing and apply transparency, data minimisation, data retention, and rights compliance principles. (Blednov, 2023)

The issue is further complicated by the fact that personal data entered as prompts may be transmitted beyond the jurisdiction of the respective state. Fulfilling the information obligation also involves informing individuals about any cross-jurisdictional transfer of personal data. For instance, on July 10, 2023, the European Commission issued a decision declaring the adequacy of personal data protection under the EU-U.S. Data Privacy Framework, which took effect on September 20, 2023. In this decision, the European Commission stated that the U.S. provides adequate protection for personal data transferred from the EU to U.S. organisations listed in a register maintained and published by the U.S. Department of Commerce. In such cases, transferring data to an organisation on this list does not require special permission (or contractual terms or corporate rules). However, if an organisation is not listed, data transfer is possible only after meeting the requirements outlined in Article 46 or 49 of the GDPR (The European Parliament and the Council of the European Union, 2016a). An important consideration for AI tools is their global accessibility, as the geographic origin of the user inputting a query can be unknown. Consequently, it is unclear who might, potentially on the other side of the world, gain access to another person's data through these tools.

Regarding AI developers, it should be noted that AI development stages have raised numerous concerns regarding processing personal data, including sensitive data. For instance, Italy temporarily blocked ChatGPT in its country due to concerns in this area. The Italian Data Protection Authority specified conditions OpenAI must meet regarding personal data to reinstate the tool's functionality in the country. This AI solution also attracted the attention of the European Data Protection Board, which formed a special working group on ChatGPT. In October 2023, the French Data Protection Authority issued GDPR compliance recommendations for creating and using AI involving personal data. Its website published "Practical AI Guidelines" as a compliance guide.

Additionally, a lawsuit was filed in a California federal court against Google for using public personal data from millions of users to train and develop AI products. A report by the Norwegian Consumer Council warns that one of the risks of training AI models is the potential download of publicly available user photos from the internet, such as social media profile pictures, which can be used without legal grounds or the knowledge of the individuals depicted to train AI models. It should be noted that images are also considered personal data. They may also be protected by copyright and related rights. The unauthorised inclusion of user photos in AI products without consent or an appropriate legal basis could be considered an infringement of image rights, requiring a case-by-case analysis. Thus, possible infringement of image rights has various dimensions, and AI solutions should be cautiously approached.

AI developers primarily use personal data during the training and resource creation stages. Here, a large volume of personal data may be processed by AI developers without users, or those whose data is included in training and resource data sets can exercise their core rights under data protection legislation. It is unclear which data are processed by developers, the source of such data, and the recipient.

AI interacts with personal data during AI training and resource creation, as well as when users input queries and generate output data. Therefore, AI developers should be subject to the obligations of data controllers at every stage of AI development where personal data processing occurs (e.g., during model training) and AI use. Their core responsibilities should include specifying the legal basis for data processing, fulfilling information obligations to individuals whose data are processed, limiting processing to the minimum necessary, and ensuring the exercise of rights by data subjects (e.g., correction or objection). Thus, the popularity of AI creates real challenges for changes to future provisions regarding personal data processing. Those processing personal data must address these issues within the existing legal framework.

D. CONCLUSIONS

The rapid development and integration of artificial intelligence (AI) into various sectors have led to significant legal challenges, especially regarding protecting confidential information, trade secrets, professional confidentiality, and personal data. Research results indicate that content, files, images, and similar materials users input into AI-generated queries may become a serious issue. The foremost concern is understanding if and how the AI developer uses the entered data, as submitting a request to obtain an AI product can lead to the disclosure of trade or other professional secrets. Finally, handling personal data is crucial for the lawful use of AI. Users should analyse all these aspects to avoid legal liability. Although AI offers numerous benefits, available AI products should be used prudently and legally.

The rapid advancement of artificial intelligence (AI) has created a pressing need for legal frameworks to adapt and evolve to address the unique challenges posed by this transformative technology. While these frameworks are still developing, businesses and individuals can take proactive steps to ensure the responsible use of AI. This includes adhering to existing laws and regulations, which provide a foundational structure for ethical AI implementation. Additionally, organisations should develop comprehensive internal policies that govern AI usage, emphasising transparency, accountability, and ethical considerations. Staying informed about ongoing legal and regulatory changes is also crucial, enabling businesses and individuals to anticipate and adapt to emerging requirements. By taking these measures, stakeholders can effectively navigate the evolving landscape of AI and its legal implications.

REFERENCES

Abinov, I. O. (2022). Pravovaya okhrana ob"yektov promyshlennoy sobstvennosti, sozdannykh iskusstvennym intellektom [Legal protection of industrial property objects created by AI]. *Young Scientist*. No. 28(423), 143-150.

Amyants, K. A., & Chemerinsky, K. V. (2019). The use of artificial intelligence in the modern judicial system and human rights. *International Journal of Humanities and Natural Sciences*. No. 11-3(38), 49-52.

Balashova, A. I. (2022). Iskusstvennyy intellekt v avtorskom i patentnom prave: Ob'yekty, sub'yektnyy sostav pravootnosheniy, sroki pravovoy okhrany [AI in copyright and patent law: Objects, subject composition of legal relations, terms of legal protection]. *Zhurnal Suda po intellektual'nym pravam*. No. 2(36), 90-98.

Batchaeva, E. K., Chistilina, D. O., Grinenko, A. V., Ryabinina, T. K., & Potapov, V. J. (2021). Russian court in adversarial criminal procedures. *Cuestiones Políticas*. Vol. 39, No. 71, 531-542. https://doi.org/10.46398/cuestpol.3971.30

Blednov, K. D. (2023). Problems of legal protection of the results of intellectual activity, including artificial intelligence systems. *Copyright*. No. 1, 114-127.

Bostrom, N. (2016). *Iskusstvennyy intellekt: Etapy, ugrozy, strategii* [Artificial intelligence: Stages, threats, strategies]. Trans. from English. Moscow: Mann, Ivanov and Ferber, 490 p.

Dobrobaba, M. B. (2022). Problema normativnogo obespecheniya prav grazhdan v usloviyakh razvitiya iskusstvennogo intellekta [Normative support for citizen rights amid AI development]. In V. N. Sinyukov (Ed.), *Rol' prava v obespechenii blagopoluchiya cheloveka* [Role of law in ensuring human well-being]: Collection of reports from the XI Moscow law week (pp. 324-327). Moscow: Publishing Center of the O.E. Kutafin University (MSAL).

The European Parliament and the Council of the European Union. (2016a). Regulation (EU) 2016/679 of April 27, 2016, on the protection of natural persons regarding the processing of personal data and the free movement of such data (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

The European Parliament and the Council of the European Union. (2016b). Directive (EU) 2016/943 of June 8, 2016, on the protection of undisclosed know-how and business information (trade secrets) from unlawful acquisition, use, and disclosure. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943

Kartskhiya, A. A., & Makarenko, G. I. (2024). Legal problems in using artificial intelligence in Russia. *Pravovaya informatika*. No. 1, 4-19. https://doi.org/10.21681/1994-1404-2024-1-4-19

Kholodnaya, E. V. (2019). About perspective directions of legal regulation in the sphere of artificial intelligence technology. *Courier of Kutafin Moscow State Law University (MSAL)*. No. 12(64), 89-96.

Kibalnik, A. G., & Volosyuk, P. V. (2018). Artificial intelligence: Doctrinal criminal law questions awaiting answers. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*. No. 4(44), 173-178. https://doi.org/10.24411/2078-5356-2018-10428

Lipchanskaya, M. A., & Zametina, T. V. (2020). Social rights of citizens using artificial intelligence: Legal bases and gaps in legislative regulation in Russia. *Journal of Russian Law*. No. 11, 77-96. https://doi.org/10.12737/jrl.2020.134

Litvin, I. I. (2021). Features of collection, processing and protection of personal data by artificial intelligence. *Bulletin of Ural Law Institute of the Ministry of Internal Affairs of Russia*. No. 4, 112-118.

Minbaleev, A. V. (2020). Regulirovaniye ispol'zovaniya iskusstvennogo intellekta v Rossii [Regulation of AI use in Russia]. *Informatsionnoye pravo*. No. 1, 36-39.

Morkhat, P. M. (2017). Pravovyye problemy primeneniya iskusstvennogo intellekta [Legal issues of AI application]. *Agrarnoye i zemel'noye pravo*. No. 10(154), 58-64.

Mosechkin, I. N. (2019). Artificial intelligence and criminal liability: Problems of becoming a new type of crime subject. *Vestnik of Saint Petersburg University. Law*. Vol. 10, No. 3, 461-476. https://doi.org/10.21638/spbu14.2019.304

Romanova, I. N., & Vidova, T. A. (2023). Problems of legal regulation of artificial intelligence in the field of jurisprudence. *Vestnik Moskovskogo universiteta imeni S.Yu. Vitte. Seriya 2. Yuridicheskiye nauki*. No. 3(39), 5-10.

Russell, S., & Norvig, P. (2015). *Iskusstvennyy intellekt. Sovremennyy podkhod* [Artificial intelligence: A modern approach] (2nd ed.). Trans. from English. Moscow: Williams, 1410 p.

Shestak, V. A., & Volevodz, A. G. (2019). Modern requirements of the legal support of artificial intelligence: A view from Russia. *Russian Journal of Criminology*. Vol. 13, No. 2, 197-206.

Sokolova, A. A. (2021). The challenges of artificial intelligence in jurisprudence: An interdisciplinary model of cognition. *Yuridicheskaya tekhnika*. No. 15, 245-249.

State Duma of the Federal Assembly of the Russian Federation. (2004). Federal Law of July 29, 2004 No. 98-FZ "On trade secrets" (latest revision) Retrieved from http://pravo.gov.ru/proxy/ips/?docbody=&nd=102088094&intelsearch=29.07.2004+%B998-%D4%C7&ysclid=m3j6xipwzu558648408

Yastrebov, O. A. (2018). Artificial intelligence in the legal space. *RUDN Journal of Law*. Vol. 22, No. 3, 315-328. https://doi.org/10.22363/2313-2337-2018-22-3-315-328

Zaplatina, T. S. (2019). Artificial intellect in the passing sentences issues or AI judge. *Courier of the Kutafin Moscow State Law University (MSAL)*. No. 4(56), 160-168.