Legal Issues in the **DIGITAL AGE**

1/2026

ISSUED QUARTERLY VOLUME 7

Publisher

National Research University Higher School of Economics

ISSN 2713-2749

The journal is registered in the Federal Service of Supervision of Communications, Information Technology and Mass Media. Certification of registration of mass media серия Эл № ФС77-83367

Address:
3 Bolshoy Triohsviatitelsky Per., Moscow 109028, Russia
Tel.:
+7 (495) 220-99-87
e-mail lida@hse.ru

Designer
Andrei Pavlov
Pre-press
Natalya Puzanova

Legal Issues in the **DIGITAL AGE**

Legal Issues in the **DIGITAL AGE**

ISSUED QUARTERLY

"Legal Issues in the Digital Age" Journal is an academic quarterly e-publication which provides a comprehensive analysis of law in the digital world. The Journal is international in scope, and its primary objective is to address the legal issues of the continually evolving nature of digital technological advances and the necessarily immediate responses to such developments.

The Digital Age represents an era of Information Technology and Information Communication Technology which is creating a reliable infrastructure to the society, taking the nations towards higher level through efficient production and communication using digital data. But the digital world exposes loopholes in the current law and calls for legal solutions.

"Legal Issues in the Digital Age" Journal is dedicated to providing a platform for the development of novel and analytical thinking among academics and legal practitioners. The Journal encourages the discussions on the topics of interdisciplinary nature, and it includes the intersection of law, technology, industry and policies involved in the field around the world.

"Legal Issues in the Digital Age" is a highly professional, double-blind refereed journal and an authoritative source of information in the field of IT, ICT, Cyber related policy and law.

Authors are invited to submit papers covering their state-of-the-art research addressing regulation issues in the digital environment. The editors encourage theoretical and comparative approaches, as well as accounts from the legal perspectives of different countries.

Publication in the journal is free of charge.

All materials are available for free download.

Legal Issues in the Digital Age. 2026. Vol. 7, no. 1.
Вопросы права в цифровую эпоху. 2026. Том 7. № 1.

Artificial Intelligence and Law

Research article
UDK: 347.3
JEL:K15
DOI:10.17323/2713-2749.2026.1.4.31

Copyright Borders in the Era of AI: Reconsidering the Concept of Free Use

Arina S. Vorozhevich
Lomonosov Moscow State University, 1 Leninskie Gory, Moscow 119991, Russia,
arinavorozhevich@yandex.ru, https://orcid.org/ 0000-0002-9908-2143

Abstract

The article examines current issue of legal qualifying use of copyright objects in artificial intelligence training. The author substantiates the need to amend the Civil Code of the Russian Federation by establishing a special case of free use of works for the purpose of training neural networks, including data collection. Based on the analysis of foreign experience and judicial practice, the author concludes that the use of works in the intellectual analysis of texts and data in digital form, including for the purpose of training neural networks, should be recognized as lawful provided that the form of the works is not perceived by human senses. It is proposed to extend this exception to any works in the public domain, including materials from the Internet and closed databases to which developers have obtained legal access. The paper substantiates the inexpediency of introducing a fee for the use of works in the process mentioned, as this may lead to a decrease in investment in technology development and complicate the process of training neural networks. At the same time, permissible and impermissible cases of use are clearly delimited: internal memorization of materials is not considered a violation, however, content generation with reproduction of significant parts of protected works is qualified as a violation of exclusive rights. It is substantiated the generation of works in the style of a particular author during neural network training based on his works may also constitute a violation of exclusive rights. Particular attention is paid to issues of liability for violations. The author proposes a differentiated approach according to which both the developer of the neural network and the user may be held liable, depending on the specific circumstances of the case. The study emphasizes the approach proposed will maintain a balance between protecting

the rights of content creators and the need to develop AI technologies are important for solving global challenges in various spheres of public life.

Keywords

copyright; rights holder; artificial intelligence; free use; infringement; exclusive rights.

For citation: Vorozhevich A.S. (2026) Copyright Borders in the Era of AI: Reconsidering the Concept of Free Use. *Legal Issues in the Digital Age,* vol. 7, no. 1, pp. 4–31. DOI:10.17323/2713-2749.2026.1.4.31

Introduction

For a neural network to be able to work with user queries, it must undergo deep training, which involves analysing large amounts of information. The neural network learns to identify patterns and establish connections between different pieces of information, understanding how textual descriptions relate to visual content in the process. This process is similar to human learning, whereby we analyse experience, find patterns and learn to apply them.

The training data sets may contain copyrighted material. It raises important legal questions about using such data. Do developers of AI systems need to obtain permission from copyright holders to use their work when training algorithms? Does using such works without consent of the copyright holders constitute an infringement of their exclusive rights? These questions must be considered in terms of both the technological process and legal norms.

The study is based on the general scholar methods of cognition: analysis, synthesis, induction, deduction, abstraction, classification, analogy and dialectical and formal logical methods.

The author follows the principles of a systematic and comprehensive consideration of the issues at hand, that reveals the various private and public interests involved. Considerable attention is paid to comparative legal methodology.

1. How Does the Training of a Network Take Place?

From a technical point of view, the learning process involves several stages.

Data collection and pre-processing. At this stage, texts and images are collected, cleaned up, and broken down into tokens. Consequently, developers receive regular copies of the data on disks and in RAM, along with the derived token sequences.[1] The main method of data collection is scraping. This automated technology extracts data from web resources for processing and storage. The second most common method is data extraction using application programming interfaces (APIs).[2]

The obtained data is filtered (second stage). Developers use automated tools to clean data sets by removing explicit content, watermarked materials and poor-quality samples. At the same time, a search is conducted for aesthetically valuable, high-level subsets of data, which are prioritised for AI training.

Deduplication is an important (third) part of processing: a technology that compresses data by removing duplicate elements. It minimises the risk of the neural network simply memorising the source information.[3] When creating datasets, developers often combine several source sets to create a single array with the desired characteristics and a wide range of data. For instance, the creators of the Pile dataset, which was used to train various language models, selected material from 22 subsets. These ones included the Pub Med Central archive, which contains nearly 5 million biomedical articles for solving applied problems in medicine, and the Books3 collection, which contains full-text books for forming coherent narratives. Developers use a process known as "ascending sampling", whereby certain subsets are given greater weight. The quality of the models depends directly on the quality of the training data[4].

The tokenisation process involves breaking down source data, such as text, into small units, or tokens, that a machine learning model is able work with. That operation converts unstructured information into a numerical format the model can interpret.[5]

---

[1] Frosio G. Copyright in Formaldehyde: How GEMA v Open AI Freezes Doctrine and Chills AI — Part 1. Available at: URL: https://legalblogs.wolterskluwer.com/copyright-blog/copyright-in-formaldehyde-howgema-v-openai-freezes-doctrine-and-chills-ai-part-1/ (accessed: 07.06.2025)

[2] An API is a software layer that facilitates communication between programmes.

[3] Copyright and Artificial Intelligence. Part 3: Generative AI Training pre-publication version: A Report of the Copyrights Register. May 2025. Available at: URL: https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf (accessed: 07.06.2025)

[4] Ibid.

[5] Why is tokenisation a "crutch", i.e. a work around? Cutting-edge approaches for next-generation large language models // Habr, 2025. Available at: URL:

a) Training cycle

Also that process involves breaking down source data, such as text, into small units, or "tokens," a machine learning model is capable then work with. This process converts unstructured information into a numerical format that the model can understand.

The system processes the dataset, performing forward and backward passes and updating billions of numerical weights. These weights are a key element of a neural network, determining its ability to learn and work with data. While they do not store information directly, they provide a mathematical description of how the model has learned to recognise patterns in the data. Once training is complete, the original corpus can theoretically be deleted, leaving only the parameter vector.

b) Model as an artifact

The saved model is an enormous matrix of weights. It cannot be "opened" to read text or view images. It is a condensed statistical representation of patterns in data and is not human-readable.

c) Generation (output) and search

The user sends a prompt to the neural network, requesting that it generate an image or text. During execution, the request is tokenised. The model then calculates the probability distribution for the next token and generates a sequence.

Analysts are debating whether training data is retained in models and distributed alongside them. AI developers insist that models do not contain copies of training materials, such as texts or images. They claim model weights are merely "long strings of numbers" reflecting statistical relationships between training tokens.[6]

However, cases in that AI has produced results virtually identical to copyrighted works call such claims into question. One such situation arose in the case of GEMA v. Open AI (see below). Based on these examples, expert community has concluded neural networks are capable

---

https://habr.com/ru/articles/873120/?ysclid=mk281q4saq556343593 (accessed: 07.06.2025)

[6] Copyright and Artificial Intelligence. Part 3: Generative AI Training pre-publication version: A Report of the Copyrights Register...

of retaining fragments of the creative works on which they were trained. Whether or not this occurs largely depends on the method used to train a particular neural network and the nature of the patterns studied. The statistical patterns that the model learns can range from the most abstract to the most specific.

The examples speak for themselves. In the first example, the neural network is trained to recognise different animals and generate images of them at the user's request. Relevant patterns relating to the appearance of animals are formed based on the analysis of numerous photographs, videos and drawings. The neural network does not need to memorise and reproduce images (i.e. protected works). This should be recognised as a general rule. However, some exceptions are possible.

In the second case, the neural network memorises either the appearance of a particular character (linking their name to an image) or the lyrics of a song. In this case, the learned pattern essentially constitutes the training data, since only one unique example was used for training[7].

According to specialists at the US Copyright Office, the degree to that data is memorised by a neural network is influenced by many factors, including the number of model parameters, presence of duplicate training data, repeated training on the same example, how unique the example is, and when the example appears in the training process.

Developers of neural networks often encounter the phenomenon of model overfitting. It occurs when the model is unable to identify common patterns in the training data, resulting in erroneous predictions when faced with new or unknown data.[8] Rather than generalising, the model merely memorises the training set. This often takes place due to limited training data or the presence of "noisy" data, resulting in the memorisation of unimportant details. The result is a system that simply reproduces the training set, rendering it practically useless.

Modern large language models integrate Retrieval-Augmented Generation (RAG) technology. That technology processes the user's request and extracts relevant information from databases, which is then supplemented before the final response is generated. The technology combines two key processes: extraction and generation. When a request is

[7] Ibid.

[8] A. Ryzhkov. Model Overfitting // Habr, 2024. Available at: URL: https://habr.com/ru/companies/skillfactory/articles/864234/?ysclid=mk2a1hfzbw794277095 (accessed: 07.06.2025)

received, the system searches the data storage for relevant materials, and the found texts are transferred to the neural network. The final answer is formed based on the content of the sources and the specifics of the initial query, ensuring the result is accurate and meaningful one.[9]

2. Legal Classification

AI training involves copying data to the computer's RAM, processing it, and then loading it into the neural network. In this context, the reproduction of works can be considered one of the ways in which they are used.

As set out in the Agreed Statements on the WIPO Copyright Treaty, the right of reproduction, as defined in Article 9 of the Berne Convention for the Protection of Literary and Artistic Works,[10] and the exceptions permitted by that Article fully apply in the digital environment. This is particularly relevant to the use of digital works.[11] Storing a work in digital form constitutes reproduction under Article 9 of the Berne Convention. According to Paragraph 2 of Article 1270 of the Russian Federation's Civil Code, reproducing a work includes recording it on electronic media and storing it in computer memory.

Reproduction of works or parts therefore also is producing when RAG technology is used. The following methods are possible: firstly, the AI developer uploads material to their own database. The generative system then extracts relevant information from this database and transmits it to the model alongside the user's query. In the second method, material is extracted from external sources, such as search engines or websites.

Content generated by neural networks does not typically reproduce works or parts of works that the AI was trained on. During training, the model only "memorised" general patterns or rules. However, this method can fail. Sometimes, a neural network will remember the specif-

[9] D. Laktionov. RAG and Big Language Models: What It Is and Why Business Needs It. Available at: URL: https://companies.rbc.ru/news/OcbKEJly0f/rag-i-bolshie-yazyikovyie-modeli-chto-eto-i-zachem-nuzhno-biznesu/?ysclid=mjyfvikn8i260495613 (accessed: 07.06.2025)

[10] Bulletin of International Treaties. 2003. No. 9.

[11] Available at: URL: https://new.fips.ru/documents/international-documents/dogovory/soglasovannye-zayavleniya-v-otnoshenii-dogovora-vois-po-avtorskomu-pravu.php?ysclid=mk2ash5xgt388580726 (accessed: 07.06.2025)

ic data examples it was trained on. In this case, works or parts thereof are reproduced or reworked when a derivative work is created at the content generation stage. The content may also be made available to the public.

Reproducing or using other people's work in any other way requires the consent of the copyright holders, unless it falls within the limits of their exclusive rights in terms of both substance and time. In some cases, AI developers seek the consent of rights holders. For example, in December 2023 Open AI company has announced its partnership with Axel Springer. According to the agreement between the two entities, Open AI has a right to use Axel Springer's works when training AI [Sag M., Yu P., 2025: 1215].

Works in the public domain (for that term of legal protection has expired) can be used for AI training. However, this cannot be the general rule for AI training. Neural networks need to process a huge array of data — i.e. thousands of works — to function with impact. It is also technically impossible to find and obtain consent from the copyright holders of all the materials used.

Training a neural network based solely on works in the public domain will significantly reduce its potential. In order for the system to function properly, it is necessary to explore contemporary cultural trends and the latest achievements in various fields, process fresh data and identify current patterns. Using outdated materials alone will prevent the model from keeping up with language developments, grasping new semantic connections and generating relevant responses.

Following expert opinion research, the US Copyright Office noted that requiring AI companies to license works included in training data could slow the development of important technology, strengthen the position of companies that can acquire or already possess sufficient data, and damage the country's competitiveness.[12]

Obviously, exceptions to exclusive rights and cases of free use are necessary in order to train neural networks. This is essential for the benefit of society. Neural networks can increase the efficiency of production and business processes, automate routine tasks and enhance forecasting in a variety of sectors. AI can also be used in creative fields, such as literature and painting, as well as in healthcare and pharmaceuticals, for example in diagnosing diseases and developing new drugs. Instead of blocking it, the law should promote the development of such technologies. However,

[12] Copyright and Artificial Intelligence.

this exception should not be used to justify any actions by neural network developers and users relating to the use of other people's work.

3. Approaches in Different Legal Systems

3.1. The Russian approach

The Russian Federation Civil Code stipulates a list of cases in that use of other people's works is free and not covered by exclusive rights. However, none of these relate to AI training. In the event of any dispute, there is a significant risk that such use will be deemed a violation of exclusive rights. According to current legislation, the legality of training a neural network based on someone else's work can be justified in some cases. According to Para 2 of Article 1270 of the Civil Code, the temporary or incidental recording of a work is permitted without the copyright holder's consent.

In many cases, data collected for AI training is only stored temporarily. The neural network analyses the data and identifies general patterns, principles and characteristics relating to specific objects. A trained model mainly contains highly abstract representations of the source data, such as patterns, regularities and connections. Neural networks do not work with letters or words, but with the numerical values assigned to them as part of the tokenisation process. The initial database may be deleted after training [Lukas A.J., 2023: 5].

In this case, the developer's collection and upload of neural network data may fall under Paragraph 2 of Article 1270, provided the initial set of selected data is deleted after training the AI. However, new questions arise here. According to the relevant legal provision, the temporary recording of a work is lawful if it is an integral part of a technological process whose sole purpose is the lawful use of the work. The problem is that AI training is not mentioned in the Civil Code as a legitimate use. It is not defined as a case of free use.

Therefore it seems that, in this case, none of the conditions required for the application of Paragraph 2 of Article 1270 of the Civil Code are met. However, this issue can be approached from a different perspective. Assuming that a trained neural network uses only abstract data and information about general patterns to generate output data, the purpose of temporary reproduction could be argued to be the ideas and information relating to the array of works rather than the form (expression) of

the works themselves. Using such data does not infringe exclusive rights. In this case, the temporary recording of the source data is carried out for legitimate purposes, provided that it was deleted after training. This means that the provisions of Paragraph 2 of Article 1270 may apply.

Additionally, neural network developers do not always delete the datasets used to train the AI. Large-scale developers often retain entire training datasets for use in future projects. This is confirmed by law enforcement practice. In such cases, the temporary nature of reproduction is irrelevant. This exception also does not apply to cases where the AI creates verbatim or substantially similar copies of training materials based on prompts without any external input from the user. This means the relevant data is present in one form or another in the weighting coefficients.

The reference to the temporary nature of reproduction does not remove a multitude of other questions about the conditions for the legality of training a neural network based on the work of others. Therefore it should be noted the Russian law needs to establish a separate exemption from exclusive rights for the purpose of training neural networks, as well as the conditions and limits of its application.

Many foreign legal systems have already addressed the challenges posed by the development of AI.

3.2. The EU experience

At the European Union level, two significant exemptions for AI development are enshrined in Articles 3 and 4 of Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market[13] (hereinafter — the Directive). These articles set out the conditions for the lawful intellectual analysis of texts and data. The Directive defines this as any automated analytical technology that aims to analyse text and data in digital form to obtain information, including patterns, trends and correlations, among other things.

Article 3 of the Directive permits research and cultural heritage bodies to reproduce and extract text and other data for academic purposes and intellectual analysis, provided they have lawful access to this data in the course of their research activities. The exception applies only to re-

[13] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market.

search bodies (non-profit entities primarily engaged in research, including educational institutions) and cultural heritage organisations (e.g. public libraries, museums and archives).

For the exception to apply, two conditions must be met: the activity must be carried out solely for academic purposes, and access to the materials must be lawful, either because the materials are available from open sources or because the organisation holds the relevant subscriptions and licences. However, subscriptions and licences do not necessarily include the right to perform intellectual data analysis. Conversely, the rights granted under Article 3 of the Directive cannot be waived or restricted by contract. This article is imperative in nature.

In accordance with Article 4 of the Directive, acts involving the reproduction and extraction of lawfully accessible works and other subject matter are permitted for the purposes of text and data mining. Any entity (not just research organisations) may benefit from the exemption. However, it only applies to publicly available data for which rights holders have not imposed restrictions on its use in AI training using machine-readable means.

According to most European scholars, the exceptions set out in Articles 3 and 4 of the Directive apply to AI training purposes. The latter is considered a specific instance of the intellectual analysis of data and texts [Hellwig F., 2019: 40]; [Senftleben M., 2022: 1480]; [Dermawan A., 2023: 45–48].[14]

Many European researchers believe that, *de lege ferenda*, AI developers should pay copyright holders for using their work. According to M. Senftleben, authors should be compensated for the "parasitic usurpation of the AI market." Generative AI merely imitates human literary and artistic creations after being given the opportunity to generate its own creative samples [Senftleben M., 2023: 1535–1560].

Scholars have proposed a scheme for calculating and collecting remuneration. AI developers are entitled to use works for AI training purposes without a licence from the copyright holders. They are obliged to pay a fee to collective management organisations, or to similar entities, for copyright and related rights for the benefit of the entire community of authors. The fee amount should be proportional to the income of the AI developers and may be reduced by royalties paid by the developers

[14] Tylec G., Kwiecień S., Sarowski Ł et. al. Is it Possible to License Works used in the Learning Process of Artificial Intelligence Algorithms? Available at: URL: https://ssrn.com/abstract=4729495 (accessed: 07.06.2025)

under standard agreements with the rights holders. Rights holders will receive a percentage of the fee, and the organisation may determine the distribution of the fee. Research indicating which works are most frequently used by AI may also be taken into account.

In July 2025, at the request of the European Parliament's Committee on Legal Affairs, a researcher N. Lucchi has prepared a study under the title "Generative Artificial Intelligence and Copyright: Training, Creation and Regulation". In the study she has highlighted the significant differences between the intellectual analysis of texts and data and AI training. She has concluded exceptions for the intellectual analysis of texts and data are not suitable for the large-scale use of data in generative AI.

In addition N. Lucchi has pointed to the absence of uniform standards that would enable rights holders to prohibit the use of their content, as well as the lack of transparency in model training processes. In particular, she proposed the following solutions: establishing a special body to oversee the use of content in AI; developing reporting standards for developers; and creating transparent mechanisms for calculating compensation. The latter involves forming a collective rights management system for small rights holders, establishing a centralised remuneration fund and developing methods for calculating payments based on the impact of content on the model's performance, the popularity of the materials used, the volume of data usage and the profits of AI developers [Lucchi N., 2025: 12–14, 29–35, 59].

3.3. The Japanese approach

Article 30-4 of the Japanese Copyright Act[15] permits the use of a work in any manner and to the extent deemed necessary in the following cases:

1) If it is done for the purposes of testing, developing or the practical implementation of technology related to the recording of sounds or the visual effects of a work, or for other similar exploitation.

2) If it is done for the purpose of data analysis, such as the extraction, comparison, classification or other statistical analysis of the constituent

[15] Copyright Act (Act No. 48 of May 6, 1970, as amended up to January 1, 2022). Available at: URL: https://www.wipo.int/wipolex/en/legislation/details/21342 (accessed: 07.06.2025)

language, sounds, images or other elementary data from a large number of works or a large volume of other such data.

3) If it is used in computer data processing or exploited in a way that renders the work imperceptible to the human senses.

4) In any other case where the user's purpose is not to derive pleasure from the thoughts or feelings expressed in the work.

It has been established that such actions should not unreasonably prejudice the interests of copyright holders, taking into account the purpose of the work and the circumstances of its use.

Article 47-5 of the Law mentioned permits the free use of minor portions of works in connection with computer data processing and the identification of results. Together, these two provisions give to Japan the world's probably most extensive exemption for training neural networks.

Meanwhile, Japan is currently discussing the possibility of tightening regulations in this area. In May 2024 the Japanese Copyright Office has published "A General Understanding of AI and Copyright in Japan." The document states that companies could face legal action if they knowingly collect data for training purposes from sources that violate copyright. It emphasises that materials generated by AI in the style of an existing work do not infringe copyright. However, if a small group of an author's works features not only a similar style, but also identical creative elements, then deliberately reproducing such a group for additional training with the aim of generating materials that include these creative elements is considered an infringement.[16]

3.4. The US approach

Section 107 of Chapter 17, "Copyright", of the United States Code[17] establishes four criteria for determining the permissibility of using copyrighted material without the consent of the copyright holder under the fair use doctrine. The criteria are: purpose of the use; nature of the work (i.e., the level of creativity); extent and significance of the borrowing from the protected work; impact of the use on the potential market or value of the protected work [Kalyatin V.O., 2015: 40–47].

[16] Available at: URL: https://www.bunka.go.jp/english/policy/copyright/pdf/94055801_01.pdf (accessed: 07.06.2025)

[17] United States Code. Title 17 — Copyrights. United States of America (17 U.S.C., amended up to Public Law No. 117-263]. Available at: URL: https://www.wipo.int/wipolex/en/legislation/details/22356 (accessed: 07.06.2025)

The first criterion is supplemented by the doctrine of expanding utility (transformative) use at the level of judicial practice. This type of use is characterised by several features. Firstly, it is creative and transformative in nature. Secondly, it involves the creation and use of new copyrighted works, including software products, as well as the extraction of additional "usefulness" from the copyrighted works of others. This usefulness can be practical, cognitive or informational.[18]

Many US scholars assume that the use of works for AI training should be defined as "fair use." This can be classified as transformative, as it expands the usefulness of the application [Torrance A., Tomlinson B., 2023: 250–253].

As M. Sag and P. Yu have noted, the intellectual analysis of works for the purpose of obtaining metadata (i.e. abstractions that are not protected by copyright) constitutes transformative use. This meets the first criterion of fair use [Sag M., Yu P., 2025: 1175]. This use clearly meets the third criterion as well. Works used for training AI are often copied in their entirety, but only unprotected elements such as facts and ideas are subsequently extracted from them. In these authors' opinion, the use in question also meets the fourth criterion, as training AI has no significant impact on the potential market or value of the copyrighted work.

M. Lemley and B. Casey are adopting a similar stance. They argue that the reproduction of copyrighted works should generally be recognised as fair use, provided there is no intention to exploit the protected form of the work. AI developers are interested in the ideas conveyed through the expression of the copyrighted object, rather than the expression itself [Lemley M.A., Casey B., 2021: 158].

According to E. Lee, "The use of larger and more diverse data sets, or the scaling method, has led to better results in the development of working AI models and advanced the state of the art." This story demonstrates that an AI developer's use of copyrighted works to train AI models for research, development, training and improvement can constitute fair use, namely the creation of new technology for public benefit." [Lee E., 2025: 223].

The US Copyright Office in its report has noted that training generative AI models on large datasets transforms the source material into statistical

[18] This concept has been applied, in particular, in the following disputes: Authors Guild v. Google, Inc., 804 F.3d 202, 218 (2d Cir. 2015); Authors Guild, Inc. v. HathiTrust, 755 F.3d 87, 97 (2d Cir. 2014).

models capable of generating new content. However, the aim of creating original works for entertainment or educational purposes may not align with the functions of AI models. In such cases, the Office states that the use of third-party works in AI training is generally transformative in nature.

Meanwhile, the degree of transformation can vary significantly depending on how it is used. The model's most transformative use should be recognised in scientific research or closed systems with limited, non-replacement-related functions. One example is the development of a language model for learning foreign languages through communication and correction of user errors.

At the other extreme is the use of technology to create content that is virtually identical to copyrighted material. For example, a model trained on frames from an animated series can generate new characters in the same style.

Most cases fall between these two extremes. The model may use copyrighted works without producing substantially similar content. However, if the aim of the training is to produce material for the same audience, the application remains only moderately transformative.

Regarding the fourth criterion, the Office has noted that generative AI poses risks to copyright markets. The mass production of AI-generated content could replace human creative labour, particularly if the results are stylistically similar to the original works. At the same time, licensing data for AI presents issues of scale, cost and identifying rights holders.

Some American researchers suggest the best solution to this problem would be for the creative content and the AI industries to enter into agreements to establish mechanisms for paying royalties for the use of works in AI training [Feldman R., 2025: 57], or to grant developers compulsory licences to scrape works for the purposes of training AI [Opderbeck D., 2024: 35–36]. It is proposed that rights holders be granted an additional right: the "right to training." This would enable them to claim a share of the income generated from the commercialisation of neural networks trained on protected works [Pasquale F., Malone T., Ting A., 2025: 218–220].

3.5. The Chinese approach

In August 2023, the Chinese regulators have approved the "Provisional Measures for the Management of Generative Artificial Intelli-

gence Systems" (hereinafter – the Provisional Measures)[19] The document requires companies to use only "lawful data" when training AI models. According to Article 7(3) of the Provisional Measures, providers of generative AI services must not infringe any intellectual property rights. In February 2024, the National Technical Committee on Cybersecurity of the Standardisation Administration of the People's Republic of China issued the "Basic Security Requirements for Generative Artificial Intelligence Services", in addition to the aforementioned Provisional Measures. [20] In accordance with Para. 5.1(a) of the document, any data set used to train generative AI must contain no more than 5% of illegal or harmful information.

According to Para 5.1(c) (2), when using a dataset that has been collected independently, the provider is obliged to keep records of the collection process and must not collect data that the rights holders have explicitly stated cannot be collected, for example by using a robots.txt file. Those persons who use commercial datasets, in turn, must have a valid contract or cooperation agreement with the data provider, in which the latter guarantees "the source, quality and security of the data" (Para 5.1(c) (3)).[21]

In 2024 China has published a draft law on the management of artificial intelligence.[22] According to its Article 24, the use of copyrighted works by an AI developer may be considered reasonable if the following conditions are met:

The use differs from the original purpose or functions of the data.

The use does not affect the normal use of the data.

---

[19] Available at: URL: https://www.chinalawtranslate.com/en/generative-ai-interim/ (accessed: 07.06.2025)

[20] Technical Documentation of National Technical Committee 260 on Cybersecurity of Standardization Administration of China: Basic Safety Requirements for Generative Artificial Intelligence Services. Available at: URL: https://cset.georgetown.edu/publication/china-safety-requirements-for-generative-ai-final/ (accessed: 07.06.2025)

[21] Intellectual Property and Artificial Intelligence Training: Transformation of the Modern Legal Landscape in Different Countries around the World: analytical review prepared by the All-Russian public-state Russian Centre for the Circulation of Rights to Creative Activity Results. Available at: URL: https://рцис.рф/storage/uploads/2025/06/05/analiticheskii-obzor-is-ii_uid_6841b77cd425d.pdf (accessed: 07.06.2025)

[22] Artificial Intelligence Law of the People's Republic of China (Draft for Suggestions from Scholars). Available at: URL: https://cset.georgetown.edu/wp-content/uploads/t0592_china_ai_law_draft_EN.pdf (accessed: 07.06.2025)

The use does not unreasonably prejudice the legitimate rights and interests of the copyright holder.

If these criteria are met, the AI developer is not required to pay remuneration to the data owner or obtain their permission to use the work. Clearly, this article mirrors the three-factor test set out in Article 9(2) of the Berne Convention and Article 13 of the Trade-Related Aspects of Intellectual Property Rights Agreement of 15 April 1994.[23]

At the end of 2025, it has emerged that China had abandoned plans to develop comprehensive AI governance legislation.

While the aforementioned documents did not allow for a general exemption from the exclusive rights of AI developers, experts claim that China imposes minimal restrictions on the use of data for AI training. This enables companies in the AI sector to grow rapidly without facing legal obstacles [Murray M., 2025: 27].

4. Law Enforcement Practice

So far, no legal system has developed consistent law enforcement practices or clear, uniform approaches to handling cases related to AI training. Meanwhile, there are a number of interesting cases. Firstly, it is useful to consider US case law.

In one case, Ross Intelligence, the defendant,[24] used Thomson Reuters' extensive database of legal texts and documents (Westlaw) to train an AI system without a licence. This AI was subsequently used to create a legal content search system. The court has concluded that the defendant's actions could not be considered fair use in the case because the using was commercial rather than transformative one and affected the value and potential market for the plaintiff's work. It was also established that Ross Intelligence had copied 2,243 annotations to Westlaw. These annotations were original enough to meet copyright protection requirements. However, the use of this content was deemed commercial and not transformative one in nature. The court has concluded that the defendant's actions harmed the Westlaw content market because the

[23] Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), concluded in Marrakesh on 15 April 1994 (as amended on 06 December 2005) // Code of Laws of the Russian Federation. 2012. No. 37 (Annex, Part VI). Pp. 2818–2849.

[24] Thomson Reuters Enterprise Centre GmbH et al v. ROSS Intelligence Inc., No. 1:2020cv00613-SB — Document 770 (D. Del. 2025).

defendant used the content to create a competing product. In this case, the issue was not training generative AI, but rather the direct transfer of elements from the plaintiff's database.

Also the court has noted that using materials for AI training purposes should not automatically be considered copyright infringement, provided it is not done with the intention of direct copying.

In the case of Bartz v. Anthropic,[25] three authors have filed a lawsuit against Anthropic for using their books to train the Claude language model. The company obtained the materials in two ways: 1) by legally purchasing and digitising paper books, and 2) by downloading more than seven million books from pirate sources. The court has recognised AI training based on digitised books as lawful transformative use. It took into account that the model was trained to reproduce human patterns and that new text-processing functionality was being created. However, the use of pirated copies was recognised as a violation of exclusive rights, as legal sources were available, and their use was not "reasonably necessary."

In the case of Kadrey v. Meta[26] Platforms, [27] a group of authors sued Meta Platforms for using their works to train the Llama language model without permission. The plaintiffs claimed that the defendant had trained its model using materials from shadow libraries such as Library Genesis, Anna's Archive and Z-Library.

The court ruled in favour of Meta, recognising the use of the materials as both transformative and fair. However, the court in the same time has noted that AI could, in theory, influence traditional markets and reduce incentives for human creativity. Therefore, actions of these sort may be deemed unlawful in the future if there is evidence of harm to the market. In this case, however, the plaintiffs did not present evidence of a negative market impact. Materials from shadow libraries should not be used to support the defendant if such downloading facilitates unauthorised copying. Nevertheless, the plaintiffs did not provide evidence of this.

The following two cases are of interest in terms of German judicial practice. The first is the case of Robert Kneschke v LAION [28] concern-

[25] Bartz v. Anthropic (Case No. 3:24-cv-05417, N.D. Cal.)

[26] Meta is recognised as extremist and banned in Russia.

[27] Kadrey v. Meta Platforms, Inc., No. 3:23-cv-03417-VC, 2025 WL 4123456 (N.D. Cal. June 25, 2025).

[28] Robert Kneschke v. LAION e.V., Case No. 310 O 227/23.

ing the creation of datasets for AI training. Kneschke, a German photographer, has discovered that LAION had used his photographs in the creation of the LAION-5B dataset with the help of a special application. LAION worked with the Common Crawl dataset, which contains 5.85 billion image-text pairs. The organisation downloaded images from links, analysed the accuracy of the descriptions and filtered out any mismatched pairs before creating a free dataset for AI training.

The court has ruled that LAION's actions were lawful under Section 60d of the German Copyright Act.[29] The main arguments for this decision were as follows: Firstly, creating a dataset for AI training is considered scientific research. LAION did not pursue commercial goals by providing the data free of charge. Using the photographs did not prevent the claimant from using their works as intended. A key aspect of the decision was the court's confirmation that copyright exceptions apply not only to the direct training of neural networks, but also to the process of creating training datasets. In this case, the defendants must prove that the database created will be used exclusively for AI training purposes.

In the case of GEMA v. Open AI,[30] the German music rights management society GEMA filed a copyright infringement lawsuit against OpenAI concerning musical works. The plaintiff claimed that ChatGPT-4 had memorised the lyrics of at least nine well-known German songs and could reproduce them almost verbatim.

GEMA lawyers have conducted an experiment: first, they programmed a neural network to reproduce song lyrics. Then, they disabled the web search function to prevent the network from obtaining information from the Internet. Simple requests were then sent, such as: "What are the lyrics to a song with such-and-such a title?" and "What is the chorus to this song?" In response, ChatGPT-4 provided substantial sections of real lyrics, occasionally supplementing them with fictional lines.

Open AI has rejected the claims, stating that users had independently removed the neural network from cautious behaviour mode. The company also insisted that its models do not store specific data, and that text generation depends on user prompts are beyond its control.

---

[29] Act on Copyright and Related Rights (Urheberrechtsgesetz — UrhG) of 9 September 1965, as last amended by Article 28 of the Act of 23 October 2024 Available at: URL: https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html (accessed: 07.06.2025)

[30] GEMA v. Open AI / Higher Regional Court of Munich — I 42 O 14139/24.

However, the court has ruled in favour of the claimant, awarding damages and prohibiting the unauthorised use of others' works. According to the court, including texts in the teaching corpus and subsequently memorising them constitutes the reproduction of others' works. The results showed that texts are stored within the model like a digital library: training data is embedded in the model weights and remains accessible for retrieval. The court has compared this to MP3 compression: while the model does not literally store texts, it can recreate them in a recognisable way. The defendant's references to TDM were rejected. Memorising song lyrics was recognised as direct copying rather than data analysis.

In 2023, Getty Images filed a lawsuit against Stability AI[31] in the United Kingdom for allegedly using millions of copyrighted images to train the Stable Diffusion image generation model. The plaintiff demanded a prohibition on training AI models using copyrighted material without compensation, and sought recognition of violations of copyright, trademark and database rights.

During the proceedings the court has found that Stability AI had infringed Getty Images' trademark rights by generating images with the company's watermarks. However, the court has rejected the claim of secondary copyright infringement relating to the import of counterfeit material (Stable Diffusion software) into the UK, ruling that Stable Diffusion does not store or reproduce copyrighted works. The judge has noted that, while the model weights change during training under the influence of copyrighted works from Getty Assets, the weights themselves are not a counterfeit copy, nor do they store or reproduce one. By the end of the training process, the model does not retain any copyrighted works from Getty Images. Nevertheless, Getty Images has withdrew its main claims regarding the initial copyright infringement during the model's training due to difficulties in gathering evidence, given that Stable Diffusion was trained and developed in the United Kingdom.

An interesting case has emerged in Chinese law enforcement practice involving a lawsuit filed by Shanghai Xinchuanghua Cultural Development Corporation, the exclusive licensee of the Ultraman character in the PRC. The defendant was an AI company that provided a drawing feature for community members via its website. This service was provided by a third-party supplier.

[31] Getty Images v Stability AI (2025) EWHC 2863 (Ch).

The court has analysed the distinctive features of Ultraman in detail, including the "symmetrical diamond-shaped protrusion resembling a fin in the middle of the forehead» and the «huge egg-shaped eyes that protrude outwards". The court ruling found substantial similarities between the generated images and the original character in several key features.[32] The court has found that the defendant's actions violated the plaintiff's exclusive copyright of the work. The defendant was ordered to stop generating Ultraman images using keyword filtering and to pay the plaintiff damages of 10,000 yuan (rather than the 300,000 yuan claimed). However, the plaintiff's request to remove materials featuring Ultraman from the training dataset was not granted. In its ruling, the court emphasised that "AI is a strategic technology that will shape the future, driving a new phase of scientific and technological revolution and industrial transformation" [Foong C., 2025: 15–17].

Based on the decisions reviewed above, we have reasons to conclude that foreign courts generally recognise the lawful use of third-party works for training neural networks, provided the generated output does not reproduce substantial parts of the works. At the same time, however, the courts' views have diverged on certain aspects of cases. Nevertheless, some questions remain unanswered. In particular: what specific works can developers use; how should their access to the database of relevant works be formalised; and is the use of counterfeit copies permissible? How should right holders demonstrate the impact that such use has on the potential market or value of the protected work? The following section of the article provides answers to these questions and sets out recommendations for the Russian legal system.

5. Analysis of Key Issues and Proposals

The Russian Federation Civil Code should allow for the free use of third-party copyrighted material for training neural networks (including data collection activities). However, upon analysing the technical aspects of AI training, foreign experience and judicial practice, a number of questions arise regarding the establishment and application of such an exemption.

[32] Shanghai Xinchuanghua Cultural Development Co, Ltd v AI Company (pseudonym) (2024) Yue 0192 Min Chu No. 113 (Guangzhou Internet Court, 8 February 2024).

a) What specific uses should be considered permissible?

Examples of free use should include using works as part of an intellectual analysis of digital texts and data to obtain information, including regularities, patterns, trends and correlations, for the purpose of training neural networks. This should be permitted provided that the form of the works is not perceived by the human senses as a result of computer processing of the data. This exemption should not apply only to non-profit organisations or non-commercial use, as this would create artificial barriers to the development of AI technologies.

Such restrictions on exclusive rights comply with the three-step test, which is enshrined in both international law[33] and national legislation (Para 5 of Art. 1229 of the Russian Federation Civil Code). First and foremost, using works to train neural networks will not conflict with the normal use of works, except in the cases described below.

Some clarification is needed here. Clearly, any instance of free use of a work prevents the copyright holder from commercialising it in an appropriate manner. Therefore, if Article 1274 of the Civil Code did not exist, rights holders could grant licences to anyone who wanted to quote their work or create a parody. However, this does not mean that such cases of free use are contrary to lawful use of the work.

When assessing the admissibility of a restriction on an exclusive right, it is necessary to determine its impact on the use that results in the right holder receiving income that is proportionate to that received from other methods of use. i.e., the main methods of commercialising works. Use is considered contrary to the normal exploitation of the copyright object if it competes with the typical way in which right holders usually derive economic value from their exclusive rights or if it deprives right holders of significant or appreciable commercial advantage.

Works of science, literature and fine arts serve to aesthetic and cognitive functions of human community and individuals. Typically, they create new "access points" for the public to such works, catering to aesthetic and/or epistemological needs. For literary works, the main mechanism is publication, and in some cases, film adaptations. Meanwhile, neural networks are trained through the 'non-expressive' use of

[33] See: Article 9(2) of the Berne Convention for the Protection of Literary and Artistic Works; Article 13 of the Agreement on Trade-Related Aspects of Intellectual Property Rights; Article 5(5) of EU Directive 2001.

works. AI deconstructs millions of works, transforming them into non-expressive statistical data, in order to create entirely new expressive and generative capabilities that are functionally distinct from the original data [Murray M., 2025: 22]. This cannot be considered a standard way of commercialising the works in question.

Generally speaking, there can be no question of unjustified infringement of the legitimate interests of the copyright holder when it comes to AI training. Such use does not provide the public with alternative "points of access" to the work.

One might argue that neuroart is displacing traditional artists from the market, particularly in the visual arts. Nevertheless, today human creativity is more valuable than ever in the past. This is because writers and artists can convey their emotions, feelings and experiences through their work, examine social and political issues, and suggest ways for society to develop. Neural networks lack these capabilities, meaning AI creativity cannot replace serious literature and painting. However, works with a low level of creativity, such as advertising texts, media articles and unoriginal images, already have a narrower scope of exclusive rights than works with a high level of creativity. Parallel creativity is possible for such works.

From the point of public interests, functions and objectives of the copyright system, violation of the interests of rights holders in the case of AI training cannot in any case be considered unjustified. AI technologies are necessary for solving global problems in industry, healthcare and education. Even if a neural network only generates aesthetically appealing images, texts and music, it still serves society's interests by satisfying aesthetic gnoseological needs.

The development of AI technologies may encourage traditional authors to produce more creative works. For instance, using neural networks to generate short news items could prompt publishers and journalists to produce more analytical content.

b) Should the use of works for AI training be a subject to payment, as proposed by many European researchers?

The answer is no. For objective reasons, AI developers will not be able to identify the copyright holders of all the works used, negotiate with them and conclude licence agreements. Scholars have proposed a scheme whereby a third party would collect remuneration and redistribute it to authors. We do not consider this to be a successful solution.

The problem is the following one: there are no transparent algorithms for distributing income that could prevent abuse in this case, and there never will be. This is confirmed by developers, who note that it is fundamentally impossible to identify all the works used in AI training. Therefore, the decision to pay a percentage would always be arbitrary and subjective.

In this approach, the right to remuneration takes the place of the author's exclusive right, which is the ability to prohibit others from using the work. In such cases, the functions of the right to remuneration should generally coincide with those of exclusive rights. A key function of exclusive rights is to encourage market participants to create and commercialise new works. However, it is unlikely that the vague prospect of receiving an unspecified percentage from a third party at some point in the future would provide an additional incentive for market participants to invest in creating and commercialising new works. At the same time, the requirement to pay this fee could result in companies reducing investment in new AI developments and increasing licence fees for AI users.

c) What materials may be used to train AI?

The restriction of exclusive rights under consideration should not apply only to the use of digital versions of legally acquired books. Otherwise, neural network developers will face problems comparable to those encountered in licensing. They will need to find sellers of paper copies, place an order, arrange delivery, digitise the material and then destroy the paper copies.

Developers of neural networks must have access to digital versions of works. Above all, this should apply to any works lawfully posted on the internet, regardless of whether the rights holders have explicitly consented to their works being used to train AI. Examples include academic articles that are freely available on journal websites or in open publication databases where authors publish their own work.

The situation is becoming more complicated when it comes to shadow libraries, pirated resources and any other materials that have been posted illegally on the internet. In any case, works posted online should not be excluded from the proposed exemption if AI developers did not and could not have known that the copies were pirated. After all, neural network developers and trainers cannot be expected to process every uploaded work manually. Accordingly, they will not be able to determine whether most works available on the internet were posted with the consent of the copyright holder.

Enacting legislation stipulating that the copyright exemption in question applies only to lawfully posted materials (assuming that this condition will be complied with by participants in the market) will significantly complicate the process of training neural networks and, in essence, negate the positive results of establishing the exemption in question.

The case for the free use of works should probably not apply to the deliberate choice by neural network developers of pirated databases, provided such use benefits the operators and owners of the databases (e.g. through access fees or additional advertising). This would encourage market participants to create pirate databases, which would make it more difficult for rights holders to commercialise their works.

Indeed, counterarguments may be offered here. Training a neural network based on shadow libraries and other pirated databases does not in itself publicise these sources. Users only see the generated result, not the links to the training material. In most cases, AI developers will not contribute to replacing legally placed copies with pirated versions, thereby drawing readers or viewers away from the websites and other resources of rights holders. Even when considering the responsibility of developers, it will often be indirect (for reproducing works when training the model) rather than direct, and secondary (for enabling violations of exclusive rights by the creators of shadow libraries).

Furthermore, the exemption in question should not apply to works for which rights holders have implemented technical protection measures. If rights holders use pirated databases to circumvent these measures, this should be considered illegal.

Thus, works that are publicly available on the internet, as well as those in closed databases to which developers have lawful access via a licence or subscription, may be used to train neural networks. Provided that their actions do not lead to the creation of new (additional) "access points" for potential readers and viewers, developers should be allowed to digitise paper versions of works for the purpose of training AI.

d) What actions by AI developers should not fall under the case of free use under consideration?

That exception should not apply when the neural network generates content that substantially reproduces protected works. Such use should be classified as an infringement of exclusive rights. Generating a work in an author's style by training a neural network on their works may also be recognised as an infringement.

As a rule, "borrowing stylistic features" does not lead to the creation of a derivative work. For example, artists can paint pictures in the same style and use the same techniques. They may even depict similar subjects and objects in their drawings. In doing so, they will not infringe each other's exclusive rights.

The situation is different with works generated by AI. Not only may the result borrow someone else's style, but it may also reproduce elements from an artist's multiple paintings, such as their characteristic brushstrokes and lines. As a result, significant parts of the work may be missing, such as the image of a person, a house or a river from someone else's painting.

Even when an artist imitates the style of a predecessor, they still create a unique piece of artwork. Conversely, AI technologies essentially recreate the "hand of the author — a famous artist" for users (in whose style the painting is to be created). The form of the derivative work reflects the artist's techniques, brushstrokes, colour choices, and so on.

The development of neural networks has led to new processing methods emerging: the creation of derivative works based on a multitude of an author's works, but without reproducing their essential elements, instead borrowing a significant number of non-essential ones.

Depending on the circumstances, liability for such violations should be borne by either the AI developer, the user, or both. Various cases are possible.

Case No. 1: The neural network developer trained the model specifically based on a limited list of works (e.g. author, copyright holder, series of works). Even when receiving a neutral user prompt, the neural network will create images or texts based on such works, using their essential parts. Clearly, in this case, the neural network developer is responsible for reproduction, processing and dissemination to the general public. Therefore, the demonstration of a work (or part of a work) on the computer screen using the corresponding neural network should be attributed to the developer, not the user who submitted the prompt.

In such cases, users shall only be liable for the subsequent reproduction, distribution or disclosure of the generated content. Even if it is clear from the circumstances that the user could not have established the use of third-party works in the content, *de lege ferenda*, they should be held liable on a no-fault basis (regardless of whether they are engaged in entrepreneurial activity), in the same way as owners of sources of increased

danger. When using a neural network to generate images and texts, users must assume the risks associated with infringing the copyright of others. Like sources of enhanced hazard, neural networks have properties that make their use potentially dangerous to the copyright of others.

Case No. 2: The user has achieved the creation of a derivative work containing elements of the protected work by sending special requests regarding the author's works, references and additional training to the neural network. During normal use, however, the neural network does not include parts of other people's works in the generated content. In such cases, the user should primarily be held liable. The AI developer may be liable as an accessory to the infringement, provided that they did not specifically prohibit the reproduction of protected works or parts thereof, did not implement adequate technical measures to prevent memorisation of works, and did not respond promptly to a claim from the copyright holder.

In the absence of a generated result reflecting the memorised copy, the potential "memorisation" of training materials by a neural network during the training process should not yet be considered a copyright infringement. As E. Lee notes, internal memorisation does not replace original works without infringing copyright [Lee E., 2025: 208].

6. Are Exclusive Copyrights Infringed upon when using RAG Technology?

The answer depends on the result generated by the neural network. If the neural network's response to the user includes only unprotected ideas from a third-party source (e.g. a website) and does not reproduce phrases verbatim, this cannot be considered a violation. This exception should apply to such practices. However, if the answer contains separate phrases from the source in question, it is necessary to determine the volume of the reproduced text and whether a reference to the original source was included. Provided the conditions set out in Article 1274 of the Russian Federation Civil Code are met, such use shall be classified as a lawful quotation. Otherwise, it would be considered a violation of exclusive rights.

Conclusion

It is urgent that a new method of free use is stipulated in the Civil Code of the Russian Federation for works used for text and data analysis

purposes in the training of neural networks, including by commercial organisations. This exemption should cover the stages of collecting and summarising relevant data, as well as the direct training of the neural network. This restriction of exclusive rights is in line with the principle of balancing private and public interests, and meets the three-step test.

Neural networks may be trained using publicly available Internet works, closed databases to which developers have access based on a licence or subscription, and digitised paper versions of works, provided this does not create new 'access points' for potential readers/viewers.

However, such an exemption should not apply to the generation of content that reproduces substantial parts of protected works, the targeted training of AI on the works of a specific author in order to create a work in their style, or the use of works to circumvent technical measures established by the copyright holder to protect against scraping.

References

1. Dermawan A. (2023) Text and Data Mining Exceptions in the Development of Generative AI Models: What the EU Member States Could Learn from the Japanese 'Non-Enjoyment' Purposes? *Journal of World Intellectual Property,* vol. 27, no. 1, pp. 44–68.

2. Feldman R. (2025) AI versus IP. Rewriting Creativity. Cambridge: Cambridge University Press, 217 p.

3. Foong C. (2025) GenAI Models and Copyright Infringement: Doctrinal Challenges and Regulatory Gap-Filling Using Unfair Competition Principles. *University of New South Wales Law Journal,* vol. 48, no. 4, pp. 70–96. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5327096

4. Hellwig F. (2013) Change in Copyright Law as a Market Intervention to Realize the Welfare Potential of Text Mining in Scientific Research. Leipzig: University of Applied Sciences, 91 p.

5. Kalyatin V.O. (2015) Prospects of Applying the Doctrine of Fair Use in Russia. *Zakon*=Law, no. 11, pp. 40–47 (in Russ.)

6. Lee E. (2025) Fair Use and the Origin of AI Training. *Houston Law Review*, vol. 63, pp. 101–223.

7. Lemley M.A., Casey B. (2021) Fair Learning. *Texas Law Review*, vol. 99, pp. 101–181.

8. Lucchi N. (2025) Generative AI and Copyright. Training, Creation, Regulation. Tilburg: University Press, 173 p. URL: https://www.europarl.europa.eu/thinktank/en/document/IUST_STU(2025)774095

9. Lukas A.J. (2023) Generative Artificial Intelligence under German Copyright Law. Part 1, pp. 1–12. Available at: SSRN: URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4635645, DOI:10.13140/RG.2.2.12823.34724

10. Murray M. (2025) AI Training is Fair Use: The Beginning of the End of the Copyright Assault on Gen AI. 2025, pp. 22–27.

11. Opderbeck D. (2024) Copyright in AI Training Data: A Human-Centered Approach. Newark (N.J.): Seton Hall Law School Legal Studies Research, 52 p. Available at: http://dx.doi.org/10.2139/ssrn.4679299

12. Pasquale F., Malone T., Ting A. (2025) Copyright, Learnright, and Fair Use: Rethinking Compensation for AI Model Training. *Northwestern Journal of Technology and Intellectual Property,* vol. 23, issue 1, pp. 205–226.

13. Sag M., Yu P. (2025) The Globalization of Copyright Exceptions for AI Training. *Emory Law Journal*, vol. 74, pp. 1163–1227.

14. Senftleben M. (2022) Compliance of National TDM Rules with International Copyright Law: An Overrated Nonissue. *International Review of Intellectual Property and Competition Law,* no. 10, pp. 1477–1505.

15. Senftleben M. (2023) Generative AI and Author Remuneration International.

Review of Intellectual Property and Competition Law, vol. 54, no. 10, pp. 1535–1560.DOI:10.2139/ssrn.4478370

16. Torrance A., Tomlinson B. (2023) Training is Everything: Artificial Intelligence, Copyright, and "Fair Training". *Dickinson Law Review*, vol. 128, pp. 233–255.

17. Tylec G., Kwiecień S. et al. (2024) Is it Possible to License Works Used in the Learning Process of Artificial Intelligence Algorithms? SSRN: URL: https://ssrn.com/abstract=4729495

Information about the author:

A.S. Vorozhevich — Doctor of Sciences (Law), Associate Professor.

The article was submitted to editorial office 11.01.2026; approved after reviewing 23.02.2026; accepted for publication 23.02.2026.

Legal Issues in the Digital Age. 2026. Vol. 7, no. 1.
Вопросы права в цифровую эпоху. 2026. Том 7. № 1.

Research article
JEL: K14
UDC: 347
DOI:10.17323/2713-2749.2026.1.32.48

Replacing Criterion of Creativity with Criterion of Investment for Results Created by Artificial Intelligence

Pavel K. Pakshin

National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Russia,

ppk-center@mail.ru, https://orcid.org/0009-0006-2829-0267

Abstract

Artificial intelligence plays a significant role in automation, minimizing human intervention in fields such as medicine, art, and law. Despite the historically close relationship between art and technology, generative AI has expanded the potential for creative activity. A sufficient catalyst for this process has been the proliferation of pre-trained AI systems, that have accelerated development of technologies in natural language processing and visual content generation. The development of artificial intelligence determines a revision of established doctrinal approaches in intellectual property. The study aims to provide a justification for the legal protection of results generated using artificial intelligence. The key legal risk in the field is the lack of legal grounds for granting protection to such results under *de lege lata* regulation. Current "silence" of the legislator regarding objects created by artificial intelligence exacerbates the issue of legal uncertainty. At the same time, there is a significant risk that artificial intelligence itself will infringe the exclusive rights of third parties. Beyond intellectual property rights, objects created by artificial intelligence, may be unreliable and misleading, as well as violate personal data laws. These challenges highlight the need to adapt legal frameworks to new digital realities. The relevance of the study stems from the dilemma facing legislators: to recognize artificial intelligence as *sui generis* legal personality or to modify the protection mechanism by shifting creativity criterion within copyright law to an investment criterion within related law. The aim of the research is to resolve this dichotomy. The methodological basis of the work

is based on comparative legal and formal logical methods. The scholar novelty lies in the comprehensive analysis of the hypothesis regarding the transition from the creativity criterion to the investment criterion. The article demonstrates that modifying the copyright protection mechanism by shifting the creativity criterion within copyright law to the investment criterion within related rights represents the most preferable vector of legal policy.

Keywords

intellectual property; intellectual rights; artificial intelligence; neural network; machine learning; results of intellectual property.

For citation: Pakshin P.K. (2026) Replacing Criterion of Creativity with Criterion of Investment for Results Created by Artificial Intelligence. *Legal Issues in the Digital Age*, vol. 7, no. 1, pp. 32–48. DOI:10.17323/2713-2749.2026.1.32.48

Introduction

The article examines several issues arising from the development of generative artificial intelligence (AI), namely, its classification as a subject or object of law, the establishment of copyright ownership for results generated using AI, and the differentiation of liability for legally significant actions performed by it. The key problem lies in integrating AI-generated results into a legal framework that has historically been based on an anthropocentric foundation.

It is important to distinguish between results created by human creativity using AI as a tool and results created autonomously by AI without human creative involvement. In the former instance, it has a sense to speak of results of intellectual activity as defined in Article 1225 of the Civil Code of the Russian Federation (hereinafter — the Civil Code). In the latter case, the results are generated by AI without any "creative activity." If appropriate amendments are made to Article 1225, such results could be equated with the product of intellectual activity[1].

[1] E.g., the means used to differentiate legal entities, goods, works, services and enterprises are entitled to appropriate legal protection are equated with the results of intellectual activity. To establish a similar legal regime for results created autonomously by AI , without human creative involvement, legislation will need to be amended to include a provision equating such results with the results of intellectual activity.

In the context of generating new ideas, it is seeing clearly a steady growth in the number of intellectual property creators who are harnessing the potential of digital technologies. Since AI systems operate on large amounts of data, some of that may be from sources that are not transparent to the user, rights holders are adopting the legitimate strategy of using the AI-generated results solely as a source of inspiration for independent creative processes.

Current AI developments present legislators in front of the need to choose between two different approaches: recognising AI has legal personality *sui generis*, or modifying the traditional IP asset protectability mechanism by replacing copyright law's creative character criterion with the investment criterion in related rights.

The idea behind this approach is the legal regime established for investment databases as objects of related rights will be applied by analogy. The content component of the investment criterion implies the need to determine the materiality of costs (including financial and organisational resources), and professional competencies within the framework of parameters such as the duration, intensity, number of stages, and the scale of work.

Notably, in the case of investment databases, compliance with the investment criterion is based on presumption. Paragraph 1 of Article 1334 of the Civil Code states: "In the absence of evidence to the contrary, a database containing at least ten thousand independent items of information (materials) constituting the content of thereof, shall be recognised as a database whose creation requires substantial investment." Instead the criterion of "ten thousand independent information elements (materials), it would be advisable to apply a criterion of distinguishability of the AI-generated result from typical texts and stock images stored in publicly available databases to the results generated by AI.[2]

Advancements in digital technology have exacerbated the issue of revising established anthropocentric paradigm, that viewed creativity as an exclusively human prerogative. Author of the paper proposes a hypothesis replacing the creativity criterion with the investment criterion does not undermine the intellectual property rights system, while offering an optimal regulatory solution under current legislation.

[2] This criterion is based on the assumption that if an AI-generated result differs significantly from a typical text or stock image, it is the result of a detailed query (prompt).

In other words, applying the investment criterion instead of the traditional creativity criterion, based on an analogy with the protection of investment databases by related rights, implies legal protection of the AI-generated results based on proof of significant financial, time, and organisational expenditure. In the author's opinion, this approach offers the most preferable solution from the perspective of current law, with reservation: since its application does not violate the established system of intellectual property rights.

1. Creative Ability of AI

The ability of AI to produce creative results has sparked sufficient interest among researchers. Currently, if such results are obtained without human creative involvement, it is not possible to guarantee their legal protectability. Judicial practice consistently demonstrates that, even when AI is used only as a tool, a necessary condition for legal protection is proving a person's substantial creative contribution to the process of creating intellectual property.[3]

S.A. Milyukov agrees with A.I. Balashova's view that potential legal regulation could be based on the legal regimes for works without an author, works that have lapsed into public domain, and works made public by a publisher [Balashova A.I., 2023: 190]. He concludes potential legal regulation could be based on the legal regime for unprotected copyrighted works and that this legal regime is special. S.A. Milyukov proposes classifying AI-generated objects under related rights and argues persons using AI should have related rights to AI-generated objects where the

[3] For example, in its sentence on case no. A40-200471/2023 of 30 November 2023 the Moscow Arbitration Court recognised the creative contribution of a team of authors to the production of video content using deepfake technology because the use of deepfake technology does not negate the creative nature of the activities related to developing the script, producing the films and creating the soundtrack. Available at: URL: https://kad.arbitr.ru/Document/Pdf/4d7f0305-69af-44fe-8841-a59e84aa7deb/8dedc372-21f6-4751-ab3c-8a320fe435ce/A40-200471-2023_20231130_Reshenija_i_postanovlenija.pdf?isAddStamp=True(accessed: 03.11.2025). In 2023, the Beijing Internet Court, in the case of *Li Yunkai v Liu Yuanchun* (Beijing Internet Court Civil Sentence Jing 0491 Min Chu No. 11279) extended the legal regime of intellectual property to AI-generated images, while maintaining the traditional anthropocentric paradigm of legal regulation. Available at: URL: https://english.bjinternetcourt.gov.cn/pdf/BeijingInternetCourtCivilJudgment112792023.pdf (accessed: 02.11.2025)

external form of such objects was created by AI implementing the user's intention [Milyukov S.A., 2023: 63].

V.O. Kalyatin notes in this regard: "Attempting to recognise [artificial intelligence] as an author does not comply with the principles of copyright law, <...> it is much more logical to speak not about copyright, but of a narrower related right, of granting rights to the organiser of the process of creating an object, similar to the rights of the producer of a phonogram, an organisation of over-the-air or cable broadcasting, etc. <...> The role of the organiser in creating an intellectual activity is becoming decisive and, from a social perspective, worthy of encouragement. <...> Perhaps it would be easier to introduce an independent protection regime under related rights without linking it to the status of the author" [Kalyatin V.O., 2022: 44].

One must agree the most methodologically sound approach is to equate objects created using AI with the category of related rights objects. Despite the key role of developers' intellectual contribution in the process of AI creation, objects cannot be created using AI due to a lack of financial and organisational investment. The point of view on assigning a related right to the person initiating and organising the AI process appears to be well-founded. In the opinion of the author of the article, this mechanism would protect the investment and organisational resources used to create the result, rather than the creative component of the result itself.

Thus, despite the increasingly creative potential of AI, the law does not offer legal protection for results that are generated directly. The ability to prove human creative participation is still essential for the appearance of protectability.

2. The Prerogative of Anthropocentric Authorship

The results of intellectual activity are among the items of civil rights listed in Article 128 of the Civil Code. Another article of the Civil Code, namely 1228 one, states: the person whose creative work produces such results is the author. The above mentioned legislative provisions raise a number of legal issues. These include: (a) whether AI can be recognised the creator of a protected result; and (b) who is liable for intellectual property rights violations related to the use of AI.

According to S.A. Milyukov, there are two approaches to defining a work: 1) the result of mental activity; and 2) a totality of thoughts, ideas, and images that have an internal structure, form, and content

[Milyukov S.A., 2023: 73]. G.U. Lukina and E.Yu. Kuprina define the existence of an idea in the creator's mind, prior to its expression in an objective form, as a "concept" — a creative stage that precedes the fixation of the work [Lukina G.U., Kuprina E.Yu., 2023: 13].

The concept of "creativity" is inseparable from the concept of "originality." When analysing legislation of different legal systems, researchers have identified the following approaches to defining the concept of "originality":

— in the European Union (EU), intellectual property rights apply only to works that are the result of the author's own intellectual creativity[4];

— in Canada, to independent works that draw on the author's own skills and judgements;

— in the United Kingdom, to works created through the author's own knowledge, efforts, judgements and labour [Ogorodnikova K.S., 2021: 61]).

— in the United States, the minimum "creative spark" or "drop of creativity" must be produced through the author's own independent work.[5]

Thus, only a person whose creative work produced the protected result is recognised as an author. This legal principle once again raises a whole host of questions in the context of AI application, such as whether AI can be recognised as the creator of an intellectual product and how to identify the party liable for violating the exclusive rights. For now, how-

[4] In the *Infopaq International A/S v. Danske Dagblades Forening* case (Court of Justice (Fourth Chamber) [2009]), which concerned the legal regime for reviews of periodicals, the court ruled that granting legal protection to objects in the capacity of works implies establishing their compliance with the criterion of the author's own intellectual creativity. The court found that the author's own intellectual creation is confirmed by such objective elements of the work as its form, the method of presenting content and the specificity of the linguistic expression. Available at: URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008CJ0005:EN:HTML (accessed: 02.11.2025)

[5] According to the ruling in *Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc.* (499 U.S. 340 [1991]), a work must possess a minimum degree of creative individuality, or a "creative spark", to be recognised as copyrightable. The argument presented in support of this view is as follows: e.g., two poets acting independently of one another have create identical poetic works. In this case, each work is recognised as the original result of independent creative work and is therefore protectable. Available at: URL: https://tile.loc.gov/storage-services/service/ll/usrep/usrep499/usrep499340/usrep499340.pdf (accessed: 02.11.2025)

ever, results generated by AI without direct human creative involvement are excluded from the scope of legal protection.

3. On Assigning Artificial Intelligence with Legal Personality

The inability of IT systems to make creative choices becomes a reason for raising one more question: how to objectively determine the minimum level of creativity required. The legal uncertainties around the protectability criteria of AI-generated results necessitate consideration of the following significant questions:

— is it permissible to create works that imitate the individual style of a specific copyright holder?

— how can the originality of adaptations and compilations synthesised from existing protected works be assessed, and how can they be distinguished from acts of plagiarism?

— how can the scope of intellectual property holders of rights for AI-generated results be established?

To test the hypothesis that AI is functionally equivalent to a conventional subject of law, it has a sense to consider a situation in which a user delegates tasks to AI in its capacity as a contractor, similar to the relationship under a work for hire or a copyright contract. In this case, the individual's creative contribution is limited to the initial stage of formulating the technical specifications, with a direct correlation established between the degree of detail in these instructions and the likelihood that the authorship will be attributed to the individual. Therefore, the inverse relationship manifests itself in situations where tasks are minimally specified, and AI operates with a high degree of autonomy.

Following the emergence of a legal personality for legal entities, a new category has been proposed for promising developments in the field of "strong" AI, namely, an "electronic personality" capable of encompassing complex autonomous systems. In this regard researchers have considered introducing a limited legal personality *sui generis* for the relevant systems based on legal fiction, by analogy with the concept of a legal entity. However, this approach is problematic, because it would lead to unjustified expansion of the system of legal categories. The concept did not receive widespread support; the European Parliament has stated it was inappropriate to grant AI legal entity status, arguing that this would have a negative impact on promoting human creativity.

Most modern legal systems take a similar position on the inadmissibility of granting legal personality to AI. AI is not granted legal personality in the current legal systems of most jurisdictions. Its functionality is primarily defined as that of a tool capable of analysing large amounts of information.

When processing data, AI systems demonstrate imitation of rational behaviour by formulating logically sound conclusions based on input parameters, established algorithms, and pre-set rules. However, there remains a legal risk that interested parties may be deprived of adequate legal remedies.[6]

A central issue is the legal uncertainty surrounding the criteria for protecting the results generated by AI. IT systems are unable to make creative choices. This makes it quite difficult to qualify the minimum necessary level of creativity, that has legal consequences for establishing of the originality of works, distinguishing them from plagiarism, and determining authorship.

Most legal systems reject the concept of granting AI legal personality, citing the need to preserve incentives for human creativity. But in the absence of a special legal regime there is a risk that it would be impossible to protect results that are objectively identical to the results of human intellectual activity.

Therefore now it makes a sense to look for solutions these problems in current legal framework, since AI systems have not yet become autonomous enough to completely break with human activity.

4. Casual Approach to Determining Level of Protection of a Work Depending on the Degree of Creative Contribution of the Individual

The anthropocentric approach to intellectual property as a whole is largely enshrined in the EU *acquis communautaire* and the intellectual

[6] In *IceTV Pty Ltd v. Nine Network Australia Pty Ltd* (HCA 14 [2009]), the High Court of Australia reaffirmed its commitment to the anthropocentric paradigm of copyright law, consistently denying legal personality to AI systems. The Court has ruled: the only person who can claim copyright for a work created using information technology is the individual who performed the necessary actions to generate the result. The Court has remained faithful to the traditional doctrine of individual authorship, declining to determine the copyright holder. Available at: URL: https://www.hcourt.gov.au/sites/default/files/assets/publications/judgment-summaries/2009/hca14-2009-04-22.pdf (accessed: 02.11.2025)

property laws of its member states [Iglesias M., 2021: 14]. This position is also reflected in the practice of the European Court of Justice with regard to concepts such a labour, personality, etc. (e.g., in the *Levola v. Smilde* decision of the European Court of Justice in [2018]) [Papadopoulou A., 2021: 417]. To prevent legal regulation dysfunction with regard to results not created with direct human involvement and to overcome legal uncertainty regarding the criteria for the protectability of results created using AI, the following alternative can be proposed: modifying the legal regime by relaxing the mandatory requirements for establishing human authorship [Picht P.G., Thouvenin F., 2023: 138]; replacing the traditional criterion of creative character with the investment criterion.

Unlike the concept of recognising AI's legal personality, the investment criterion does not require a fundamental overhaul of legislation, indicating its greater feasibility in the short term. In the prevailing legal paradigm, the criterion of creative character assumes that a person must be involved in creating of intellectual property. Therefore, to obtain legal protection, it is necessary to prove the extent of a person's creative contribution. Regarding works generated exclusively by AI, most jurisdictions have no grounds for recognising them as objects that may be protected.

A key element of legal qualification is demonstrating that person has had a creative influence on the generated content. In particular, when modifying a result created by AI, the person has to document the changes made to justify authorship.

The main problem with the traditional casual approach involving individual judicial assessment of human contribution in each case, is the lack of a unified methodology for measuring the contribution. This could lead to excessive reliance on judicial discretion and encourage rights holders to deliberately make formal changes to AI-generated objects (e.g., editing images or applying filters) solely to formally meet the protectability criteria.[7].

Because of it, under the conventional approach, protectability arises exclusively when human creative participation can be proven, which

[7] One example of this is the practice of the US Copyright Office. The Office assumes the works created without human creative input are not subject to copyright protection. However, it has secured copyright for the *Invoke* image generator because it combines human creativity with the generation and documentation of creative techniques.

provokes deliberate artificial modification of AI-generated content. The key issues are the lack of a unified methodology for assessing creative contributions and the prevalence of subjective judicial discretion when resolving disputes.

5. Reasons for Replacing Security Criterion for AI-generated Results

The key problem with legal regulation of AI is the subject/object paradigm that dominates jurisprudence. As an alternative doctrinal basis, the categories of Dasein (existential being) and Das Man (impersonal existence) from Martin Heidegger's philosophy are proposed. Within this paradigm AI is classified as "Das Man" that demonstrates a mechanical imitation of the creative process ("Das-Man-creativity"), lacking an existential dimension and the capacity for existential reflection. The individual (the party to the legal relationship: a user, a developer) is interpreted as Dasein, the primary source of genuine creative potential ("Dasein-creativity").

Extrapolating Heidegger's categories of Dasein and Das Man offers a key to the theoretical justification for replacing the creativity criterion with the investment criterion. Dasein "questions" its own existence, whereas Das Man is a mechanical imitation devoid of ontological reflection. I.A. Ivanyushkin classifies AI as a technical entity devoid of any ontology, which emphasizes its fundamental alienation from the existential dimension of human existence [Ivanyushkin I.A., 2019: 15].

Under the traditional "subject-object paradigm," the functional capacity of AI to perform legally significant actions creates the formal basis for classifying it as a legal entity, by analogy with humans. However, when moving on to the categories of Dasein-belonging and Das Man-belonging, it becomes clear only humans possess "genuine legal personality." For instance, legal entities have social relationships between participants that are not mere imitation, but this is not the case with AI.

The cognitive activity of AI is a mechanical imitation of the creative act, i.e., Das-Man-creativity. Traditional copyright protection should apply to Dasein-creativity, while derivative Das-Man-creativity, as imitation, should be regulated under related rights. As A.V. Pushkarev notes, the synthesis of the artificial and the natural constitutes potential existence as a necessary condition for the actualisation of creative meanings and an ontological guarantee of creative existence, pointing

to the derivative nature of the creative potential of intellectual systems [Pushkarev A.V., 2017: 10].

To secure the legal protection of AI-generated results, the creative character criterion should be replaced by the investment criterion. Similarly to the legal regime governing investment databases, protection of the results of Das-Man-creativity should be carried out under the institution of related rights the subject of which is Dasein that has invested resources in the creation of the result.

Thus, the hypothesis proposed in this article is confirmed: granting AI legal personality is unnecessary; modifying the mechanism of protectability by changing the criteria and introducing related rights in relation to the AI-generated results is the best solution. Consequently, when classifying AI as a subject of law, it would be methodologically unsound to recognise AI as having legal personality *sui generis*. Likewise, applying the legal concepts of copyrighted works or works for hire to results created by AI attributes artificial intelligence with the qualities of a performer (employee) and thus a subject of legal relations.

When AI is applied, systems operating on the basis of algorithmic and mathematical models process information arrays to generate results. The final results of intellectual activity are created by many entities: developer of the algorithmic system, project organiser (or investor), user who initiates the generation process, and the AI system itself, that acts as a creation tool. Each participant in this process potential has the right to claim ownership of the results obtained, which creates a complex legal problem in distinguishing their respective rights.

The analysis suggests that it would be inappropriate to recognise AI as a legal entity. In this regard, legal models that exclude granting AI the status of an independent legal entity being considered. As for the developer of algorithmic solutions, the investor, and the user, the difficulty lies in the fact each of them can claim a certain amount of authority over the result created.

6. Qualification of User Agreements on the Use of Online Services that Generate Results Using Artificial Intelligence

Nowadays, we are seeing an increasing number of online services that use AI to generate results comparable to those produced by human intellectual activity. In most cases, the document users read before using

these services is called a "user agreement." This raises the issue of the legal classifying such user agreement. Indeed, since the current legislation does not contain such a category, the rules on a particular contract specified in the Civil Code should be applied to the "user agreement."[8]

M.A. Rozhkova notes that when studying the features of a user agreement associated with the digital environment: "The essence of any digital service lies precisely in the service <...>, in any case, we will be talking about mixed or even unnamed contractual structures" [Rozhkova M.A., 2024: 128]. Since the core value of any online service lies in its service component, the specific nature of online services necessitates the use of either hybrid contractual schemes that combine elements of different contracts, or completely original contractual models (contractus innominati) that are not described in law. Therefore M.A. Rozhkova concludes, the legal nature of a user agreement may be either a traditional contract for the provision of paid services or a mixed contract incorporating elements of a licence agreement and a contract for the provision of paid services; this mixed contract is not exclusively a licence agreement.

Analysing the possible classification of user agreements as licence agreements, A.E. Shchukina argues this classification is only justified if the service is recognised as intellectual property. If the contract only regulates access to the service and does not transfer ownership of the intellectual property, it should be considered a contract for the provision of paid services, and more specifically, information services.[9]

Expanding on this idea, M.A. Rozhkova writes: "A contract for the provision of information services <...> does not relate to licence agreements but is a type of contract for the provision of paid services, the defining feature of which is the absence of a tangible outcome of an action or activity" [Rozhkova M.A., 2024: 128]. Consequently, the contract for the provision of information services referred to in Paragraph 2, Article 779 of the Civil Code is a special type of paid service provision, rather than a licence agreement, since the key feature is that the result of the activity performed is intangible.

---

[8] Hereinafter, the term "user agreement" refers exclusively to the user agreement for the use of online services that enable one to create results using AI.

[9] Shchukina A.E. User agreement: licence agreement vs service agreement // Zakon.ru. 2020. Available at: URL: https://zakon.ru/blog/2020/06/18/polzovatelskoe_soglashenie_licenzionnyj_dogovor_vs_dogovor_okazaniya_uslug (accessed: 02.11.2025)

Regarding the understanding of the user agreement as a mixed contract, A.E. Shchukina writes: "It is possible to conclude a mixed-type contract that will contain both the terms of the licence and the terms of service provision."[10]. Judicial practice confirms this point of view.[11]. Paragraph 47 of Resolution No. 49 of the Plenum of the Supreme Court of the Russian Federation of 25 December 2018 states that when legally qualifying an agreement in accordance with Paragraphs 2 and 3 of Article 421 of the Civil Code, the essence of the relevant obligations should be considered.

The formal aspects, such as the title of the contract, the names of the parties, the terminology used to describe performance, etc., are not decisive. E.B. Poduzova claims: "In addition to the essential terms and conditions <...>, the user agreement must contain terms and conditions regarding the procedure for providing and processing user information using artificial intelligence technologies, <...> terms and conditions regarding the legal regime for such information" [Poduzova E.B., 2023: 75].

It would initially seem reasonable to recognise the hybrid nature of "user agreements," given the peculiarities of the functioning online platforms that combine the service provision and the generation of intellectual activity results. It seems obvious the use of services based on generative AI simultaneously involves both elements of a license agreement and a contract for the provision of paid services.

At the same time, it should be borne in mind: in Russia results created using technical means without creative human activity are not subject to copyright[12]. According to the Russian Federation Supreme Court's stance, regardless of what the "user agreement" results will be deemed unprotectable due to the lack of human creative input and the use of automated generation without human intervention. Consequently, such

[10] Ibid.

[11] See: Sentence of the Arbitration Court of the Moscow District of 18.06. 2015 No. F05-7093/2015 in case No. A40-91072/14. Available at: URL: https://kad.arbitr.ru/Document/Pdf/277fdd53-f30b-4de4-a282-732bc448297e/cab5453e-c3de-4d99-bdf3-5d162236b2e0/A40-91072-2014_20150618_Reshenija_i_postanovlenija.pdf?isAddStamp=True (accessed: 02.11.2025)

[12] Paragraph 10 of Resolution No. 10 of the Plenum of the Supreme Court of the Russian Federation of 23.04. 2019 "On the Application of Part Four of the Civil Code of the Russian Federation." Available at: URL: https://www.vsrf.ru/documents/own/27773/ (accessed: 02.11.2025)

results will be subject to the legal regime of free use, and no one will be able to obtain intellectual property rights to them.

Therefore, under current Russian legislation, a "user agreement" is exclusively either a contract for the provision of paid services or a contract for the provision of free services not specified in the Civil Code. In this case, no licensing relations arise, since the results created by AI are not protectable and there is no rights holder, which precludes the emergence of such legal relations. At the same time, if the amendments proposed by the author concerning the introduction of related legal protection for AI-generated results are incorporated into legislation, the "user agreements" discussed above will be classified as mixed contracts, thereby allowing for the licensing of related rights.

Conclusion

Artificial intelligence performs a communicative function between the creators of the source data and the person formulating a targeted query. The most relevant legal analogy in this context is the legal regime governing databases. However, AI demonstrates a higher level of functionality by generating derivative data based on the perception of the original information without modifying the concept of legal personality. In process of classifying legal regime for results created using AI, the creative nature criterion should be replaced by the investment criterion, similar to the legal protection of investment databases.

Two types of "creativity" were discussed in the paper:

"Dasein-creativity" is a process whereby the result is initially formed in the creator's mind and the receives legal recognition through the criterion of creative character and becoming protectable under copyright law.

"Das-Man-creativity" is the process of generating results through the mathematical modelling of intellectual activity. This process is subject to legal qualification based on investment criteria and is protected under the institution of related rights.

Dasein should be recognised as the subject of related rights to such results, since it provided the organisational, technical, and investment conditions for their creation. In this context, AI acts as an "information intermediary," processing data arrays and facilitating communication between entities. However, unlike the latter, it lacks the capacity for existential reflection. Empirically studies have shown that the absence of

human participation in the communication chain negatively impacts AI performance.

Consequently, the previously proposed hypothesis is confirmed: the creativity criterion should be replaced by the investment criterion for the results of *Das-Man*-creativity. Alongside this, there is a need to improve the regulatory oversight of the commercial use of AI systems, including issues relating to the use of generated results and the distribution of revenues among rights holders [Watiktinnakorn C., 2023: 9].

Results, generated by using AI, have potential to unintentionally infringe on the exclusive rights of third parties. The person using the AI system and receiving the corresponding result is generally recognised as being responsible in the event of any resulting damage. AI should be used as a tool for expanding human capabilities, and not limiting them.

So, under current law replacing the creativity criterion with the investment criterion appears to be the best solution. By extrapolating Heidegger's Das Man philosophical category to the legal nature of AI, a philosophical and legal rationale was developed for replacing the creativity criterion with the investment criterion. It has been established that legal protection through the granting of related rights should be extended to the results generated by AI systems. In this work, these results are defined as "Das-Man-creativity."

Another important issue is the legal protection term granted under related rights to results created by AI:

For results that are the product of human creativity, where AI was used merely as a tool, the term of legal protection should the same as the term of exclusive rights to the work, which lasts throughout the creator's lifetime and for 70 years thereafter.

In the case of results created autonomously by AI, without any human creative input, the legal protection term should equal the database manufacturer's exclusive rights term and remain in force for 15 years.

Therefore, author proposes replacing the criterion of creativity with the criterion of investment as a means of protecting the results created by AI. In any case, artificial intelligence is considered a tool, and the related rights to its results should belong to the person who invested resources in creating them. This decision is technically sound and represents the optimal solution, as it reduces legal uncertainty and does not require fundamental changes to legislation.

References

1. Balashova A.I. (2023) Legal Regime of Results of Artificial Intelligence Activities: Unity and Differentiation of Approaches. *Zhurnal Suda po intellektual'nym pravam*=Journal of the Court on Intellectual Property Rights, no. 3, pp. 190–206 (in Russ.)

2. Iglesias M. (2021) Intellectual property and artificial intelligence. A literature overview. Luxemburg: EU Publications Office, p. 14. Available at: URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC119102 (accessed: 04.06.2025)

3. Ivanyushkin I.A. (2019) Artificial Intelligence: Prospects for Sociocultural Transformations. *Vestnik Moskovskogo pedagogicheskogo universiteta. Filosofskie mauki*=Bulletin of Moscow Pedagogical University. Philosophical Sciences, no. 4, pp. 10–20 (in Russ.)

4. Kalyatin V.O. (2022) Definition of Subject of Rights on Results of Intellectual Activity Created using Artificial Intelligence and its Impact on Civil Legislation. *Pravo. Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 15, no. 4, pp. 24–50 (in Russ.)

5. Lukina G.U., Kuprina E.Y. (2023) Reasoning About the Concept of "Artistic Intent". *Khudozhestvennaya kul'tura*=Artistic Culture, no. 4, pp. 12–33 (in Russ.)

6. Milyukov S.A. (2025) AI-created Objects as Objects of Copyright and Related Rights. *Zhurnal Suda po intellektual'nym pravam*=Journal of the Intellectual Property Court, no. 1, pp. 63–73 (in Russ.)

7. Ogorodnikova K.S. (2021) Issue of Originality of a Work in Copyright. *Voprosy rossiyskogo i mezhdunarodnogo prava*=Issues of Russian and International Law, vol. 11, pp. 60–67 (in Russ.)

8. Papadopoulou A. (2021) Creativity in Crisis: Are the Creations of Artificial Intelligence Worth Protecting? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, no. 3, pp. 408–418.

9. Picht P.G., Thouvenin F. (2023) AI and IP: Theory to Policy and back again — Policy and Research Recommendations at the Intersection of Artificial Intelligence and Intellectual Property. *International Review of Intellectual Property and Competition Law,* vol. 54, no. 4, pp. 123–145.

10. Poduzova E.B. (2023) User Agreement, Confidentiality Agreement: Content in the Context of Using Artificial Intelligence Technologies. *Aktual'nyye problemy rossiyskogo prava*=Issues of Russian Law, no. 2, pp. 71–78 (in Russ.)

11. Pushkarev A.V. (2017) Philosophical Foundations of Artificial Intelligence: Candidate of Philosophical Sciences Summary. Ufa, 20 p. (in Russ.)

12. Rozhkova M.A. (2024) Differences between License Contract and User Agreement. *Zhurnal Suda po intellektual'nym pravam*=Journal of the Intellectual Property Court, no. 4, pp. 121–133 (in Russ.)

13. Rusakov S.S. (2024) Early Heidegger and Relationship between Subject and Dasein. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Gumanitarnye nauki*=Bulletin of Tula State University. Humanitarian Sciences, no. 2, pp. 143–151 (in Russ.)

14. Shchukina A.E. (2020) User Agreement: License Contract vs. Contract for Provision of Services. Available at: URL: https://zakon.ru/blog/2020/06/18/ polzovatelskoe_soglashenie_licenzionnyj_dogovor_vs_dogovor_okazaniya_uslug (accessed: 03.11.2025) (in Russ.)

15. Watiktinnakorn C. (2023) Blurring the Lines: How AI is Redefining Artistic Ownership and Copyright. *Discover AI,* pp. 1–10.

Information about the author:

P.K. Pakshin — Postgraduate Student.

The article was submitted to editorial office 03.11.2025; approved after reviewing 15.12.2025; accepted for publication 15.12.2025.

Legal Issues in the Digital Age 2026. Vol. 7, no. 1.
Вопросы права в цифровую эпоху. 2026. Том 7. №1.

Research article
JEL: K00
UDK: 378.1:004.8:174
DOI:10.17323/2713-2749.2026.1.49.70

Ethical Aspects of AI Regulation for Higher Education

Said S. Gulyamov[1], Islambek R. Rustambekov[2]

[1,2] Tashkent State Law University, 35 Sayilgokh, Tashkent 100047, Uzbekistan,

[1] said.gulyamov1976@gmail.com, https://orcid.org/0000-0002-2299-2122

[2] i.rustambekov@tsul.uz, https://orcid.org/0000-0002-8869-8399

Abstract

The article provides a comprehensive analysis of the AI Code of Ethics for education developed at the Tashkent State Law University. The AI Code ushers in a distinctive shift from prohibitive approaches to AI governance in higher education on the basis of the principle of precedence of education and mentorship over restrictive measures. By analyzing in detail the Code's thirty-one articles contained in four parts (general provisions, AI usage in education, AI usage in research, governance and supervision) as supplemented by methodological framework for AI assessment and governance structures, this study showcases a comprehensive system introduced by the Code to establish precedence of education over prohibitions while maintaining academic integrity. The analysis flags innovative governance mechanisms (such as tripartite AI ethics councils including professors, technical specialists, students) and functions, all-around risk assessment protocols, adaptive phased introduction strategies and methodology for AI-assisted academic performance assessment based on a parallel system for analyzing the share of human involvement and AI. The Code integrates international standards (such as the UNESCO Recommendation on the Ethics of Artificial Intelligence, GDPR principles, International Center for Academic Integrity' values) in adapting them to specific educational context. The authors examine both the Code's potential benefits for education institutions (AI competency development, vocational preparedness, critical thinking skills) and implementation problems to be carefully considered (available resources, change management, methodological aspects of AI-assisted verification of outcomes). Much focus is made on the model's scalability in view of variable budgeting levels and international cooperation mechanisms to achieve equitable access to technolo-

gies. The Code is important for showcasing a practicable model designed for education institutions worldwide to address the issues of responsible AI integration while maintaining academic standards and human-centered approach to education in the context of technological change.

Keywords

artificial intelligence; educational ethics; academic integrity; governance; higher education; technology policies; human center education; ethics council.

For citation: Gulyamov S.S., Rustambekov I.R. (2026) Ethical Aspects of AI Regulation for Higher Education. *Legal Issues in the Digital Age,* vol. 7, no. 1, pp. 49–70. DOI:10.17323/2713-2749.2026.1.49.70

Background

Integrating AI into education systems is largely transformative for universities as it radically changes the ways knowledge is transmitted and the nature of the learning process[1]. With the growing sophistication and accessibility of AI technologies, education institutions worldwide find it considerably difficult to match innovation with academic process integrity, student wellbeing and ethical responsibility as they prepare students for vocational environments where AI competencies become critical.

Traditional responses to introducing technologies into education will assume prohibitions, only to create tensions between technological change and educational values[2]. This approach often proved inadequate since it did not recognize either the potential of new technologies or a need to make students ready for technologically integrated vocational contexts with increasingly valuable AI competencies [Koshel A.S., Kuzminov Ya.I. et al., 2025: 58].

[1] Trapeznikov V., Zinovieva E. Neural networks and generative AI in higher education: international experience and national practices. Russian Council on International Affairs. Available at: URL: https://russiancouncil.ru/analytics-and-comments/analytics/neyroseti-generativnyy-ii-v-vysshem-obrazovanii-mezhdunarodnyy-opyt-i-rossiyskaya-praktika/?sphrase_id=150634182 (accessed: 28.01.2026)

[2] Digital learning and ICT in education. Available at: URL: https://digital-strategy.ec.europa.eu/en/policies/digital-learning?utm_source=chatgpt.com (accessed:12.01.2026)

The AI Code of Ethics drafted at the Tashkent State Law University ushers in a shift from prohibitive to education-focused AI governance in academic context[3]. The Code's comprehensive design comprises four sections of 31 articles supported by detailed implementation strategies and governance structures. This represents a systematic attempt to put in place an ethical AI governance system at education institutions for precedence of mentorship and skill development over restrictive measures.

The authors offer a detailed analysis of the AI Code of Ethics and supporting documents in examining the Code's fundamental principles, scope, methodological approaches and implications by reviewing each of its parts. The study purports to fill the gaps in AI governance literature and proposes governance arrangements for education institutions which strive to responsibly integrate AI technologies.

1. Historical Background and Educational AI Ethics

1.1. Restrictive and prohibitive approaches

Education institutions would historically respond to disruptive technologies by a varying extent of resistance and gradual upgrade in the wake of restrictive and prohibitive patterns. The emergence of web technologies in the 1990s first raised concerns over violation of academic principles of teaching, only to cause numerous institutions to restrict Internet access in education. Similarly, the outburst of social media platforms in the 2000s raised concerns over distracted student attention and improper content resulting in the platforms being blocked. The widespread use of mobile devices brought about more waves of prohibitions in an attempt to maintain the traditional classroom dynamics [Rodgers D.J., 2012: 88].

Each technological wave followed the same path: initial prohibition caused by fear of risk, gradual recognition of education potential of the innovation, reluctant upgrade and integration. Education institutions would finally recognize both the value of restrictions and the need to make their students ready to embrace technologically integrated vocational environments. However, the transition being time-consuming, the institutions that prefer prohibitive approaches would often put their

[3] AI Ethics Code in Education. 2024. Tashkent State University of Law. Complete information is available at the University's website at: www.tsul.uz.

students at a disadvantage compared to those adopting integration strategies.

The COVID-19 pandemic accelerated digital transformation in education by putting gradual change on the adaptive fasttrack[4]. Transformation revealed both the potential of technologically bolstered education, as well as the long overdue need to establish and strengthen ethical attitudes for introducing technologies at scale. The institutions that made digital teaching and ethical restrictions part of their academic practices were better positioned to maintain the education quality during transition while those relying on prohibitions turned out to be unprepared for technologically mediated education.

1.2. Generative AI challenges in educational contexts

The emergence of generative AI systems, especially of large language models is fraught with challenges differing from past education technologies in a number of ways. Unlike those previous technologies which were primarily about access to information and communications, generative AI systems can create content which resembles an academic thesis, only to raise the questions of authorship, originality, evaluation precision and the nature of learning[5].

The ability of modern AI systems to produce consistent, contextually suitable texts for various disciplines makes inadequate the mechanisms to identify plagiarism as they were designed to identify copying from traditional sources, not newly generated content [Weber-Wulff D., 2023: 15]. Explosive AI progress means that static assumptions quickly become obsolete and require adaptive governance to keep pace with technological change and maintain ethical standards[6]. Potential benefits of AI-assisted learning are numerous and well documented, only to make general prohibitions useless [Luckin R., 2016: 23].

---

[4] Eurocommission: Directorate-General for Education, Youth, Sport and Culture. The impact of COVID-19 on higher education. A review of emerging evidence. Luxemburg, 2021. Available at: URL: https://data.europa.eu/doi/10.2766/069216 (accessed: 01.12.2025)

[5] Guidance for generative AI in education and research. Available at: URL: https://unesdoc.unesco.org/ark:/48223/pf0000389639 (accessed: 01.12.2025)

[6] The ethics of artificial intelligence: Issues and initiatives. EU Parliament Research Service. Available at: URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU%282020%29634452_EN.pdf (accessed: 03.12.2025)

Studies demonstrate that university students are currently apt to widely use AI in their academic work irrespective of institutional policies, with varying patterns depending on disciplines, academic level and cultural contexts [Perkins M., 2023: 1]. As follows from behavioral studies, a large share of students experimented with AI writing tools, with many aware of a gap between institutional restrictions and vocational expectations [Johnston H., 2024: 1]. The reality again underlines the weakness of prohibitive approaches and their negative outcomes. Such approaches create an environment where students develop AI competencies outside any ethical guidance or institutional support.

1.3. Legal and regulatory context

The AI Code of Ethics is drafted in a legal and regulatory environment where a line is drawn between the international and national frameworks. It is harmonized with the Recommendation on the Ethics of Artificial Intelligence approved by the UNESCO in 2021 and setting out the global principles of AI development to be followed with respect for national sovereignty[7]. This harmonization is meaningful as the Code translates the UNESCO's broad principles into guidance for education institutions.

References to the Universal Declaration of Human Rights (1948)[8], especially Article 26 (right to education) and Article 19 (freedom of expression), are designed to make the Code solidly based on international law. This positions the AI ethics as part and parcel of human rights with implications for access to education, equity and human dignity.

Nationally, the Code comprises references to the Constitution of Uzbekistan[9] (primarily its Article 51 on the right to education), Law on Education[10], National Development Strategy for 2022–2026[11], 2030 Digital

[7] UNESCO Recommendation on the Ethics of Artificial Intelligence. Available at: URL: https://unesdoc.unesco.org/ark:/48223/pf0000385082 (accessed: 01.12.2025)

[8] Universal Declaration of Human Rights. Available at: URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights (accessed: 03.12.2025)

[9] Constitution of Uzbekistan (8.12.1992 as amended on 30.04.2023). Available at: URL: https://lex.uz/docs/6445147 (accessed: 01.12.2025)

[10] Law of Uzbekistan on Education No. ZRU-637 of 23 September 2020. Available at: URL: https://lex.uz/ru/docs/5013009 (accessed: 01.12.2025)

[11] Presidential Decree No. UP-60 "On the development strategy of new Uzbekistan in 2022–2026". 28 January 2022. Available at: URL: https://lex.uz/ru/docs/5841077 (accessed: 01.12.2025)

Strategy for Uzbekistan[12] and the 2030 Higher Education Development Concept[13]. This integration highlights the understanding of linkages between international principles and national approaches towards their implementation.

The Code's political neutrality matched with respect for national sovereignty reflects recognition that, while AI ethical principles gain from global coordination, their introduction should be adapted to national educational traditions, regulatory systems and cultural contexts.

2. Fundamental Principles

2.1. Scope and purposes

The Code's opening article describes its fundamental purpose by establishing that it "determines ethical principles and guidelines for responsible use of artificial intelligence in education" (Article 1.1). This wording differentiates the Code from purely prohibitive measures by presenting it as a guiding document for support of ethical and responsible approach to AI integration into the learning process.

The purposes stated in Article 1.2 (maximizing AI educational potential along with protecting human dignity, developing AI competencies and making education opportunities equally accessible) reflect understanding of manifold implications of AI implementation at education institutions. These purposes are structured so as to avoid false dichotomies between technological change and ethical responsibility by positioning them as auxiliary for educational precedence.

Article 1.3 contains the Code's fundamental principle that "education and mentorship are more useful than prohibitive measures for attaining ethical use of AI". This principle highlights a shift from traditional politicized approaches and establishes a philosophical foundation of education. Rather than considering AI as a threat to be countered, the Code views it as a tool to be mastered through good governance and skill

[12] Presidential Decree No. UP-6079 "On Approving the 2030 Digital Strategy for Uzbekistan and Relevant Measures for its Efficient Implementation " of 05 October 2020. Available at: URL: https://lex.uz/docs/5031048 (accessed: 03.12.2025)

[13] Presidential Decree No. UP-5847 "On Approving the 2030 Higher Education Development Concept". 08 October 2019. Available at: URL: https://lex.uz/ru/docs/4545887 (accessed: 03.12.2025)

development. This approach reflects the findings of behavioral studies in the context of technological change. Researchers note that the strategy of positive engagement is often more supportive of ethical standards than negative sanctions.

2.2. Comprehensive institutional coverage

Article 2 discards narrow approaches to AI which often apply only to students or specific channels of academic activity. In embracing "all members of academic community: students, professors, researchers, administrative staff and third-party partners" (Article 2.2), the Code recognizes that ethical AI use requires institution-wide commitment instead of fragmented compliance with the interests of specific groups.

The inclusive approach reflects recognition that AI ethics in education cannot be served by student-centered policies alone. Professors using AI for research and teaching should understand ethical practices; administrative personnel deploying AI systems should ensure they operate in line with ethical principles; third-party partners for AI-related services should be respectful for institutional values. The Code's comprehensive approach will consistently support ethical standards across all these interactions.

The provision on adapting to "various educational contexts in supporting the fundamental ethical principles" (Article 2.3) reflects the awareness of institutional diversity. Rather than imposing rigid requirements, the Code provides for a flexible framework enabling contextual adaptation to support essential ethical standards. Moderate flexibility represents a desire to avoid mistakes of the previous attempts to govern technologies which would often fail by being overly rigid or too slack to the point of ignoring standards[14].

2.3. Definitional framework

Content of Article 3 refers to key concepts that often lack precision in AI governance documents. Defining AI as "systems that can process data and information in ways entailing elements of reasoning, learning,

[14] Regulatory complexity and the quest for robust regulation. Reports of the Advisory Scientific Committee No. 8. 2019. European Systemic Risk Board. Available at: URL: https://www.esrb.europa.eu/pub/pdf/asc/esrb.asc190604_8_regulatorycomplexityquestrobustregulation~e63a7136c7.en.pdf (accessed: 01.12.2025)

perception, prediction, planning or control" (3.1) agrees with modern AI studies while being accessible to non-technical audiences[15].

The definition of academic integrity (Article 3.2) refers to fundamental values of the International Center for Academic Integrity[16] — trust, equity, respect, responsibility, valor — and provides for continuity with prior educational values acknowledged in AI-related contexts. Instead of taking a view on AI as fundamentally disruptive for academic integrity, the Code presents it as a new context where the established values apply.

The concepts of "human in the loop" and of "significant human contribution" (3.3 and 3.4) reflect concerns over AI's educational role. Serving to prevent a view at AI as either panacea or critical threat, these definitions present AI as a tool that calls for well-thought human involvement. The definition of significant human contribution as "intellectual activity" includes "problem statement, critical analysis of outcomes, final decision-making and creative development of ideas". This is to provide guidance in judging whether the use of AI is supportive of the relevant human activities.

2.4. Fundamental principles

Eight fundamental principles of Article 4 are at the heart of the philosophy of the Code's approach to AI governance harmonized with the Ethical Guidelines on the use of artificial intelligence and data in teaching of educators developed by the European Commission in 2022[17]. The said principles deserve to be discussed both individually and collectively.

"Education over prohibition" — traditional approaches are apt to back down in the face of risk rather than exploit new opportunities. As follows from studies of technologies used in education, prohibitive

[15] Thus, it agrees with definitions contained in EU regulations such as Regulation (EU) 2024/1689 on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act, Article 3 (1). Available at: URL: https://artificialintelligenceact.eu/article/3/ (accessed: 03.12.2025)

[16] International Center for Academic Integrity (no date and place). Available at: URL: https://academicintegrity.org/ (accessed: 02.12.2025)

[17] Eurocommission. 2022. Ethical guidelines on the use of artificial intelligence and data in teaching and learning for educators. European Education Area. Available at: URL: https://education.ec.europa.eu/news/ethical-guidelines-on-the-use-of-artificial-intelligence-and-data-in-teaching-and-learning-for-educators (accessed: 04.12.2025)

approaches often result in antagonisms while being unable to develop competencies for ethical use of technologies. This principle recognizes the ethical use of AI as a competency to be developed under human control, not a subject to coercion and prohibition.

The principle whereby "AI amplifies human intelligence but does not replace it" reflects concerns over technological bias in acknowledging AI potential. AI is thus presented as an incremental technology designed to amplify human abilities rather than autonomous entity functioning independently of man. Human-centered approach requires AI to be implemented on the basis of extensive human agency in decision-making and creative work.

Transparent disclosure of AI use reflects concerns over fraudulent practices in teaching how to use patterns. This requirement serves multiple functions such as avoiding misleading presentation of AI-assisted outcomes; revealing patterns being used; opportunities for exchange of experience. Accountability mechanisms make sure that persons continue to be responsible for the work they perform even where AI is involved.

Integrating AI within the framework of academic integrity serves to prevent the emergence of parallel ethical systems while highlighting the importance of this technology. That principle portrays AI is a new context subject to the established values rather than fundamentally disruptive for academic integrity.

Adherence to non-discrimination and equal opportunities reflects concerns over AI bias and how the principle of equality in education is observed. Equity requires from AI systems and policies to avoid creating or perpetuating defects on the basis of protected parameters in regulating access to technological capabilities.

The requirement to AI to be relevant to educational goals serves to prevent both excessive technological dependence and poor use of what the technology is capable of. Relevance calls for AI usage intensity to be in line with educational goals and general development needs.

Concerns over environmental and social sustainability recognize broad social implications of AI. The sustainability principle calls for attention to environmental costs and social implications of AI systems.

The transparency and explainability requirement refers to technical obstacles in supporting accessibility. This principle assumes that different stakeholders will require different explainability levels with respect to AI systems.

2.5. Rights and duties

Articles 5 and 6 establish the framework of rights and duties by combining personal autonomy with collective obligations. The framework of Article 5 refers to stakeholder groups in promoting universal principles. The right to "equal access to educational opportunities irrespective of how well AI technology is mastered" (5.1) purports to bridge the digital gap that can exacerbate the existing inequality.

Student rights (5.2) include the right to be instructed on AI use; mentorship to develop competencies; equitable evaluation of AI-assisted outcomes; maintaining access to technologies irrespective of economic situation. Professor rights (5.3) include protection of intellectual property; academic freedom in the process of AI integration; opportunities for vocational development; participation in the design of operating methods.

The duties under Article 6 highlight collective responsibility for ethical use of AI while avoiding punitive language. The recommendation of "active development of AI competencies" while stating that "a lack of such competencies cannot serve as a basis for discrimination" (6.3) demonstrates understanding of the problems of transition faced by educational communities.

2.6. Operating basis

Articles 7 through 10 of the Code establish operating framework of data protection, non-discrimination, academic freedom and international cooperation. Provisions of Article 7 (data protection) are harmonized with international standards including GDPR[18]. The non-discrimination requirements of Article 8 reflect concerns over AI bias in establishing the obligations of institutional support. Academic freedom protection (Article 9) purports to ensure that AI integration serves the achievement of educational objectives without restricting them. The provision for international cooperation (Article 10) reflects the recognition that AI governance challenges go beyond institutional borders with due respect for national sovereignty.

[18] General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 (2016). Available at: URL: https://gdpr-info.eu/ (accessed: 01.12.2025)

3. AI in Education: Implementation Framework

3.1. Approaches to integration and assessment

Articles 11–18 translate the fundamental principles into practical guidance for educational activities. These articles address pedagogical problems exposed by AI integration, with the main focus on learning outcomes. The integration context of Article 11 highlights the priority of pedagogical relevance over technological capabilities by requiring that AI implementation be "methodologically adequate, transparent, validated and ethically reasonable". The focus on measuring "learning outcomes rather than AI use patterns" reflects the understanding that the value of technology comes from its educational impact rather than mere availability (11.1).

3.2. Students development

Article 12 (AI student literacy) refers to a subject is often left out. Competencies include the knowledge of technology, ethical awareness, critical judgment skills and creative abilities. The Article reminds that AI integration into education calls for active student involvement, not passive consumption of AI-generated content.

A human-centered educational model established in Article 12 relies on three components: technological literacy; significant involvement of human intelligence; and academic quality (12.1).

3.3. Academic integrity and AI-assisted work

Articles 13 and 14 refer to supporting academic integrity when using AI. The documentation requirements of Article 13 are a practical approach to transparency in the process of learning and accountability. Requiring students to document scrupulously the tools, methods of use, their role in driving the outcomes, as well as to recognize the responsibility for the final product (13.2), provides guidance without introducing general prohibitions.

Article 14 addresses critical judgment skills as well as concerns over student dependence on AI systems. Under 14.2 critical judgment of AI-assisted outcomes includes verification of facts, assessment of logical consistency, identification of bias, identification of data relevance and

comparison with alternative sources. These requirements contribute that AI promotes critical judgment skills rather than replaces them.

3.4. Assessment methodology

Article 15 addresses the assessment of students' academic performance where AI is used. A focus on "quality of thinking, understanding and skill development" including "in-depth understanding, quality of critical thinking, AI use performance, originality of problem-solving and ability to improve on AI outcomes" creates the context for assessing AI-assisted projects (15.1). Meanwhile, introducing all these criteria at one time will create problems to be addressed by institutions through capacity building and resource distribution.

The Code's methodology puts in place a parallel system of assessment with independent "analysis of AI/human involvement" and "analysis of originality". This two-track approach enables institutions to support academic integrity while allowing appropriate AI assistance although this methodology requires empirical assessment based on implementation experience in order to be effective.

3.5. Capacity building and support of professors

Articles 17 and 18 refer to the role of professors in educational environments integrated with AI. Describing professors as "active mentors for ethical use of AI" (17.1) reflects a shift from restrictive stereotypes to educational approaches which recognize the value of competencies required for AI integration. As defined in 17.2, the role of professors includes: teaching to use AI responsibly; establishing clearly formulated expectations; designing assessment methods; modelling the use and supporting critical thinking.

In defining what is meant by professor skill development, Article 18 reminds that AI integration requires to improve their abilities. Adaptive program approach taking into account the roles of participants, technical and ethical aspects, practical skills and communities of practitioners relies on understanding skill development principles[19]. Meanwhile, the requirements to resources for comprehensive capacity building of professors are unlikely to bring fruit in case of institutions on a limited budget.

[19] European Commission. 2023. Commission staff working document on digital education and training 205 final. Available at: URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023SC0205 (accessed: 01.12.2025)

4. Harnessing AI for Science

4.1. Ethics of research

Articles 19-25 address the questions of dishonest research in the context of innovations. They provide guidance for harnessing AI for research. Principles of Article 19 support traditional standards of research ethics while recognizing AI potential for science. The accent on "using AI to amplify rather than substitute for human judgment, creativity and expertise" (19.2) serves to ensure human-centred research where technological resources are used.

A requirement to "researchers to support expertise to understand, assess and validate AI outcomes" (19.3) refers to concerns over growing human dependence on AI. This provision is to ensure that researchers develop their own intellectual potential and apply AI responsibly.

4.2. Research integration approaches

Article 20 addresses the use of AI over the whole cycle of research. The cycle includes: review of literature, proposing hypotheses, collecting data, analyzing and disseminating findings (20.1).

A requirement of "methodologically appropriate, transparent, validated and ethically reasonable integration in line with disciplinary standards" (20.2) contains research assessment criteria.

4.3. Standards of originality and contribution

Article 21 addresses the issues of originality of AI-assisted research by setting the standards of novelty. The principle of novelty ("unique problems, innovative methodologies, new interpretation of previously accumulated material, creative use of AI and meaningful contributions to knowledge" in 21.1) refers to the process of promoting valuable research. A requirement to "researchers to document the role of AI and demonstrate their own intellectual inputs" (21.2) fosters accountability.

4.4. Reproducibility of research

Article 22 refers to methodological concerns over AI-assisted research, with requirements to documentation including "AI tools, soft-

ware versions, datasets and validation methods" (22.1) to make sure that research remains verifiable despite technological sophistication. The provision on collective use of "codes, data and methodologies to an ethically permissible degree" (22.2) balances the transparency requirements with legitimate concerns over confidentiality.

4.5. Framework of collective research

Articles 24 and 25 address collective research and intellectual property issues. The principles of "mutual respect, innovative development, transparency and ethical responsibility" provide a basis for AI-assisted research partnerships. The issue of intellectual property in line with "applicable national law and institutional policies" (25.1) under "appropriate attribution of participants" is raised where AI systems contribute to research findings.

5. Governance and Institutional Implementation

5.1. Ethics Council's architecture

Articles 26–30 address the issue of governance in order to translate the ethical principles into institutional practice. Article 26 requirement to AI Ethics Councils composed of "professors, technical specialists and students" provides for a variety of prospects in maintaining technical expertise (26.2). The Council's composition is called upon to reflect multiple views for AI governance.

The provision that Ethics Councils should be "well equipped for assessing AI research proposals including AI technology expertise, understanding of standards and ability to assess ethical issues" (26.3) addresses a need for capacity building which is often neglected in governance processes. The Council's functions include guidance with regard to implementation solutions, ethical review of proposals, strategy design, compliance monitoring and addressing complaints.

5.2. Requirements to resources and infrastructure

Ethical AI integration under Article 27 requires institutional investment while maintaining flexibility in the face of variable capacities. The priority of "equitable access, training, safe infrastructure and benefit assessment" means that integrating AI will require systematic support (27.2).

Meanwhile, requirements to resources might leave institutions with hard choices if their budget is limited or technical infrastructure poor.

5.3. Monitoring and adaptation systems

Monitoring will help to develop approaches to assessment and quality of AI governance. Tracking "baseline indicators and wellbeing of participants" as much as available resources allow demonstrates practical approaches to accountability (28.1). Feedback mechanisms such as "consultations with the community, strategy review and incident analysis" create training-focused governance systems.

A three-year review cycle involving international experts provides for a third-party validation while ensuring that governance keeps pace with technological developments. However, in view of the speed of AI progress, more frequent review cycles may be required.

5.4. Implementation and equity considerations

Articles 29 and 30 address AI implementation challenges and concerns over deepening inequality along the way. A phased approach to implementation through "awareness policies, pilot programs and integration of the organizational culture" reflects the understanding of change management (29.1). Participation of students which positions them as "partners in AI integration" follows from the principles of stakeholder involvement (29.2).

Non-discrimination provisions of Article 30 demonstrate that differences in implementation do not give rise to new inequalities while recognizing legitimate variations of institutional capacities. The provision on "alternative approaches to international cooperation" for institutions with limited resources demonstrates the commitment to the principles of accessibility and observance of ethical standards (30.2).

6. International Comparison Analysis

6.1. Harmonizing with the UNESCO's Principles

Harmonizing the Code with the UNESCO Recommendation is tantamount to a detailed guidance to implement AI specifically for education purposes. While the Recommendation establishes broad princi-

ples for AI development across different sectors, the Code provides the mechanisms to address challenges and opportunities in a single area, that of education.

The Recommendation's principles (human dignity, human rights, equality and non-discrimination) are set out in the Code's fundamental principles and operating frameworks. However, the Code does not go beyond harmonization while offering implementation mechanisms that address unique educational contexts. The Code's approach to transparency and explainability adapts the UNESCO's principles to educational needs by specifying different explanatory levels that stakeholders may need.

6.2. Mainstreaming human rights

The Code's reliance on international law, especially on the Universal Declaration of Human Rights, provides for the ethics of AI use in education to be viewed from the perspective of human rights rather than of administrative issues. Recognizing education as a fundamental right provides the brickwork for the Code's accent on equitable access and non-discrimination which is translated into assurance that AI integration will not create additional barriers to education.

6.3. Harmonizing with data protection regulation

The Code's harmonization with GDPR principles as adapted to educational contexts highlights progress in understanding the value of protecting data that may be used by AI in education. The principles of lawfulness, transparency, equity, restricted purpose, minimization of data, accuracy, limitation of data storage and accountability formulated in the GDPR are reflected in the Code's data protection provisions. However, the Code goes beyond regulatory compliance by addressing educational implications of data protection requirements.

6.4. Mainstreaming academic integrity standards

The Code's mainstreaming of fundamental values of the International Center for Academic Integrity — trust, equity, respect, responsibility, valor — into specific AI guidance signals progress in understanding academic integrity in technological contexts. Rather than regarding AI as fundamentally disruptive for academic integrity, the Code demonstrates how the established values can apply to new technological circumstances.

7. Critical Assessment: Strengths and Constraints

7.1. Strengths

The Code of AI Ethics has a number of merits to set it apart from prior efforts to govern education technologies. Comprehensive integration of ethical principles into a practical AI implementation guidance creates a topic both philosophically coherent and detailed [Barthwal A., 2025: 22]. Extending beyond the prohibition-permission dichotomy, the education-centric approach sets the stage for combining positive engagement with AI technologies to serve educational goals [Rasul T., 2024: 1].

The challenge of keeping stakeholders involved requires governance to stay responsive to community needs in supporting institutional leadership and ethical standards [Karran A.J., 2024: 2]. Methodological innovations, especially a parallel AI-assisted system for assessment of academic performance, constitute an input to educational assessment approaches [Deep P., 2025: 3]. Governance architecture, especially the Ethics Council model, creates institutional mechanisms specifically designed to regulate AI-related challenges.

7.2. Implementation challenges and constraints

Despite the Code's strengths, there are significant implementation challenges to be carefully handled by institutions. The Code's comprehensive nature assumes building of institutional capacity for AI implementation. This capacity includes: technical infrastructure, capacity building programs for professors, support service for students and governance mechanisms — things that might overstretch currently available resources of many education institutions.

The requirements to resources to implement AI are significant and permanent: it is not one-time investment. Institutions should develop technical infrastructure capable of supporting AI integration as well as safety and confidentiality standards. The teaching staff need in vocational advancement and development of competencies required for AI integration, while students are interesting in support services for AI literacy. Governance systems require expertise and ongoing attention to the problems they face [Xu X., 2025: 7].

Governance challenges that transformation of the institutional culture entails should not be downplayed [Bond M., 2024: 41]. A shift to-

wards education-centric approaches requires changes to how institutions approach technology governance. It is always important how academic integrity is taught to students and how they understand their duties to learn and develop [Felani H. et al., 2024: 11214].

7.3. Methodological Concerns

Since the Code's parallel assessment methodology is innovative, a number of concerns merit attention. The impact of AI/human input analysis depends on advanced detection devices which are not available to all institutions [Kamali J., Alpat M. et al., 2024: 98], while interpretation of findings depends on expertise which may not exist at many of them. The likelihood of falsely positive or negative findings revealed by AI is able to result in unfair advantages or disadvantages for students.

Hopes for documentation and self-accountability as required by transparency may be inadequate for accurate analysis of AI use [Ateriya N., 2025: 4–5]. Students might fail to understand what constitutes "appropriate documentation" or might be encouraged to underreport AI use to avoid penalties while professors might lack adequate expertise for accurate assessment of AI-assisted projects.

7.4. Scalability and adaptation Issues

The Code's comprehensive approach might impede scalability. High resource requirements, a need for expertise, institutional capacity requirements will restrict the use of its provisions by under-resourced institutions, only to exacerbate rather than address the inequality of access to education and undermine its quality.

The model of voluntary adoption within institutional autonomy may contain the Code's impact on AI governance in education. In the absence of regulatory requirements, structures and incentives its adoption may be limited to institutions already committed to ethical AI integration thereby restricting the Code's scope for a wider impact.

Cultural and institutional diversity in global education systems will require much effort to adapt the Code's principles and implementation mechanisms. Legal frameworks vary significantly across jurisdictions, only to create room for conflict between the Code's requirements and national or local regulations.

7.5. Need for future research

The Code's implementation expands the opportunities for studying the level of governance, technological impact and educational outcomes, something that can considerably help to integrate AI into education. Multidisciplinary studies of its implementation in different institutional contexts could be valuable for the theory and practice of governance.

Empirical validation of the Code's assessment methodologies is necessary for identifying how efficiently they support academic integrity where AI is involved. Studies of the impact of different implementation approaches can focus practice on dissemination of knowledge via institutions and cultural contexts.

Conclusions

The AI Code of Ethics for education developed at the Tashkent State Law University is a meaningful contribution to education technology governance as it puts in place comprehensive approaches to match innovation with responsibility, institutional needs with personal rights and global principles with local adaptation. The Code is an attempt to make arrangements for systematic ethical governance for AI at education institutions.

The Code's shift from prohibition makes up its primary contribution towards approaches to governance. In positioning AI as a tool to be mastered rather than a threat to be contained, it enables education institutions to harness transformative technologies while supporting ethical standards. This approach recognizes both the extent of AI dissemination and possibility for its ethical implementation through systematic attention to development of competencies and ongoing learning.

Education-focused approach transforms the potentially antagonistic relations of students and institutions into a collaborative partnership aimed at learning and development. Instead of "monitoring compliance" by identifying violations, the Code provides guidance how competency and mentorship development could serve education goals while supporting integrity.

The Code's methodological approach, especially a parallel AI-assisted system for assessing academic performance, attempts to address assessment challenges of educational environment using AI. Qualitative

assessment criteria focused on in-depth understanding, quality of critical thinking, technological integration, creative originality and assessment of AI input, create a framework for assessing learning through AI.

Meanwhile, empirical validation of implementation experience is required for these methodologies to be useful. Delimitating AI and human contributions might prove to be more difficult than envisaged by the Code although it requires ongoing improvement and adaptation.

The architecture of governance, especially the AI Ethics Council model, puts in place institutional mechanisms designed to address AI-related challenges. A mix of consultative and supervisory functions in the Council assumes accountability while supporting institutional autonomy and academic freedom.

Integration of ethical review processes for AI implementation projects strives to ensure systematic discussion of ethical implications of technologies before they are deployed. However, to what extent these mechanisms are effective depends on institutional commitment and distribution of resources that might not be available everywhere.

The Code's likely global impact lies in its detailed approach to introduction of international principles. It envisages mechanisms to address educational challenges harmonized with international standards. The Code's accent on adaptation rather than wholesale adoption enables implementation in supporting fundamental ethical principles.

However, the voluntary adoption principle and requirements to resources for implementation may constrain its impact. In the absence of regulatory framework or incentive structures the Code's adoption may be limited to institutions already committed to ethical AI integration.

Implementing the Code will facilitate understanding of effective governance in a rapidly evolving technological landscape. Adaptive and review mechanisms will promote learning systems that keep pace with technological progress while supporting commitment to ethics.

Comprehensive integration of stakeholder views and adaptability to varying institutional capacities present models of governance approaches that could inform international efforts to develop ethical requirements for innovative technologies. However, future challenges of practical implementation and rapid pace of technological change will put the Code's adaptability and usefulness to test.

The Code is a major effort to regulate the challenges of AI integration into education through comprehensive ethical governance. Though

the Code envisages potential benefits for education institutions willing to integrate AI technologies responsibly, its value is conditional on successful implementation and empirical validation of its approaches. The Code contributes to further discussions of ethical AI governance in education by establishing a framework away from prohibitive approaches in recognition of challenges which result from balancing technological innovations with educational values.

References

1. Ateriya N. et al. (2025) Exploring Ethical Landscape of AI in Academic Writing. *Egyptian Journal of Forensic Science*, vol. 15, no. 36, pp. 1–9. https://doi.org/10.1186/s41935-025-00453-1

2. Barthwal A., Campbell M. et al. (2025) Privacy Ethics Alignment in AI: A Stakeholder-Centric Framework for Ethical AI. *Systems*, vol. 13, no. 6, pp. 1–22. https://doi.org/10.3390/systems13060455

3. Bond M., Khosravi H., De Laat M. (2024) A Meta Systematic Review of Artificial Intelligence in the Higher Education: a Call for Increased Ethics, Collaboration, and Rigor. *International Journal of Educational Technology in Higher Education,* vol. 21, no. 4, pp. 1–41. https://doi.org/10.1186/s41239-023-00436-z

4. Deep P., Edgington W. et al. (2025) Evaluating the Effectiveness and Ethical Implications of AI Detection Tools in Higher Education. *Electronics*, 23 p. https://www.mdpi.com/2078-2489/16/10/905.

5. Felani H. et al. (2024) The Influence of Learning-Oriented Organizational Culture on Innovation and Firm Performance in The Creative Industry. *Eduvest-Journal of Universal Studies*, no. 12, pp. 11214–11225.

6. Johnston H., Wells R. et al. (2024) Student Perspectives on the Use of Generative Artificial Intelligence Technologies in Higher Education. *International Journal of Education Integration*, vol. 20, no. 2, pp. 1–21. https://doi.org/10.1007/s40979-024-00149-4

7. Kamali J. et al. (2024) AI Ethics as a Complex and Multifaceted Challenge: Decoding Educators' AI Ethics Alignment through the Lens of Activity Theory. *International Journal of Educational Technology in Higher Education,* no. 62, pp. 96–99. https://doi.org/10.1186/s41239-024-00496-9

8. Karran A.J., Charland P. et al. (2025) Multi-stakeholder Perspective on Responsible Artificial Intelligence and Acceptability in Education, 28 pp. https://www.nature.com/articles/s41539-025-00333-2#citeas

9. Koshel A.S., Kuzminov Ya. I. et al. (2025) Experience of Foreign and Domestic Regulation of Digital Platform Activities: Searching for Regulatory Optimum. *Pravo. Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 18, no. 2, pp. 4–58 (in Russ.) DOI: 10.17323/2072-8166.2025.2.4.58.

10. Luckin R., Holmes W. et al. (2016) Intelligence Unleashed: an Argument for AI in Education. London: Pearson, 58 p.

11. Perkins M. (2023) Academic Integrity Considerations of AI Large Language Models in the Post-Pandemic Era: Chat GPT and beyond. *Journal of University Teaching & Learning Practice,* vol. 20, no. 2, pp. 1–17.

12. Rasul T., Nair S. et al. (2024) Enhancing Academic Integrity among Students in Gen AI Era: A Holistic Framework. *The International Journal of Management Education,* vol. 22, no. 3, article 101041.

13. Rodgers D.J. (2012) The Social Media Dilemma in Education: Policy Design, Implementation and Effects. PhD Thesis. Los Angeles: University of Southern California, 193 p.

14. Weber-Wulff D. et al. (2023) Testing of Detection Tools for AI-generated Text. *International Journal for Educational Integrity*, vol. 19, no. 1, pp. 1–39.

15. Xu X., Meng F., Gou Y. (2025) From Theoretical Navigation to Intelligent Prevention: Constructing a Full-Cycle AI Ethics Education System in Higher Education. *Educational Sciences*, vol. 15, no. 9, pp. 1–18. https://doi.org/10.3390/educsci15091199

Information about the authors:

S.S. Gulyamov — Doctor of Sciences (Law), Professor.
I.R. Rustambekov — Doctor of Sciences (Law), Professor.

The article was submitted to editorial office 22.09.2025; approved after reviewing 17.11.2025; accepted for publication 12.12.2025.

Legal Issues in the Digital Age. 2026. Vol. 7, no. 1.
Вопросы права в цифровую эпоху. 2026. Том 7. № 1.

Digital Age: Labour Law

Research article
JEL: K31
UDC: 352.075
DOI:10.17323/2713-2749.2026.1.71.95

Social and Labour Rights in Context of Platform Employment: the Case of Passenger Transportation by Private Taxi

Yulia D. Zhukova[1], Anna S. Podmarkova[2]

[1,2]National Research University Higher School of Economics, 20 Myasnitskaya Str., Moscow 101000, Russia,

[1]Julia-jukova@yandex.ru, https://orcid.org/0000-0002-4455-1096

[2] apodmarkova@hse.ru, https://orcid.org/0000-0003-4549-4588

Abstract

The digitalization of the economy has given rise to fundamentally new forms of labor and employment organization, among that are platform employment and self-employment. The lack of legislative definitions and full-fledged regulation of these phenomena actualize distinguishing of labor and civil law relations. Also the consideration of the legal status of platform employees and self-employed individuals, determination of the need to provide them with social and labor rights and guarantees. Especially considering the existence of different types of platforms and special regulation in certain areas of activity. The article examines these issues on the example of regulating passenger and baggage transportation by passenger taxi. The authors analyze the directions of regulation of non-standard forms of employment and models of regulation of platform employment and self-employment that have developed in world practice. Also, the regulation of non-standard forms of employment proposed by the Russian legislator and the existing regulation of the platform economy and passenger and baggage transportation by passenger taxi. The authors come to several conclusions. First, the legislator's choice of a model for the existing regula-

tion based on the entrepreneurial nature of the activities of self-employed carriers and other platform employees. Secondly, the legislator's awareness of the need to provide these and other individuals with non-standard employment with certain social and labor rights and guarantees. Thirdly, about the possibility of future differentiation of regulation by introducing the category of «dependent self-employed».

Keywords

platform employment; self-employed citizens; Tax on Professional Income; passenger taxi transportation; owner of aggregator of information about goods (services); responsibility in the field of passenger taxi transportation.

Acknowledgements: The article was prepared with using Consultant Plus reference legal system.

For citation: Zhukova Yu.D., Social and Labour Rights in Context of Platform Employment: the Case of Passenger Transportation by Private Taxi. *Legal Issues in the Digital Age,* vol. 7, no. 1, pp. 71–95. DOI:10.17323/2713-2749.2026.1.71.95

Introduction

The digitalisation of the economy has led to the emergence of new forms of work and employment. Among these, platform employment occupies a prominent place. This involves indirect interaction between service providers and customers through digital platforms that act as market organisers and aggregators of demand and supply. This phenomenon poses a challenge to traditional labour and civil-law models, requiring legal adaptation.

An important step towards legitimising flexible forms of economic activity in Russia appeared to be introduction of a provision into Paragraph 2, Clause 1 of Article 23 of the Civil Code of the Russian Federation (hereinafter — CC), that allows certain types of entrepreneurial activity to be carried out without state registration as a self-employed entrepreneur under certain conditions. Pursuant to this legal provision, Federal Law No. 422-FZ "On the Experiment to Establish a Special Tax Regime: Professional Income Tax" (hereinafter[1] — Law on PIT) was approved 27 November 2018.

As the law permits entrepreneurial activity without state registration as a self-employed entrepreneur and as there is no legal concept of a

[1] SPS ConsultantPlus

"self-employed individual", a new category of business entities with an uncertain legal status and ambiguous classification of their activities has emerged.

A self-employed individual is not a hired worker, which is the defining feature of self-employment. They cannot hire workers or engage third parties to fulfil their obligations under civil contracts. There are also restrictions on the types of activities in which PIT can be applied, and a cap on the amount of income that is taxable under PIT (2.4 million RUB per calendar year)[2].

This taxation scheme cannot be applied to activities where registration as a self-employed entrepreneur is mandatory under federal law (Part 6, Article 2 of the Law on PIT). Until 2022 [3] these included taxi transport.

On the one hand, Law 580-FZ recognises the right of self-employed individuals to obtain a license to operate taxis as of 01 September 2023, alongside self-employed entrepreneurs and legal entities. This allows us to hypothesise that the Russian Federation Civil Code validly qualifies their activities as entrepreneurial. However, this raises questions about the specific nature of their activities and of the need to establish a special legal regime for them as part of taxi rules and regulations. This would include the need to grant them certain social and labour rights and guarantees.

In this regard, it would be useful to consider the details. How Law 580-FZ stipulates the admission of self-employed individuals to taxi services? This would allow to analyse how relations in this area are organised and determine whether the new regulation takes the specific nature of such persons' activities into account by establishing a special regime for self-employed individuals as opposed to other carriers and drivers working for hire. It is also important to analyse the distribution of liability between the parties involved in taxi services in order to determine the nature of self-employed individuals' work as carriers. After we have determined the Russian legislator' approach to regulating taxi traffic and examined global practices for regulating non-standard forms

[2] Part 7, Art. 2, Paragraphs 5, 8; Part 2 Art. 4, Law on PIT.

[3] Before entry into force of Federal Law No. 580-FZ of 29 December 2022 "On the Organisation of Passenger and Luggage Transport by Taxis in the Russian Federation, on Amendments to Certain Legislative Acts of the Russian Federation and on Recognition as No Longer Valid of Certain Provisions of Legislative Acts of the Russian Federation" (hereinafter — Law 580-FZ).

of employment, as well as models for regulating platform employment and self-employment, and have analysed the proposed regulation of non-standard forms of employment in the Russian law and the existing regulation of the platform economy, we would be able to conclude whether it is necessary and feasible to assign social and labour rights to self-employed carriers.

1. Obtaining a License for Taxi Service

Self-employed carriers must obtain a license for this activity[4] and work personally.[5] That is to say, they must simultaneously meet the requirements of both Article 11 of Law 580-FZ for carriers and Article 12 of the same Law for taxi drivers. Failure to meet the requirements for taxi drivers is grounds for refusal of a license for carrier operations (Para 3, Part 9 of Article 5 of the Law).

Compared to the previous regulation, the legislator has significantly increased the number of requirements for taxi drivers.[6] Essentially, it has established three categories of requirements for self-employed individuals, similar to those that exist for hired drivers and self-employed entrepreneurs in the transport industry. These categories are based on physical fitness, knowledge and legal obedience, and do not differentiate depending on the nature of the activity or the legal status of these individuals.

The legislator followed a slightly different approach in setting out the requirements for self-employed individuals acting as carriers. Like other carriers, a self-employed carrier independently complies with all legal requirements, unless they have assigned some of these to another party under a contract in the respective field (Parts 4 and 5 of Article 11 of the

[4] The license is granted by an authorised agency of the Russian Federation entity in whose territory the applicant resides (Part 1, Article 5 of Law No. 580-FZ). In Moscow, this is Department for Transport and Development of Road and Transport Infrastructure (para. 2.3.1 of the Administrative Regulation for the Provision of Moscow State Service, approved by Resolution of the Government of Moscow No. 1665-PP. 29 August 2023).

[5] If a self-employed person transfers the management of a vehicle to another person for the purpose of transport under a taxi charter contract, this constitutes grounds for revoking the license (Para 7, Part 4, Article 8 of the Law).

[6] Subpara 2, Part 16 of Art. 9 of law No. 69-FZ dated 21 April 2011 "On Amendments to Individual Legislative Acts of the Russian Federation" as amended 21 December 2021. On 01 September 2023, the article lost its validity.

Law). These other parties are primarily the taxi booking service, i.e. a self-employed entrepreneur or a legal entity authorised to receive orders for taxis from potential passengers and/or transfer them to potential carriers, with the subsequent conclusion of a public charter contract.

The legislator has made it mandatory for self-employed individuals to sign a contract with an Internet-based taxi booking service[7] in order to be admitted to transport passengers by taxi. Self-employed persons must conclude the contract before obtaining a license (Art. 20, Parts 2, 3 of the Law). The absence of a contract is grounds for suspending the license (Subpara 3, Part 1 of Art. 8 of the Law). When a contract with a self-employed person is terminated, the taxi booking service must notify the relevant authority (Subpara 14, Part 3 of Art. 19 of the Law).

Thus, the special feature of obtaining a license for self-employed persons to carry passengers and luggage in a taxi and entering this market is the use of a "technical intermediary" and the mandatory conclusion of an agreement with this intermediary. According to the explanatory note to the draft which became the Law, the legislator initially chose this model for the organisation of transport relations in order to entrust the taxi booking service with the responsibility of collecting and transmitting information on self-employed carriers to authorised agencies[8] or to relevant information registers[9]. At their discretion, the parties to such relationships can redistribute the duties of compliance with statutory requirements for carriers and the liability for failure to comply among themselves on the basis of a contract.

Unlike other carriers, self-employed individuals may see a greater reduction in the list of requirements they have to comply with, as these will be transferred to taxi booking services. Regarding the requirements that have not been transferred, the legislator does not allow self-employed carriers to comply with them as an act of goodwill, but enforces compliance by charging taxi booking services with the relevant obligations.

For example, the taxi booking service must not transfer orders to a self-employed individual if they do not meet the requirements set out in Law No. 580-FZ for taxi drivers regarding the completion of the motor

[7] Which means it is in actual fact an operator of a digital intermediary platform.

[8] Executive agencies of the Russian Federation entities that carry out regional state control (supervision) in the field of passenger and luggage transport by taxis.

[9] In particular, to the regional register of taxi carriers.

vehicle trip ticket[10] (if the booking service is entitled to receive notifications about such cases from the respective information systems) (Subpara 13, Part 8 of Art. 19). The taxi booking service must not transfer orders to a self-employed carrier if fulfilling the orders would result in a violation of the Government's requirements for the period in question.[11] This also applies if such information is not provided to the booking service or if information is received about the driver violating the aforementioned requirements (Subpara 3, Part 8).

On the basis of available monitoring data, the booking service must ensure compliance with the working hours, rest periods and driving times prescribed by federal legislation (Subpara 15, Part 3, Article 19). It must not transfer orders to a self-employed driver-carrier if they exceed the above norms. This Law demonstrates that the legislator takes into account the fact that self-employed individuals must work personally, and that the working routine of a self-employed carrier differs in certain respects from that of other carrier-entrepreneurs who have hired drivers.

At the same time, self-employed carriers are independent from the financial and organisational point of view, unlike drivers hired by carriers (e.g. they determine their working hours, with account for existing regulations), and they bear the risks associated with taxi operations.

With regard to financial independence, the legislator has stipulated that a self-employed individual does not have to own a vehicle suitable for taxi operations. Therefore, the legislator has set out that such an individual may receive a vehicle for this purpose from either a legal entity or another self-employed individual, on the basis of a contract for the transportation of passengers and baggage by taxi (Part 6, Article 5 of the Law).

The subject matter of the contract consists of five material conditions (Article 13). These include providing a car for use as a registered taxi, enabling the driver to undergo pre- and post-trip medical examinations

[10] Document used to record and control the operation of the vehicle and the driver (Subpara 14, Para 1, Art. 2 of Federal Law No. 259-FZ. 8 November 2007 "Charter of Road Transport and Urban Land Electric Transport").

[11] This is the time interval during which a taxi order is transferred from the taxi booking service to the taxi driver. This must be within the working hours, rest time, and vehicle driving time limits established by the Russian Federation Government (Government Decree No. 872 of 30 May 2023 "On the Approval of Requirements for the Period of Transfer of Taxi Booking Orders from Taxi Booking Services to Taxi Carrier Services").

and pre-trip inspections of the taxicab's technical condition, and providing car maintenance and repair services. The customer must notify the authorised agency or the regional information system of the transfer of a taxi for use by the individual in question, as well as the period of such transfer. Furthermore, the customer must notify the regional information system if, in their capacity as a taxi driver, they have taken advantage of the opportunity to undergo a medical examination or have the technical condition of the car checked, or if they have omitted this opportunity.

Failure to meet the latter three conditions by the person in question is grounds for excluding vehicle information from the regional register of taxis (Part 5, Article 10).

It is noteworthy the law does not provide a detailed regulatory mechanism for contracts for the provision of taxi services or for taxi booking services. This may result in difficulties when selecting applicable legal norms. Probably, one must agree with V.V. Toschchenko that "the question of the legal classification of a taxi contract under a car rental agreement is highly relevant," [12] and that "qualifying it exclusively as a contract for the provision of paid services would enable the application of provisions relating to a unilateral refusal to provide services and to cases where the contract cannot be performed." He also states that "at present, there is every reason to speak of the mixed nature of the contract that contains elements of a rental contract and a contract for the provision of paid services" [Toschchenko V. V., 2023: 16–19].

Insufficient regulation of these contracts will not solve practical issues, such as taxis not arriving or arriving late, or access to the taxi booking service being suspended when a driver's rating falls below a certain level. [13] Moreover, it may also result in new problems relating to applicable law when disputes over these contracts are adjudicated in court.

---

[12] He is referring to the application of the rules regarding the lessor's liability for defects in the leased property; for breach of duty to warn about third-party rights in the property; of the rules on early termination of the contract, extension of the contract, and exercise of the priority right to conclude the contract for a new term.

[13] In practice, courts predominantly support taxi booking services, citing their right to control service provision under the contract. Examples include the Appeal Ruling of the Moscow City Court of 24 August 2021 in case No. 33-33780/2021, and Ruling of the Second Court of Cassation of General Jurisdiction of 15 February 2022 in case No. 88-681/2022. The grounds for restricting access to the taxi service and for terminating the contract with the booking service should probably be regulated by law.

At present time, of course it is difficult to predict the scale of this because, on the one hand, self-employed entrepreneurs and legal entities for whom this activity will be either their main or additional business in relation to taxi transport will be able to conclude a contract for the provision of taxi services.[14] However, due to the absence of a statutory ban, self-employed individuals will still have the opportunity to enter into other contracts for the temporary use and operation of vehicles for use as taxis, including contracts with individuals, as was the case before the Law came into force.

Therefore the legislator permits various options for establishing the property base for the activities of self-employed carriers. At the same time, receiving property for use in a taxi service from professional entrepreneurs entails, by analogy with taxi booking services, imposing on these persons the fulfilment of requirements originally intended by the legislator for self-employed carriers. The possibility of transferring the fulfilment of legal requirements to other parties distinguishes the regime governing the activities of self-employed persons from that governing other carriers.

Another distinguishing factor is the validity period of the license required to carry out this activity. According to Law No. 580-FZ, individuals are granted a license for a period of five years, unless they specify a shorter period in their application (Part 4, Article 5). Legal entities and self-employed entrepreneurs are granted permission for a period established by a regulatory act of the federal constituent entity, but not for less than five years. Self-employed individuals have the right to choose the validity period of the license on condition that they personally drive the taxi and that the PIT regime itself and the activities carried out under it are experimental in nature.

The introduction of a special legal regime for self-employed carriers neither refutes nor confirms the hypothesis that the activities of self-employed persons can be classified as entrepreneurial under the Civil Code. Therefore, there is an urgent need to analyse the nature of their activities and legal status in order to determine their liability and identify how these activities relate to the liability of other participants in taxi transportation.

[14] The ruling of the Fourth Court of Cassation of General Jurisdiction of 21 May 2024 in case No. 88-15341/2024 indicates that such agreements are concluded.

2. Distribution of Responsibility among the Parties

So, Law No. 580-FZ does not explicitly define taxi passenger transportation as a form of self-employment. However, by prohibiting unlicensed individuals from carrying out this activity, the law makes it clear that transporting passengers and luggage by a vehicle for hire may constitute a business activity (Part 7 of Article 3).[15] The same provision also prohibits disseminating information offering transportation without a valid license, except for on-request transportation and other cases provided for by federal law. Booking services are obliged to check the register of carriers and the register of taxis daily for information on licenses, as well as for suspensions and cancellations (Subpara 7, Part 3 of Article 19). The law stipulates that booking services can only offer orders to individuals who hold a licence.

The issue of transporting passengers and luggage by unlicensed taxicabs is closely linked to the question of liability for harm caused to passengers during such transportation. Essentially, it comes down to distributing liability between drivers, carriers and taxi booking services. The grounds for the latter's liability and the limits of such liability must also be considered.

As early as 2018, the Judicial Panel for Civil Cases of the Supreme Court of the Russian Federation has ruled in Ruling No. 5-KG17-220 of 9 January 2018 that a taxi booking service could be held liable as a provider of passenger search services. According to Paragraph 1 of Article 1005 of the Russian Federation Civil Code, "in a transaction between an agent and a third party on behalf of and at the expense of the principal, the agent becomes liable, even if the principal was named in the transaction or entered into direct relations with the third party for the performance of this transaction." [16]

The panel reached this decision despite the fact that the driver was in employment of a self-employed entrepreneur who was the carrier and owner of the vehicle. The owner worked with the booking service under an information services agreement, whereby the customer-carrier was

[15] Starting from 1 September 2024, Article 5 of Federal Law No. 259-FZ of 08 November 2007 "Charter of Motor Transport and Urban Land Electric Transport," explicitly classifies the transportation of passengers and luggage by taxis as a type of entrepreneurial activity.

[16] That is, the party to an agency agreement that instructs the other party (the agent) to perform legal and other actions.

liable for any damage caused to third parties during with the transportation of clients. The court ruled that entering into a relationship with the principal's employee (the taxi driver) or having the ability to obtain information about the principal did not affect the agent's obligations who entered into a relationship with a third party on their own. Consequently, the driver, the carrier and the taxi booking service were held liable and were to pay compensation for moral damage and reimbursement of funeral expenses to the relatives of the deceased passenger.

In holding the ordering service liable, the court took into account that its main activity, as stated in the organisation's charter and in the information from the consumer protection service and the social insurance fund, was to provide taxi services alongside information services. The court also considered the company's advertising materials promoting taxi services, as well as a screenshot of a text message sent by the company to the customer's mobile phone indicating the price of the service and thanking them for using it. The plaintiffs believed that, by offering taxi services and accepting orders, the booking service was acting on its own behalf.

The above position (albeit without reference to Article 1005 of the Civil Code) was afterwards developed in Para 18 of Resolution No. 26 of the Plenum of the Supreme Court of the Russian Federation of 26 June 2018 "On Issues Concerning the Application of Legislation on Contracts for the Carriage of Goods, Passengers and Luggage by Road and on Contracts for Freight Forwarding." The essence of this position is as follows: the taxi booking service is liable to the passenger for any damage caused if a contract of carriage is concluded on its behalf, or if a good-faith individual customer might have been led to believe, through advertising signboards, information on the website, or correspondence between the parties when concluding the contract, for example, that the contract of carriage is being concluded directly with this service and that the actual carrier is an employee of, or a third party engaged by, this service to perform carriage obligations. Thus, the conditions for holding taxi booking services liable have been clarified by the explanations provided by the Supreme Court.

Almost immediately after the explanations were published, amendments were made to the Consumer Protection Law[17] that introduced the

[17] Federal Law No. 250-FZ of July 2018 "On Amendments to the Law of the Russian Federation "On Protection of Consumer Rights" (hereinafter — Consumer Protection Law).

concept of an "aggregator of information about goods and services." The changes established the obligation of the owner of an aggregator to provide consumers with information about themselves and the seller of the goods, and also stipulated how responsibility for inaccurate information about goods and services would be distributed between them. According to the Consumer Protection Law, the owner of an information aggregator[18] is not liable for losses incurred by a consumer as a result of providing inaccurate or incomplete product (service) information, provided they do not alter the information provided by the seller (contractor) and included in the contract offer. It is the seller (contractor) who is responsible for performing the contract and complying with consumer rights, not the owner of the information aggregator, unless otherwise stipulated in their agreement or arising from the nature of their relationship.

The introduction of these provisions led courts to consider recognising taxi booking services as information aggregators. Until around mid-2022, courts ruled that booking services should be held administratively liable under Part 2, Article 14.7 of the Code of Administrative Offences of the Russian Federation (CAO) for misleading consumers about the quality and safety of transport services by failing to inform them whether or not a driver had a licence for taxi operations.[19] However, in several rulings in Autumn 2022, the courts did not recognise booking services

[18] The Consumer Protection Law defines an "information aggregator" as an organisation, regardless of its legal form, or a self-employed entrepreneur who owns computer software and/or a website and/or an Internet page, and who provides consumers with the opportunity to familiarise themselves simultaneously with the seller's (contractor's) offer to conclude a contract for the sale of a specific product (service) (contract for the provision of services for remuneration), conclude a contract of sale (contract for the provision of services for remuneration) with the seller (contractor), and make an advance payment for the specified goods (services) by cash payment or transfer of funds to the owner of the aggregator, in accordance with applicable non-cash payments methods (Paragraph 13 of the preamble to the Consumer Protection Law). From 1 October 2026, the operator of an intermediary digital platform will be equated with an information aggregator for the purposes of this Law.

[19] Ruling of the Arbitration Court of the East Siberian District of 02.03.2020 F02-443/2020 in case No. A10-4822/2019; Arbitration Court Ruling of the North-West Federal District of 17 June 2020 No. F07-6188/2020 in case No. A56-111312/2019; Arbitration Court of the East-Siberia District of 26 January 2021 No. F02-6845/2020 in case No. A10-2634/2020; Arbitration Court Ruling of the Far-East District of 22 September 2021 No. F03-4427/2021 in case No. A73-16600/2020; Arbitration Court of the Central District of 23 December 2021 No. F10-5703/2021 in case No. A68-2686/2021; Ruling of the 9th Arbitration Court of Appeal of 1 June 2022 No. 09AP-24510/2022-GK in case No. A40-285054/2021.

as owners of information aggregators or as entities liable under Part 2 of Article 14.7 and Part 1 of Article 14.8 of the CAO.[20] According to the decision of the Moscow District Court of Appeal, "the company does not meet the definition of an information aggregator, since the mobile application does not allow to effect advance payments; does not allow carriers to post offers to conclude charter contracts; or contractors/consumers to conclude contracts for the provision of paid services (of transportation)".[21]

However, the Supreme Court has disagreed with the lower courts' position in the absence of changes to the Code of Administrative Offences and the establishment of liability for booking services that transfer orders to persons without a transport license. The Court assumes that the booking service, "by informing the public about the possibility of obtaining the service, by accepting the relevant applications, by forming a database of these applications, and by notifying consumers of the receipt of applications from carriers, creates the impression among consumers that the service of transporting passengers and luggage in a taxi will be provided by a person authorised to carry out such activities."[22] Thus, failure to inform consumers that the service may be provided by someone without the necessary licenses required to carry out this type of activity constitutes grounds for liability under Part 2 of Article 14.7 of the Code. The Supreme Court holds that lower courts must establish whether the company has the status of an aggregator of information about goods and services.[23]

---

[20] Ruling of the Moscow Region Arbitration Court of 31 October 2022 No. F05-26986/2022 in case No. A40-37711/2022 (repealed), Ruling of the 9th Arbitration Court of Appeal of 14 November 2022 No. 09АП-61837/2022 in case No. A40-94657/2022 (repealed).

[21] Ruling of the Moscow Region Arbitration Court of 14 February 2023 No. F05-839/2023 in Case No. A40-94657/2022 (The ruling was overturned by Ruling No. 305-ES23-8620 of the Judicial Panel on Economic Disputes of the Supreme Court of Russia of 30 August 2023 in case No. A40-94657/2022).

[22] Ruling of the Moscow Region Arbitration Court of 31 May 2023 No. A40-37711/2022, and No. 305-ES23-8620 of 27 July 2023 in Case No. A40-94657/2022.

[23] Ruling of the Judicial Panel on Economic Disputes of the Supreme Court of Russia of 13 July 2023 No. 305-ES22-29622 in case No. A40-37711/2022, of 30 August 2023 No. 305-ES23-8620 in case No. A40-94657/2022. Lower courts began to follow this position when reconsidering these cases (Ruling of the 9th Arbitration Court of Appeal of 25 April 2024 No. 09AP-6572/2024 in case No. A40-37711/2022, dated 21 May 2024 No. 09AP-5451/2024 in case No. A40-94657/2022).

There are several underlying reasons for the different ways to classifying taxi booking services as owners of information aggregator. Firstly, due to freedom of contract, owners of information aggregators can choose how to build relationships with sellers of goods (service providers) and their buyers (customers). Many scholars have noted it [Ivanov A.A., 2017: 145–156]; [Belov V.A., 2022: 68 –82]. This is not confined to taxi booking services. As A.A. Ananyeva writes, "Various forms of interaction between services and direct carriers may be in demand and relevant. There is no point in limiting such forms of interaction as long as passengers' right to receive reliable information about direct operators is not violated, and different service models are not confused" [Ananyeva A.A., 2020: 20–23]. One more researcher, L.V. Kuznetsova notes that, in practice, booking services have adopted a model of providing information services — that is to say, the role of "intermediaries in the economic sense"– whereby they "create only the technical possibility of placing information and concluding a transaction, but do not participate in it as a party, agent, commission agent or representative" [Kuznetsova L.V., 2019: 39–65]. Ultimately, neither the Supreme Court nor the legislature have agreed to this attempt to be absolved of responsibility. Scholars researching legal doctrine continue to analyse the legal nature of the relationship between taxi booking services and carriers [Skvarko U.A., 2024: 51–55].

Secondly, the concept of an "information aggregator" complicates the qualification process because it requires all characteristics to be present simultaneously. Due to its universality, it does not take into account the specifics of placing orders for taxi transportation. For example, S.M. Mironova and D.I. Kozhemyakin point out that, unlike commodity aggregators, "consumers do not choose the driver who will provide them with the service; in many respects, therefore, the aggregator determines the terms of the contract" [Mironova S.M., Kozhemyakin D.I., 2022: 11–18].

Thirdly, linking the liability of the aggregator owner to the communication of inappropriate information reduces the qualification's relevance. Prior to the entry into force of Federal Law No. 580-FZ, and before the Supreme Court of Russia had stated its position, some lower courts ruled that, in the absence of a legally established obligation or technical capability for booking services to verify the existence of a license for taxi operations, the services could not be accused of providing passengers with inaccurate, incomplete or misleading information.

Finally, the absence of a unified doctrinal opinion covering the possibility of holding them liable to consumers prevents from qualifying them

as owners of information aggregators. L.V. Kuznetsova believes that "attempting to shift all or part of the liability for transactions carried out by users of relevant internet services/platforms to e-commerce aggregators is the wrong approach" [Kuznetsova L.V., 2019: 39–65]. E.D. Suvorov believes that "there are sufficient arguments in favour of the aggregator owner's liability to the consumer." In his opinion, "the question of what model such liability should be based on—in addition to the liability of the goods owner under the surety model or the liability of the aggregator as a party to the contract—should be the subject of a separate study" [Suvorov E.D., 2019: 57–67]. Even before its approval, V.A. Belov analysed the provisions of the draft European Union Directive on Online Intermediary Platforms and has concluded that "establishing joint and several liability for platform operators for obligations arising from contracts concluded between suppliers and customers is, in a number of cases, a highly justified and adequate legal solution, which is confirmed by foreign and domestic case law" [Belov V.A., 2022: 116–125].

In general, a self-employed individual acting as a carrier is solely liable for any damage to a passenger's life, health or property during transportation by taxi (Part 1, Article 29 of the Law). However, exceptions to this rule apply when other parties to the carriage relationship are liable to the passenger.

3. Liability of other Parties in the Field

3.1. Liability of the taxi booking service

The taxi booking service is fully liable for any harm caused to the passenger if they were not properly informed of the carrier's name. This is consistent with the Supreme Court's approach to holding the booking service liable for a passenger's honest mistake about the carrier's identity. If the booking service fails to provide the passenger with this information, the carrier is presumed to be bound by the contract with the booking service. In this case, the self-employed carrier shall not be liable for any damage caused.

The taxi booking service is jointly liable for any damage caused by an unlicensed driver or in the event of a licence being suspended or cancelled. The booking service is not liable if it is unable to obtain information about changes in the regional register of taxi carriers, or if the authorised body fails to transfer this information to the taxi service in machine-readable form more than one day before the damage occurred

during transportation. By imposing joint liability, the legislator has reinforced the service's obligation to verify the existence of transport licences and to enforce the prohibition on transport for persons who do not hold one. The legislator's logic is clear: passengers have the right to safe, high-quality transportation for themselves and their luggage provided by a professional with the appropriate licence.[24] If they suffer any damage, they can claim compensation from the person who failed to provide them with such transportation.

The booking service bears subsidiary liability for any shortfall in compensation for actual damage to passengers, where this is not covered by the insurance pay-out for compulsory civil liability of carriers or vehicle owners under the relevant legislation. A compulsory vehicle owners' civil liability insurance contract for taxi transport is a mandatory requirement for the carrier. Additionally, Law No. 580-FZ mentions compulsory insurance agreements that cover the civil liability of carriers for harm caused to the life, health or property of passengers. (Subpara 10, Part 1 of Art, Subpara 2. Part 1, Subpara. 6 Part 4 of Art. 8 of Law No. 580-FZ).

Law No. 67-FZ has began to apply to taxi services on 1 September 2024.[25] Within 60 days of this date, carriers were required to take out compulsory third-party motor liability insurance for each vehicle listed in the regional register of taxis, and submit details to the authorised executive authority of the constituent entity.[26] Failing this, the licence will be suspended and then revoked within the legally established timeframe.

Neither the conclusion nor the subsequent termination of the contract shall release the insurer from the obligation to pay insurance compensation for insured events that occurred during the contract's term.[27] The insurer shall be entitled to claim compensation from the carrier for

[24] However, Resolution No. 09AP-19630/2022 of the 9th Arbitration Court of Appeal of 11 May 2022 in case No. A40-263181/2021 states that "the mere fact that a carrier has a license does not guarantee the safety of passenger and luggage transportation services by taxi, since the procedure for issuing licenses does not include research and assessment of factors that directly affect the safety of transportation."

[25] Federal Law No. 67-FZ of 14 June 2012 "On Compulsory Insurance of Civil Liability of Carriers for Damage to the Life, Health and Property of Passengers and on the Procedure for Compensation for Such Damage Caused During the Carriage of Passengers by Metro" (hereinafter referred to as Law No. 67-FZ).

[26] Article 4 of Federal Law No. 278-FZ of 24 June 2023 "On Amendments to Certain Legislative Acts of the Russian Federation."

[27] Part 3 of Art. 9 of Law No. 67-FZ.

insurance payments made to the passenger in the event of an insured event occurring as a result of the self-employed carrier violating the work and rest regime, or using a car with technical faults for transportation, which is prohibited. The same applies when self-employed individuals carry out transport operations while their licence is suspended or when they do not have a taxi service contract. Similarly, self-employed individuals may not carry out transportation services outside the Russian Federation constituent entity in which they have obtained a license, except in cases provided for by Law No. 580-FZ.[28] According to researchers, this regulation will protect the interests of taxi passengers [Karimullina A.E., 2023: 13–16], while preventing self-employed carriers who do not comply with the requirements of this Law from shifting their liability for harming passengers to insurance companies.

It is important to note that establishing the joint and several liability of taxi booking services does not reduce the liability of the self-employed carrier. This is because Part 3 of Article 29 of Law No. 580-FZ allows a taxi booking service to claim the full amount paid from the carrier (who is responsible for causing harm to the passenger) by way of recourse. At the same time, the law allows the fault of the taxi service to be taken into account when determining the share that can be recovered from the carrier for causing harm to the passenger.

In accordance with the law, the booking service is liable for the transfer of orders in violation of the order transfer period established by the Decree of the Government of the Russian Federation. In this case, it seems that we should be talking about administrative liability, but the necessary elements are currently lacking.

3.2. Liability of the contractor under a contract for the provision of taxi services

This liability shall apply in the event of damage caused to a passenger when self-employed individual fails to notify the authorised body or the regional taxi information system about receiving a taxi for use and well as about the duration of such provision before the commencement of the carriage of passengers and luggage (Part 4 of Article 13 of Law No. 580-FZ). Essentially, if such notification is not provided, the taxi remains in the actual possession of its owner, which makes them the liable party.

[28] Art. 19 of Law No. 67-FZ.

Liability also arises from this person's failure to fulfil their obligations regarding the technical maintenance and upkeep of the taxi. Part 4 of Article 29 of the Law establishes the joint and several liability of the contractor, the self-employed carrier, and the taxi booking service for harm caused to passengers. This raises a number of questions: should this provision be considered special in relation to Part 4 of Article 13 of the Law, given that the latter refers not only to harm caused to passengers, but also to harm caused to third parties? Will liability be joint and several by default under the law, or will it depend on the terms and conditions of the contract?

Despite the lack of clarity in the provisions of the Law regarding liability for damage to passengers' lives, health or property during taxi transport, it can be concluded that liability is distributed quite reasonably between the parties involved. The fact that self-employed individuals are generally held fully liable for any harm caused to passengers supports the hypothesis that their activities are entrepreneurial in nature.

At the same time, the exclusively personal nature of their transport operations, the possible lack of their own property for this activity, and the provision of such property by a third party, the mandatory mediation of the taxi booking service between these individuals and their clients, as well as the possibility of transferring part of the mandatory requirements to other parties to the contract lead us to consider the social vulnerability of these individuals and the need to grant them certain social and labour rights and guarantees.

4. Regulation of Platform Employment and other Non-standard Forms of Employment

In practice across the world, there are two possible approaches to regulating non-standard forms of employment: Including persons with such employment in the scope of labour legislation; Addressing specific issues related to ensuring decent work for them [Golovina S.Yu., Serova A.V., 2022: 62–76].

The first approach essentially involves distinguishing between civil and labour law, and striking a balance between the two by analysing the features of the latter. In this connection, some researchers note that digitalisation and the increase in non-standard employment types have resulted in the need to revise the criteria for distinguishing between civil law relations and labour law relations, as stipulated by legislators and

formulated by courts.[29] In addition to conventional organisational dependence on the employer, the dependent nature of work should be determined by financial and informational dependence, or the asymmetry of the parties' economic opportunities [Chernykh N.V., 2023: 104–113].

The criteria mentioned are difficult to criticise with respect to taxi transportation, particularly when this activity becomes the only source of income for the self-employed person in the absence of employment, and when it is mandatory to enter into a contract with the booking service and impossible to influence the terms and conditions of the offer made by the service. The second approach is used in the case of non-standard employment, for example, in granting permission for such persons to establish trade unions, in regulating labour protection issues, and in addressing some other related aspects.

Based on the Labour Code norms, [30] the Russian legislator intends to incorporate non-standard employment types into the framework of labour law by establishing certain legal mechanisms that would guarantee certain rights for those employed under such types, e.g. the right to join a trade union. Unfortunately, the legislator's approach to determining the various types of non-standard employment has been rather unclear and inconsistent. In particular, it is difficult to ascertain which forms of employment fall within the remit of the general labour law provisions and other legislation containing labour law provisions.

The legislator goes on the premise that non-standard employment types are a system of social and labour relations that, for certain reasons, deviate from statutory work activities. This type of work activity has socially useful consequences and creates a public good. However, the parties involved are not in a formal employment relationship as there is no employment contract between the employee and the employer. The main criteria for defining non-standard employment types include the duration of working hours, relationships with employers who commission work or services (particularly those performed remotely or at home) and the form of relationship management. This includes employment

[29] De Stefano V. The Rise of the 'Just-in-Time Workforce': On-Demand Work, Crowd Work and Labour Protection in the 'Gig-Economy' . October 28, 2015. Bocconi Legal Studies Research Paper No. 2682602. Available at: URL: https://ssrn.com/abstract=2682602 (accessed: 20.09. 2025)

[30] Draft Federal Law No. 858157-8 "Labour Code of the Russian Federation" (version submitted to the State Duma in the wording as at 06 March 2025) (hereinafter: Draft Labour Code, the Draft) // Consultant Plus Legal Information System.

under a civil law contract and the application of the special taxation scheme, "Professional Income Tax", i.e. self-employment. The project also classifies platform employment as a form of non-standard employment. This is defined as the use of an online platform as an intermediary between service providers and consumers. The draft of the Russian Labour Code therefore clarifies that both self-employment and platform employment are considered non-standard forms of employment, and that the legislator is considering granting individuals in such employment certain social and labour rights and guarantees.

The doctrine describes three models of legal regulation of platform employment and self-employment in other countries [Golovina S.Yu., Serova A.V., 2022: 76]. The first model involves creating special legal solutions for platform workers, such as enabling them to recognise their relationship with the platform as an employment relationship in court, despite the civil law contract concluded between them. However, this approach has not been approved in the Russian legal system with regard to taxi transportation. In practice, there is a reclassification of the relationship between self-employed drivers, for the one part, and carriers-legal entities and self-employed entrepreneurs, for the other part, who provide them with taxis under civil law lease agreements, but who actually determine the conditions of their activities. Perhaps one should agree with N. E. Savenko's view that "the likelihood of reclassifying a civil law contract as an employment contract is much greater for a self-employed individual than for a platform worker" [Savenko N.E., 2024: 26–41]. This approach is not reflected in the draft generally permitting the reclassification of non-standard employment relationships based on civil law contracts as standard employment relationships. At the same time, it is advisable to specify the proposed regulation with regard to the possibility of reclassification, taking into account the regulation of the platform economy[31] and the organisation of passenger transport by taxi.

This regulatory model also enables platform workers to be classified as civil law subjects who are only subject to labour and social legislation to a limited extent. The recently enacted Platform Economy Law of 31.07.2025 has both embraced and avoided this approach. Firstly, it defines the platform economy as a set of property relations arising from the interaction of an unlimited number of individuals via digital platforms for business activities or other objectives. These other objectives

[31] Federal Law No. 289-FZ of 31 July 2025 "On Certain Issues of Regulating the Platform Economy in the Russian Federation; will come into force on 1 October 2026 (hereinafter referred to as the Platform Economy Law).

are likely to primarily satisfy the interests of consumers who purchase goods, works, and services through platforms. The law defines the goal of platform operators and their partners as making a profit; these include not only legal entities and self-employed entrepreneurs, but also PIT payers (with the exception of individuals conducting transactions on a digital platform unrelated to their business activities). Therefore, this law implicitly assumes that self-employed individuals performing work or providing services through a digital platform are engaged in entrepreneurial activity. This approach is generally consistent with that taken in the Law on the Organisation of Passenger Transport by Taxis.

Chapter 3 of the Platform Economy Law sets out the specifics of interactions between digital platform operators, users who commission work and partners who carry out the work and are natural persons. It also qualifies relations with contractors who are natural persons as civil law relations, provided they meet certain requirements.[32] This means that they are not guaranteed weekly days off and holidays in accordance with labour legislation or any additional social guarantees (unless otherwise entrenched by law) (Subparagraphs B and C, Paragraph 5, Article 15 of the Law). At the same time, the Law stipulates that the above provision does not restrict contract partners from taking breaks and resting, and establishes the operator's obligation to give preference to contract partners who are natural persons and have entered into compulsory pension and social insurance and/or voluntary medical and/or pension insurance. It also provides for the operator's right to fully or partially reimburse the costs incurred by implementing partners in connection with such insurance. Thus, the provisions of this Law and the draft demonstrate the legislator's understanding of the need to protect individuals who are partners of intermediary digital platforms socially, something which is currently lacking in Law No. 580-FZ and in practice.-

The second model for the legal regulation of platform employment and self-employment in other countries involves categorising intermediate workers and self-employed entrepreneurs as "dependent self-employed persons". This model is used, e.g., in Austria, Germany, Spain and Italy.[33]

[32] For example, the absence of a work schedule and compliance by the partner-contractor, who is a natural person, with the rules of internal labour regulations and local regulatory acts of the operator and/or user-customer containing labour law norms.

[33] In Spain, for example, this distinction is made in the Law on the Status of Individual Labour Activity. Available at: Ley 20/2007, de 11 de julio, del Estatuto del trabajo autónomo (accessed: 20.09. 2025)

The main criteria for non-entrepreneurial self-employment are personal, continuous cooperation organised by the client, including determining the time and place of work, and receiving at least 50% or 75% of income from this client. According to N.E. Savenko, self-employed persons are individuals who independently carry out income-generating activities, which activities are neither labour nor entrepreneurial since their characteristics and criteria do not fully correspond to the aforementioned modes of activity [Savenko N.E., 2024: 40].

So far, Russian lawmakers have not demonstrated any willingness to introduce such an intermediate category into legislation. In the legal regulations we have examined, they proceed from the dichotomy between labour and civil law relations associated with the conduct of entrepreneurial activity. However, the draft introduces the category of non-standard forms of employment and creates special regimes for platform partners or carriers who are individuals paying personal income tax, i.e. self-employed persons, which somewhat blurs the dichotomy.

In the field of taxi transportation, there are factual grounds for applying the category of "dependent self-employed" to self-employed carriers. In other words, an intermediate category could be introduced between employees and independent contractors, as some foreign scholars have proposed [Harris S.D., Krueger A.B., 2015]; [Stewart A., Stanford J., 2017]. Such grounds include, e.g., the mandatory conclusion of a contract with a taxi booking service that operates a digital platform, the self-employed person's inability to influence the terms of the offer or the amount of remuneration for transportation determined by the platform operator, and the platform operator's ability to restrict the self-employed person's access to orders. Other grounds include receiving a taxi, which is necessary for this activity, from third parties who often organise its use, and frequent taxi transportation activities as the sole source of employment income. Under these conditions, it would be unreasonable to place all the associated risks on self-employed individuals who lack social and labour rights and guarantees.

The third global regulatory model, chosen by Russian lawmakers and typical of post-Soviet states such as Azerbaijan and Belarus, is based on forming a set of legal norms that regulate the legal status of self-employed individuals operating as business entities without third-party involvement. This model forms the basis of legislation governing the platform economy and the organisation of taxi services, which generally do not provide self-employed transport operators with social or labour

rights or guarantees. The regulation of self-employment in the Russian legal system remains fragmented. As N.E. Savenko notes, the status of self-employed persons and platform workers remains uncertain, as the definitions of self-employment and platform work were not included in the relevant draft law that became the 2023 Employment Law[34] [Savenko N.E., 2024: 41]. In this context, the imminent adoption of the Platform Economy Law is undoubtedly a positive development. However, analysis of the regulatory framework and practices shows that regulation of self-employment and platform employment will mainly remain within the third model even in the future, without granting subjects of these forms of employment social and labour rights and guarantees.

Conclusion

The law on the organization of taxi services allows participants to choose different models for organising activities in this field. Thus, an individual can become an employee of a carrier and significantly reduce their risks and scope of liability by relying on their employer, while complying with the working hours established by the employer and remaining under their control. They can also become independent, self-employed carriers, who, with the mandatory technical intermediation of a taxi booking service and using their own or another person's property, will work for themselves. They will independently comply with all requirements and bear all risks and responsibilities, except for those that Law No. 580-FZ transfers or allows to be transferred to other participants in the relevant relations.

Self-employed entrepreneurs (except those persons who drive taxis independently) and legal entities may now only provide taxi services through their own hired drivers. They must use booking services to obtain orders or find orders independently, as they are prohibited from transferring orders to other carriers under Part 1 of Article 21 of that Law. As with other entrepreneurs, self-employed entrepreneurs and legal entities engaged in transportation are able to create conditions for self-employed carriers to operate by providing them with vehicles and related services, while ensuring compliance with carrier requirements.

The activities involved in providing booking services under Law No. 580-FZ essentially amount to creating the technical capability to receive

[34] Federal Law No. 565-FZ of 12 December 2023 On Employment of the Population in the Russian Federation // SPS Konsultant Plus.

orders from passengers and transfer them to carriers for the purpose of concluding a public charter agreement. In other words, it is essentially "technical intermediation," which imposes certain public law obligations and liability on them in certain cases.

In general, the activities of self-employed carriers may be classified as entrepreneurial, taking into account the licensing regime for their implementation and the provisions of Subpara 2, Para. 1 of Article 23 of the Civil Code. This is supported by the fact they independently bear many risks and are liable for harm caused to taxi passengers. It is also supported by the fact that liability is imposed on other parties primarily to comply with public law prohibitions and requirements in this area, as well as to protect the rights and legitimate interests of passengers, rather than to reduce the liability of self-employed carriers.

At the same time, recognising the particularities of personal taxi operations by self-employed individuals, the legislator has established an operating framework differing them from other entrepreneurs. It is characterised by the ability to select the applicable requirements and the use of "intermediaries" to ensure their implementation. Self-employed carriers are required to conclude a contract with a taxi booking service that operates an intermediary digital platform.

The authors have considered the trends in global practice regarding the regulation of non-standard forms of employment, as well as models for regulating platform-based and self-employment, and assessed the proposed regulation of non-standard forms of employment by Russian legislators alongside the current regulation of the platform economy and taxi services, and have reached several conclusions. Firstly, the legislator has chosen to regulate the model based on the entrepreneurial nature of the activities of self-employed carriers and platform workers. Secondly, the legislator has recognised the need to grant them certain social and labour rights and guarantees. Thirdly, the category of "dependent self-employed persons" may be introduced in future regulations.

References

1. Anan'eva A.A. (2020) Improving Legal and Individual Regulation of Taxi Ordering Services Operations as one of Measures aimed at Protection of Passenger Rights. *Transportnoe pravo*=Transport Law, no. 4, pp. 20–23 (in Russ.)

2. Belov V.A. (2022) Online Intermediary Platforms: Discussed Approaches and the Domestic System of Regulation. *Zakon*=Law, no. 6, pp. 116–125 (in Russ.) DOI: 10.37239/0869-4400-2022-19-6-116-125

3. Belov V.A. (2022) Digital Intermediation and Consumer Relations: Legal Nature and Liability. *Aktual'nye problemy rossiyskogo prava*=Current Issues of Russian Law, no. 8, pp. 68–82 (in Russ.) DOI: 10.17803/1994-1471.2022.141.8.068-082

4. Chernykh N.V. (2023) Transformation of Labor as Object of Social Relations and Spread of Non-Standard Forms of Employment. *Aktual'nye problemy rossiiskogo prava*=Current Issues of Russian Law, no. 12, pp. 104–113 (in Russ.) DOI: 10.17803/1994-1471.2023.157.12.104-113

5. De Stefano V. The Rise of the 'Just-in-Time Workforce': On-Demand Work, Crowd Work and Labour Protection in the 'Gig-Economy' (October 28, 2015). Bocconi Legal Studies Research Paper No. 2682602. Available at: URL: https://ssrn.com/abstract=2682602 (accessed: 20.09.2025)

6. Dolgov S.G. (2021) Civil Liability of Taxi Aggregators. *Grazhdanskoe pravo*=Civil Law, no. 1, pp. 3–7 (in Russ.) DOI: 10.18572/2070-2140-2021-1-3-7

7. Gaganov A.A. (2015) Legal aspects of illegal transportation of passengers and goods by motor passenger cars. *Administrativnoe i munitsipal'noe pravo*=Administrative and Municipal Law, no. 3, pp. 256–262 (in Russ.) DOI: 10.7256/2454-0595.2015.3.12519

8. Golovina S.Yu., Serova A.V. (2022) Legal Regulation of New Forms of Labor Employment. *Zhurnal rossiiskogo prava*=Journal of Russian Law, vol. 26, no. 8, pp. 62–76 (in Russ.) DOI: 10.12737/ jrl.2022.084

9. Ivanov A.A. (2017) Aggregation Business and Law. *Zakon*=Law, no. 5, pp. 145–156 (in Russ.)

10. Harris S., Krueger A. (2015). A Proposal for Modernizing Labor Laws for Twenty-First-Century Work: «Independent Worker». The Hamilton project. Available at: URL: https://www.hamiltonproject.org/assets/files/modernizing_labor_laws_for_twenty_first_century_work_krueger_harris.pdf

11. Karimullina A.E. (2023) Compensation of Damage to Life and Health of Passenger Taxi Passengers. *Transportnoe pravo*=Transport Law, no. 2, pp. 13–16 (in Russ.) DOI 10.18572/1812-3937-2023-2-13-16

12. Kuznetsova L.V. (2019) Civil liability of e-commerce aggregators. In: E-commerce and related areas: a collection of papers. M.A. Rozhkova (ed.). Moscow: Statut, 446 p. (in Russ.)

13. Mironova S.M., Kozhemyakin D.V. (2022) Liability of owners of Taxi Aggregators to Consumers. *Tsivilist*=Civilian Lawyer, no. 2, pp. 11–18 (in Russ.)

14.Savenko N.E. (2024) Employment, Self-Employment and Platform Employment of Citizens in the Light of Draft on Employment. *Khozyaistvo i pravo*=Economy and Law, no. 2, pp. 26–41 (in Russ.) DOI: 10.18572/0134-2398-2024-2-26-41

15. Skvarko U.A. (2024) Legal nature of relationships between a taxi booking and a taxi driver. *Pravo i ekonomika*=Law and Economy, no. 6, pp. 51–55 (in Russ.)

16. Stewart A., Stanford J. (2017) Regulating work in the gig economy: what are the options? *The Economic and Labour Relations Review,* vol. 28, no. 3, pp. 420–437. Available at: URL: https://www.sci-hub.ru/10.1177/1035304617722461?ysclid=mi2vgvz16u642640337 (accessed: 20.09.2025)

17. Suvorov E.D. (2019) Issues of e-commerce: liability of owners of rideshares to consumers. *Vestnik ekonomicheskogo pravosudiya*=Bulletin of Economic Justice, no. 9, pp. 57–67 (in Russ.)

18. Toshchenko V.V. (2023) On the System of Agreements on Passenger and Baggage Transportation by Passenger Taxis. *Transportnoe pravo*=Transport Law, no. 2, pp. 16–19 (in Russ.) DOI: 10.18572/1812-3937-2023-2-16-19

19. Toshchenko V.V. (2024) The place of chartering contracts of passenger taxi in the system of contracts of carriage by motor transport. *Transportnoe pravo*=Transport Law, no. 1, pp. 18–21 (in Russ.) DOI: 10.18572/1812-3937-2024-1-18-21.

Information about the authors:

Yu.D. Zhukova — Candidate of Sciences (Law), Associate Professor.
A.S. Podmarkova — Candidate of Sciences (Law), Associate Professor.

The article was submitted to editorial office 09.07.2025; approved after reviewing 29.09.2025; accepted for publication 30.10.2025.

Legal Issues in the Digital Age. 2026. Vol. 7, no. 1.
Вопросы права в цифровую эпоху. 2026. Том 7. № 1.

IT. Industries. Law: Telemedicinet

Research article
JEL: K2
UDC: 34.09
DOI:10.17323/2713-2749.2026.1.96.120

Prospects for a Digital Healthcare

Aleksander A. Kartskhiya
Russian State Oil and Gas Gubkin University, 65 Lenin Avenue, Moscow 119991, Russia,
arhz50@mail.ru, https: //orcid.org/0000-0002-8041-0055

Abstract
The aim of the research is to identify characteristics of the digital transformation process and the potential for its advancement in the healthcare industry. The author investigates current challenges in determining the specific use of advanced digital technologies in medicine, as well as the specific legal framework in the digitalization of domestic health care. Additionally, the analysis explores the potential of utilizing contemporary technologies to establish value-based healthcare and optimize the health system's focus on patient interests. The author employs a comprehensive analytical research methodology, a comparative legal approach to analyzing the legal dimensions of digital health care regulation. He also utilizes the method of modeling process of digitalization and the prospects for technological advancement in healthcare field, including identification of potential threats and risks associated with extensive use of advanced technologies like artificial intelligence (AI), bioengineering, and digital twins. These technologies aid in the development of personalized treatment strategies tailored to the unique characteristics of each patient by analyzing genomic data, as well as large volumes of biometric and other patient-related data from both patients and healthcare institutions. As a result, the author concludes the modern healthcare system is at the brink of revolutionary transformation due to the rapid integration of digital technologies. This emerging paradigm in healthcare, known as digital healthcare, presents unique opportunities for the development of the healthcare industry and necessitates legal regulation and responsible use of these new digital medical technologies. These technologies provide fundamentally new possibilities for diagnosis, treatment, rehabilitation, development of novel medications, and a personalized approach to patient care. Digital technologies are

not merely modernizing traditional treatment methods, but are fundamentally altering the way human society delivers medical care, and have a significant impact on healthcare development. In the future, it is envisaged to establish a full-functional digital healthcare ecosystem, which will be understood as a digitally integrated information technology infrastructure (including the interchange of medical data) utilized by all healthcare institutions, regulatory bodies, service providers, and patients.

Keywords

digitalization in healthcare; telemedicine; artificial intelligence; digital medicines; disease diagnostics; data security; digital medications; remote monitoring and diagnostics.

Acknowledgements: the study was conducted as part of the research project "Improving mechanisms for Protecting Intellectual Property Rights in the EAEU countries" in accordance with the State Assignment for the Russian State Academy of Intellectual Property (2-GZ-2024-2).

For citation: Kartskhiya A.A. (2026) Prospects for a Digital Healthcare. *Legal Issues in the Digital Age*, vol. 7, no. 1, pp. 96–120. DOI:10.17323/2713-2749.2026.1.96.120

Introduction

The rapid integration of artificial intelligence into information technology has brought about revolutionary change in the healthcare system. According to the World Economic Forum 2024[1], value-based healthcare is crucial for optimising healthcare worldwide. Digital solutions are a vital means of improving health, and as they evolve, information technologies coupled with big data and AI are playing an ever-more significant role in healthcare. In order to realise the full potential of these tools, it is essential that all relevant stakeholders, including patients, service providers, medical and pharmaceutical companies, investors, regulators, technology companies and developers, collaborate closely to drive the digital transformation of healthcare.

Digital technologies are a key factor in accelerating progress in healthcare. However, they are not a universal solution. Optimising healthcare requires improvements to its social determinants, such as increased ac-

[1] WEF 2024. Transforming Healthcare: Navigating Digital Health with a Value-Driven Approach. Available at: URL: https://www.developmentaid.org/api/frontend/cms/file/ 2025/04/WEF_Transforming_Healthcare_2024.pdf (Last accessed: 13.11.2025)

cessibility and investment, support for healthcare workers, the accelerated adoption of biomedical innovations, and better access to medicines and medical devices.

According to UN documents[2], the aim of digital healthcare is to provide equal and universal access to high-quality, affordable medical services, and to develop prevention, diagnosis and treatment services, as well as rehabilitation and palliative care. This system should promote the confidentiality and security of patient health information, and ultimately improve the usefulness and sustainability of national healthcare systems. The documents emphasise that health data should be treated as confidential personal data. Such data requires high security and protection standards necessitating the development of a regulatory framework. This framework aims to protect privacy, confidentiality and cybersecurity, as well as ensuring the integrity, availability and proper processing of personal health data. Almost 30% of the global data growth will come from the healthcare sector, which uses imaging, diagnostics and wearable devices. This necessitates the strengthening of infrastructure security, for which reliable analytical platforms and intelligent technologies capable of swiftly converting raw data into useful information are required.

The World Health Assembly (WHA78), which approved the extension of the global digital health strategy for 2020-27, confirmed the undeniable universal importance of digitalisation in healthcare, particularly in the context of the UN Sustainable Development Goals.[3] The global strategy aims to improve health worldwide by accelerating the development and implementation of affordable, scalable and sustainable digital solutions focused on preventing, detecting and responding to epidemics and pandemics, and on developing infrastructure and applications that enable the use of health data to improve health and well-being, and achieve sustainable development. It also aims to promote research, development and innovation in the health sector, as well as cooperation.

[2] World Health Organization. 2021. Global strategy on digital health 2020–2025. Available at: URL: https://iris.who.int/handle/ 10665/ 344249 (accessed: 13.11.2025); WHO guideline recommendations on digital interventions for health system strengthening: evidence and recommendations. Geneva, 2019. Available at: URL: https://iris.who.int/handle/10665/311980 (accessed: 13.11.2025)

[3] Global strategy on digital health 2020–2027. World Health Organization 2025. Available at: URL: https://www.who.int/publications/i/item/9789240116870 (accessed: 13.11.2025)

1. Cutting-edge Technologies at the Heart of Modern Digital Healthcare

A turning point has been reached in healthcare, medical technology and pharmaceuticals, and a decision must be made between: should the system be rapidly transformed, or should it be improved gradually? Ground-breaking medical solutions using the latest technologies, including AI, telemedicine, and cutting-edge treatment and prevention methods, can reduce costs and improve healthcare outcomes. AI is part of a broader digital revolution that promises to transform healthcare in many ways. Introducing digital technologies can improve healthcare, making medicine more accessible and affordable. However, implementing the concept of digital medicine will require overcoming risks and challenges relating to confidentiality, cybersecurity, the professional development of doctors and patients, and equitable access to medical services.

There are now unique opportunities to accelerate the digital transformation of healthcare by expanding the use of digital technologies and data. This will open up a new era of healthcare, with a focus on enhancing the value of medicine. The digital transformation of healthcare involves several key factors. These include the use of patient-centred digital applications and tools to improve healthcare; the introduction of advanced digital technologies, platforms and systems, and the widespread use of life science and pharmaceutical technologies. Digital applications can be used to collect large amounts of medical data, enabling improved and accelerated drug development and delivery, as well as portable and rapid therapies and diagnostics with better accuracy.

These factors are adding new meaning to medicine. The digitisation of patient care applications and the use of digital technologies, big data and AI primarily aim to provide better-quality medical care. However, most healthcare systems currently have fragmented IT infrastructure, incompatible data processing standards, outdated data exchange methods, and a multitude of digital solutions that hinder their use. Overall, the healthcare sector still lags behind others in terms of digital maturity.

The new paradigm in medicine is linked to the digitalisation of healthcare. Digital healthcare involves the use of digital information and communication technologies (ICT) for medical activities and the provision of medical care (services). Digital healthcare is a much broader concept than telemedicine technologies defined in Article 2 of Federal

Law No. 323-FZ of 21 November 2011 "On the Fundamentals of Protecting the Health of Citizens"[4] as enabling remote interaction.

Digital healthcare has emerged as a result of digitalisation, leading to the use of modern information technology (IT) in diagnosis, treatment and prevention. Digital healthcare can also be understood as the field of knowledge and activity concerned with developing and applying digital technologies to improve population health. One could speak of a digital health ecosystem, which is an infrastructure comprising functionally compatible IT systems used by the medical community in all areas of healthcare. The aim of digitalisation is to create this ecosystem. This system involves an interoperable digital IT infrastructure that connects healthcare institutions and patients, public healthcare authorities, universities and research centres, enabling data exchange between users, healthcare providers, healthcare system managers and data processing services.

Various models of artificial intelligence have already found widest application in digital medicine.

Digital twins (DTS) use AI technology to create digital representations of systems enabling advanced simulation, predictive modelling, and real-time optimisation in various fields, including healthcare. Digital twins are digital copies of physical objects, processes, or systems which are updated continuously with data to reflect the state of their real-world counterparts. They offer predictive modelling, decision support, and personalised modelling. Digital twins are often depicted as 3D models or information panels. A digital twin, for example, is a visual representation of a patient's heart. Medical applications using digital twins enable the simulation of complex treatment scenarios for patients, support prognostic diagnostics and allow for real-time, personalised treatment planning based on health data. Digital twins in healthcare cover a wide range of clinical and operational applications at various stages of development, ranging from theoretical models to advanced experimental stages [Zhou H. et al., 2024: 2–17]; [Ringeva M., Armel F., 2024].

Modelling medical processes based on AI technologies. For instance, generative AI can help with the design of studies and the writing of protocols by automatically matching clinical concepts with standardised study definitions, selection criteria and variable selection, using electronic health records as a basis. AI can model scenarios that are concep-

[4] Collection of Legislation of the Russian Federation. 2011. No. 48. P. 6724; 2025. No. 23. P. 3009.

tually similar to digital twins or medical models. This enables researchers to estimate clinical outcomes for alternative treatment strategies, timelines or dosing regimens that cannot be observed directly in real-world data. Synthetic data generation increases statistical significance and objectivity, helping to overcome limitations related to sample size and improving the representation of rare diseases and underrepresented populations [Azarfar G. et al., 2025: 2–5]. Generative AI technologies are used in the mortality and disease research to analyse specialised clinical images, such as retinal images [Nusinovici S. et al., 2022: 4–5] and chest X-rays [Raghu V., Weiss J., 2021: 6–7]. These technologies can also predict the biological age of patients based on a large group of facial images indicating age, gender, and ethnicity. This has been tested on four different clinical groups, including patients with various types of cancer [Bontempi D., 2025: 2–3].

In operations involving big data and biometric personal data, AI enables processes and their results to be modelled based on actual data. It also makes it possible to create 'synthetic data', i.e. artificially generated information designed to emulate the characteristics and statistical properties of real data. In healthcare, synthetic data is often used to supplement or extend real-world datasets (e.g. electronic health records or registries) in order to address privacy concerns and overcome the limitations of these datasets [Koul A., 2025: 1–2].

One of the latest trends is using blockchains to process large amounts of patient information and health data, including the results of various tests, quality assessments, and health surveys. Blockchain technology also enables sharing of patient data, such as name, date of birth, diagnosis, treatment and medical history, etc. with healthcare providers in the form of electronic health records (EHRs). These records are typically stored in cloud computing environments or traditional databases. Blockchain technology can also be used to collect and process anonymised data to tailor prescription drugs and services to patients. Furthermore, blockchain technology enables seamless communication and information exchange between various organisations in the healthcare ecosystem via a distributed ledger, thereby enhancing the security and transparency of these exchanges. Users can exchange and track data and actions within the system without the need for additional solutions to maintain integrity and confidentiality.

The creation of biobanks and the use of biodata are new trends in digital medicine. Most traditional risk assessment tools are based on

clinical parameters such as age, gender and family history, as well as a limited set of basic disease-specific biomarkers. However, these tools cannot capture the full range of biological processes underlying many diseases. Biobanks that combine electronic health records and multi-omic data, such as standard blood test results, proteomics and metabolomics, open up unprecedented opportunities for searching for new biomarkers and sets of biomarkers for more accurate prediction of disease onset [Garg M., Karpinski M., 2024: 1821–1831]. The biobank contains a variety of phenotypic data, including continuously updated medical records, biometric measurements, lifestyle indicators, biomarkers, and images.

The British Biobank [Backman J., 2021: 628–634] is one of the largest biobanks worldwide. It contains medical records and genetic sequencing data from half a million human persons aged between 40–69. This enables numerous genetic associations and potential therapeutic targets to be identified. It also makes it possible to identify combinations of biomarkers capable predict disease onset more accurately than any single biomarker. In addition to predicting disease and detecting biomarkers, biomarker-based predictions for individuals with the disease can also complement genetic discovery analysis. A common limitation of most biobanks is that phenotype definitions are often based on calculated codes and self-reports, which can result in participants being misclassified, data being missing, and variability in the definition of case-control cohorts. Identifying individuals who may be patients but are either not coded appropriately or have not been clinically diagnosed remains challenging [Cortes A., Johnston I., 2023: 699].

Quite new field is currently emerging in medicine: engineered living therapy. This involves using advanced probiotic systems — namely microbes, cells and fungi associated with human health — to produce therapeutic substances such as medicines, enzymes and hormones. These treatments have been made possible thanks to synthetic biology and genetic engineering. In this treatment, a genetic code is introduced that promotes the creation of biological control mechanisms to regulate the production of therapeutic drugs in the patient's body, ensuring accurate and safe activation. This therapy promises to overcome the serious limitations of traditional medicines, particularly the high cost of biopharmaceuticals. Such preparations are now produced in laboratories using modified cell lines, followed by thorough purification, processing and formulation. Producing therapeutic drugs directly in the body avoids these stages, which typically were account for up to 70% of

production costs. Furthermore, for drugs that require frequent administration by injection, their sustained production in the patient's body ensures a stable, long-term supply, improving adaptation to treatment — a particularly important consideration in the treatment of diabetes, for example. NEC, for instance, is conducting Phase I/II clinical trials using a weakened strain of Salmonella bacteria to activate the immune system and fight cancer cells.

Safety is also a key focus, with issues such as unintended gene transfer, immune responses and environmental release being actively addressed. Promising approaches that are currently being investigated include metabolic and genetic programmes that can either prevent bacterial growth or kill bacteria on command, as well as the safe encapsulation of bacteria in polymer-based containers [Zalatan J., Petrini L., 2024: 2–7].

Autonomous biochemical sensor (biosensor) technology is in development. This involves connecting biological sensors to provide real-time information. Standalone biochemical sensors are analytical devices that are able to continuously detect and quantify biochemical parameters (markers) to enable personalised patient treatment or to monitor chemical changes in soil or water. These sensors detect controlled chemical substances using specialised physicochemical transducers or biological sensors that utilise enzymes, antibodies, or even modified living cells. Designed to operate and transmit data without human intervention, they use wireless communication and harvest energy from autonomous power sources, such as biofuel cells [Maity D., Guha P., 2023: 1–14] for continuous real-time monitoring. Since these sensors can be accessed remotely, they are ideal for use in hard-to-reach or remote locations. This enables continuous monitoring of people's and nature's health.

Unlike conventional disposable sensors, such as those used for testing for the SARS-CoV-2 virus, the aim of standalone biochemical monitoring is to enable continuous monitoring and electronic data collection. Due to technical limitations mentioned, standalone biochemical sensors are only used in very specific areas. The most useful example is the wearable glucose sensor, that measures glucose concentration and exchanges data with a smartphone that controls an insulin pump to stabilise glucose levels. Thanks to advances in materials science, nanotechnology, biomimetics and wireless technologies, standalone biochemical sensors are now being used to address other challenges in different fields [Zargartalebi H., 2024: 1146–1153]. New forms of this technology could transform the lives of patients who require ongoing monitoring.

However, many sensors have a short service life and must be replaced regularly. Compared to conventional medical or environmental sensors, microbial whole-cell biosensors face additional regulatory hurdles and ethical concerns because they are genetically modified organisms that could potentially be released into the environment.

The decentralisation of diagnostics through wearable devices and biosensors installed in healthcare facilities will enable testing to take place not only in medical institutions, but also at home and in remote areas. The dissemination of such diagnostic data could transform the approach to treatment, enabling earlier intervention and generating significant amounts of data on public health [Lino C., 2022: 2–9]. In addition designing physical sensors, integrating data is another important area of development. Standalone sensor networks generate a continuous stream of molecular information in various areas, so new analytical systems and control models are needed to process this data. Privacy and security issues, particularly in the field of health monitoring, require regulatory approaches balancing innovation with the protection of confidential information. The convergence of continuous monitoring capabilities in the fields of environmental protection, food safety and healthcare suggests molecular detection will become an integral part of everyday infrastructure rather than a specialised function in future [Florea L., Diamond D., 2022: 1–7].The enhanced capabilities of connected big biometric data systems for collecting, processing, and making decisions in the context of using various smart sensors have resulted in their widespread use at the workplace and integration with systems, using artificial intelligence systems.

Artificial catalyst reproduction technologies enable the production of nanomaterials (nanozymes) with natural enzyme properties (nanoenzymes) in laboratories or on production lines. Unlike enzymes produced by living organisms or synthesised chemically, nanoenzymes are more stable, cheaper and easier to produce. Consisting of nanoparticles of metals, metal oxides, carbon and other substances, nanoenzymes behave like catalysts and promote the same chemical reactions as enzymes. Thanks to their robustness, they are capable to function in a much wider variety of environments, broadening their potential applications in biomedicine, ecology, and industry. Advanced nanoscale design and manufacturing techniques make it possible to create multifunctional nanoferments. The rapid advances in nanoenzyme technology over the past two decades have attracted the attention of major pharmaceutical companies, resulting in increased investment in R&D in this field. This

increased funding has accelerated innovation and expanded the possibilities for using nano-enzymes in various fields of medicine, such as the treatment of cancer and neurodegenerative diseases, and as a means of targeted drug delivery. This increases the effectiveness of chemotherapy while reducing side effects [Sen A., 2024: 25].

Nanoenzymes have the potential to transform diagnostics and treatment, particularly in areas such as the early detection of diseases, targeted drug delivery, environmental remediation and targeted therapy. However, nanoenzymes require the integration of AI, computational design and specialised knowledge [Cao X., 2024: 27].

According to verious researchers, digital technologies make it possible to solve various problems [Thirumal M., Monika S., 2024: 1–4]; [Lee B., Ghovanloo M., 2019: 74–80]. For example, digital measuring instruments allow for the objective and continuous collection of data, which reduces the likelihood of bias and errors associated with traditional methods of data collection. This facilitates the collection of large volumes of patient data, enabling the development of personalised, accurate treatment approaches tailored to individual needs.

Surgical robots and medical assistants (including the foreign models Da Vinci, Dixion Revo-i, Senhance, MAKO, and Russian models AST, and LevshAI) are key elements of modern instrumental medicine. They increase the accuracy of operations and the quality of patient care, while also making staff's work easier. Despite their high cost and the need for surgeons to undergo special training, they provide increased accuracy, minimally invasive procedures and the ability to work in hard-to-reach areas, as well as reducing hospitalisation time. Medical assistants such as nurse robots, assistant and consultant robots, companion robots, disinfection and rehabilitation robots, perform a variety of tasks to improve patient care. While they do not replace doctors, robots in medicine become their indispensable assistants, improving the quality of treatment and care. However, their widespread adoption requires solutions to issues related to cost, training and ethics.

Biotelemetry, also known as biomedical or medical telemetry, enables the monitoring and transmission of physiological data from a patient to a remote location for analysis, interpretation and diagnosis. This technology enables the wireless or remote monitoring of physiological parameters such as heart rate, blood pressure and temperature, as well as other vital signs. Biotelemetry is widely used in cardiology, for example, for the remote monitoring of cardiac activity and in the treatment of

heart disease. It enables the early detection of abnormalities, facilitates timely intervention and improves the overall care and treatment of patients with chronic diseases.

Implantable biomedical devices are designed to interact with biological systems, can range from simple sensors to sophisticated electronic systems. They are typically used for the long-term monitoring and treatment of chronic diseases. For example, pacemakers and defibrillators are used to regulate abnormal heart rhythms and deliver electrical impulses to the heart. Implantable cardiac monitors are used to monitor the heart's electrical activity in order to detect arrhythmias and other abnormalities. Implantable neurostimulators use electrical stimulation to treat chronic pain, movement disorders and other neurological conditions by targeting nerve fibres or areas of the brain. Implantable glucose monitors continuously track glucose levels in persons with diabetes, providing valuable data to help manage blood sugar levels. Implantable drug delivery systems provide targeted treatment for conditions such as chronic pain or cancer by delivering drugs directly to specific areas of the body.

Digital imaging and diagnostic tools, such as digital radiography, PACS (Picture Archiving and Communication System), as well as AI-based diagnostic tools, enable fast and accurate diagnoses and the seamless sharing of medical images and reports. Digital medicines increase patient engagement in the treatment process and their adherence to the treatment plans. Mobile applications can remind patients to take their medication and track their symptoms. However, digital medicine safety standards and patient data security and confidentiality must be observed in accordance with the objectives and needs of the medical institution.

One of the most advanced areas of digitalisation is the application of neurotechnology, or neuroprosthetics, and its integration into the healthcare system. The most promising trend here is the development of prosthetics for sensory systems, such as hearing, vision, etc., and for limbs.

2. Building Digital Healthcare in Russia

Global issues such as population growth, an ageing population, the prevalence of chronic non-communicable diseases and constantly rising healthcare costs, coupled with simultaneous shortages in resource, including human resources, can be resolved through the active imple-

mentation of a wide range of IT and digital technologies [Maleina M., 2023: 5]; [Pugachev P., 2021: 12]; [Sheremetyeva N., 2024: 43].

This increases the need for the regulation of the application of advanced technologies, including AI. Legal regulatory methods must be balanced and coordinated to create conditions that encourage development of modern technologies, including AI [Bogdanovskaya I. et al., 2025: 124–148].

The digital transformation of healthcare using modern technologies such as the Internet of Things, remote monitoring and telemedicine, AI, blockchain, smart wearables and digital information platforms has proven its great potential. These technologies enable the remote collection and exchange of data and relevant information across the ecosystem, ensuring continuity of care, improving medical diagnostics and facilitating data-driven treatment decisions, digital therapy, and clinical trials. They also support autonomous, human-centred healthcare and care management, and contribute to the creation of a data-driven knowledge base on the skills and competencies of healthcare facilities and personnel.

Digital technologies are modernising traditional treatment methods and also radically changing the delivery of medical care, which significantly influences the development of the healthcare industry. The transition to digital healthcare is not just a matter of modernisation; it is a necessity for improving treatment outcomes, optimising medical operations and providing personalised care. During the digitisation of clinical information, access to complete patient data in real time enables informed decision-making, reduces errors and optimises the coordination of medical care. Meanwhile, data analytics based on digital systems helps to identify early signs of disease and gaps in medical care, as well as optimising the treatment process. The volume and variety of medical information in healthcare has skyrocketed due to the widespread adoption of electronic health records and the use of wearable and internet-enabled devices, as well as the wealth of information contained in medical records and laboratory test results. A continuous stream of real-time data has further increased this volume.

In Russia, digital medicine has found its widest application in Moscow. Replacing analogue equipment with digital technology has enabled the creation of a unified digital circuit for the city's healthcare system. Appointments with doctors, patient records, planned and emergency hospitalisations, prescriptions, vaccinations, test results, and other

medical information are stored in the EMIAS unified medical information and analysis system, which is accessible online. AI technologies, computer vision and the analysis and interpretation of X-ray images have been shown to be highly effective in electronic medical records, diagnostic systems, medical service management and "digital resuscitation" [Sizov G., 2024: 41–52].

The level of digitalisation in health care is best assessed through the concept of "digital maturity," which is defined as the use of digital systems and technologies in healthcare provision, management, and patient interaction. This reflects the extent to which information technologies are integrated in the business processes of healthcare institutions, as well as the quality of their use, and compliance with legal requirements.

In accordance with Decree No. 1014 of the President of the Russian Federation of 28 November 2024 "On Assessing the Effectiveness of Senior Officials of the Constituent Entities of the Russian Federation and the Activities of the Executive Bodies of the Constituent Entities of the Russian Federation," the criterion of "digital maturity" is used to assess public administration, including administration in healthcare.[5] The "digital maturity" in this field, as defined by Presidential Decree No. 309 of 7 May 2024 "On the National Development Goals of the Russian Federation for the Period up to 2030 and the Outlook for 2036"[6], is identified as a major national development goal. This involves automating most transactions within unified industry digital platforms, as well as implementing a data-driven management model in line with the accelerated adoption of big data processing technologies, machine learning, and AI.

Digital maturity components include medical information systems, remote interaction and care (i.e., telemedicine), and digital tools for managing medical data and services. In particular, Article 9.1 of Federal Law No. 323-FZ of 21 November 2011[7] provides for the creation of a Unified State Information System ("USIS") in the field of healthcare The USIS operates in accordance with the updated regulations, as approved by the Government of the Russian Federation in Resolution No. 140 of 09 February 2022[8]. It is a complex system including federal integration systems, such as registries of medical and pharmaceutical

[5] Collection of Legislation of the Russian Federation. 2024. No. 49. (Part V). P. 7576.

[6] Collection of Legislation of the Russian Federation. 2024. No. 20. P. 2584.

[7] Collection of Legislation of the Russian Federation. 2011. No. 48. P. 6724.

[8] Available at: URL: http://pravo.gov.ru (accessed: 13.11.2025)

employees and organisations, electronic health documents and regulatory reference information in the field of healthcare. It also includes an electronic registry and integrated electronic health cards. It contains a number of subsystems, including drug registries for medical use; automated collection of health indicator information from various sources; anonymisation of personal data; a geo-information subsystem; an information protection subsystem. The USIS implements a number of functions: identifying and arranging in a system of information about individuals contained in the unified system's subsystems; database management forming a single data warehouse; protecting information; and facilitating IT interaction between unified system's subsystems and other information systems. It also performs the functions of common system technological services.

Digital maturity is also defined as an indicator based on the methodology approved by Order No. 1210 of the Ministry for Digital Technology, Communication and Mass Media of 28 December 2024. Federal Law No. 426-FZ "On the Federal Budget for 2026 and the Planning Period for the Years 2027 and 2028" of 28 November 2025, provides [9] for the creation of a unified digital contour in domestic health care, for implementation of medical information systems and state information systems in the field of healthcare, ensuring interaction with the USIS and in healthcare institutions of the public health system. Digital maturity is determined by the extent to which digital systems and technologies are used in healthcare provision, healthcare management and patient interaction. It reflects the degree to which IT is integrated in the business processes of healthcare institutions, how well it is used and whether it complies with legal requirements.

Digital maturity reflects the extent to that digital technologies, platform solutions and computer applications are used in medical care provision, healthcare management and patient interaction. It demonstrates the extent to which IT is integrated into the business processes of healthcare institutions, how effectively it is used and whether it complies with legal requirements, with the ultimate aim of improving the quality and accessibility of healthcare.

Modern tools are required to assess the digital maturity of healthcare institutions in the context of the digital transformation of healthcare. The criteria used for this assessment may depend on the methodology of

[9] Collection of Legislation of the Russian Federation. 2025. No. 48. (Parts I to III). P. 7237.

the applied model. In practice, a large number of cases demonstrate the use of such models [Voshev B., 2023: 615–627]. E.g., there is the Electronic Medical Record Adoption Model developed by the international Healthcare Information and Management Systems Society, evaluates the degree of integration of electronic medical records and digital solutions in the operations of healthcare institutions on a scale from 0 to 7.

In Russia, the Ministry of Health's experience enabled the creation of a methodology for the objective and systematic assessment of digital maturity levels. This methodology records the structures and activities of different healthcare organisations, and their adaptability to various levels of healthcare. It promotes the standardisation of digital transformation, identifies and analyses problem areas, and offers recommendations to enhance the digital maturity of organisations. The methodology contains an algorithm for calculating digital maturity levels and establishing readiness for digital transformation. It covers the main aspects of digitalisation and provides an integrated approach to analysing and identifying problems that hinder digital transformation. It also allows recommendations to be developed for eliminating these problems.

Telemedicine technologies are becoming more and more widespread in Russia and other countries. According to Art. 36.2 of Federal Law No. 323-FZ of 21 November 2011, medical care involving telemedicine is organised and provided in accordance with the procedure established by the Ministry of Healthcare, based on clinical recommendations and in line with standards. Telemedicine technology may be used during consultations with healthcare practitioners and for the remote monitoring of patients' conditions based on data collected using medical monitoring devices and/or data entered into the USIS or the state information system of a Russian Federation constituent entity. According to the programme approved under Federal Law No. 258 of 31 July 2020 "On Experimental Legal Regimes in the Field of Digital Innovations", the use of telemedicine technologies is permitted for private healthcare clinics that participate in a pilot legal regime in the field of digital innovations."[10] The organisation and provision of medical care using telemedicine technologies is approved by Order 193n of the Ministry of Healthcare of Russia of 11 April 2025.

Article 34 of Federal Law No. 323-FZ of 21 November 2011 defines specialised care as a distinct type of medical care. This includes the pre-

[10] Collection of Legislation of the Russian Federation. 2021. No 27. (Part I). P. 5159.

vention, diagnosis and treatment of diseases and conditions (including during pregnancy, childbirth and the postpartum period) that require specialised methods and medical technologies, as well as rehabilitation. This care is provided in licensed medical institutions and other organisations within the state, municipal and private healthcare systems.

High-tech medical care is a form of specialised care involving new, complex and/or unique methods, as well as resource-intensive treatment methods with scientifically proven benefits. These include cell technologies, robotic technology, information technology, and genetic engineering methods developed based on advances in medical science and related fields. This type of care is provided in accordance with Order No. 186n of the Russian Ministry of Health of 11 April 2025, which sets out the types of high-tech medical care available. The order outlines the treatment methods and funding sources established under the state programme of guarantees for free medical care. This programme includes a list of types of high-tech medical care involving unique treatment methods. This assistance is provided by healthcare institutions that are included in a unified registry.

The prospects of digital health are primarily related to the area's comprehensive development. In accordance with Order No. 959r of the President of the Russian Federation of 17 April 2024, the document under the title Strategic Direction for Digital Transformation in Healthcare was approved.[11] The Direction largely defines the prospects for the development of domestic digital health. It has set the goal of achieving a high level of digital maturity, as well as accelerating the transition of healthcare to new levels of management and technology. This will be achieved through the complete adoption of digital twins and other cross-cutting technologies, also will be of use ensuring the creation of a platform ecosystem based on coherent and homogeneous primary data.

From a strategic standpoint, digital transformation serves a broader purpose: it helps to achieve technological sovereignty and creates conditions for the development of healthcare and the long-term social and economic development of the country amid rapidly changing internal and external factors. Healthcare is digitised using domestic ICTs, including domestic "cross-cutting" digital technologies that ensure technological sovereignty. This is achieved through the formation of platforms involves developing sector-specific technical policies in the field

[11] Collection of Legislation of the Russian Federation. 2024. No. 17. P. 2388.

of ICT, creating unified approaches to the architecture of health information systems and forming sectoral information system architectures using common modelling and description tools. Digital transformation in healthcare is based on common information models and unified information exchange standards. It involves regulated interaction between different systems and actors, as well as the creation of an infrastructure platform to solve problems at all levels of government. All these steps help to maintain a high level of information security. Particular focus is placed on establishing a digital ecosystem for the collection, processing and use of data to improve medical care, advance biomedical research and introduce individual electronic medical devices, as well as dynamic observation technologies using centralised diagnostic service platforms.

The goals and objectives of digitalisation are implemented as part of the Ministry of Healthcare's public policy on digital transformation, in collaboration with other stakeholders in the field, through the use of the GosTech platform, while observing the principles of customer centricity.

The key technologies required to implement the policy have been identified. In particular, AI will be used to automate processes, optimise resources, detect anomalies, and analyse information to support decision-making in healthcare. Big data technologies will facilitate predictive modelling in drug development and enhance patient treatment. Big data analysis will also enhance the precision of clinical trial planning. Wireless technologies, integrated into technology management platforms, will facilitate communication between various devices and systems. Digital industry technologies will be applied within the healthcare domain to facilities and processes that are required by law.

In this context it is important to certify portable devices and other medical products (as provided for in Art. 38 of Federal Law No. 323-FZ) so that they are considered digital medical diagnostic products unlike health gadgets such as tracker watches, smart bracelets, etc.

Digital regulation tasks are addressed through the legal mechanism of the regimes introduced under Federal Law No. 258 of 31 July 2020.[12] Testing legal regulations in pilot mode (the sandbox regime) enables the various regulatory aspects of digital technologies to be tested quickly, while legal means and mechanisms for their application in healthcare are being developed.

[12] Collection of Legislation of the Russian Federation. 2020. No 31. (Part I). P. 5017.

This mechanism are widely used in medicine in recent years. For example, Resolution No. 2276 of the Russian Federation Government of 9 December 2022, established a pilot legal regime for digital innovations in medical activities involving the collection and processing of information on individuals' status and diagnoses, as part of the socio-economic development initiative "Personal Medical Assistants" (PMAs). This legal mechanism is used to gather, process, store, and transmit measurement data obtained by medical devices registered under the Rules of State Registration of Medical Products (approved by Government Decree No. 1416 of 27 December 2012) to healthcare institutions' IT systems.

During the pilot scheme for remotely monitoring patients' conditions using PMAs, the impact of this technology was confirmed, as were the mechanisms for securely communicating information between information systems. In 2024, the PMA information system was integrated with the USIS. The PMA platform monitors compliance with the national PNST 995-2024 standard "Cyber-Physical Systems. PMA. Data Exchange Formats. General Requirements". It was concluded special regulations could be used for general regulation.[13]

According to Government of Moscow Decree No. 1706 of 31 October 2025, an experimental legal regime for digital and technological innovations has been established in the city. This regime will run for three years and will cover the signing or refusal of informed voluntary consent for medical intervention using an electronic graphic signature.

Biometric personal data (information on a person's physiological and biological characteristics that can be used to establish their identity) is subject to special legal regulations and procedures for processing and use, in accordance with Federal Law No. 152-FZ "On Personal Data" of 27 July 2006 (as amended on 24 June 2025),[14]" and Federal Law No. 572-FZ "Implementation of Identification and (or) Authentication of Individuals Using Biometric Personal Data, Amendment of Individual Legislative Acts of the Russian Federation and Recognition of Certain Provisions of Legislative Acts Invalid" of 29 December 2022

[13] Consolidated analytical report of the Ministry of Economic Development. 05 December 2025. Available at: URL: https://www.economy.gov.ru/material/file/download/3ffe5db176a775124b76812453fdf362/svodniy_analiticheskiy_otchet_122025.pdf (accessed: 13.11.2025)

[14] Collection of Legislation of the Russian Federation. 2006. No 31. (Part I). P. 3451.

(as amended on 28 December 2024).[15] Biometric data includes photographic and video images of a person, their fingerprint data, DNA analysis, voice data and iris data.

Biobanks are a specialised area of medical regulation. They are used to store human biological materials and biomedical cellular products in a way that ensures their biological properties are preserved and they are not infected or contaminated, as described in Art. 37 of Federal Law No. 180-FZ "On biomedical cellular products", of 23 June 2016 (as amended 04 August 2023).[16] Biobanks are still a new category under Russian law [Ostanina E.A., 2023: 66–67]; [Mokhov A.A., 2021: 343] involving the storage of a large amount of patients' biomaterials, similar to the International Community of Biological and Environmental Repositories biobank. The biobank of hereditary pathology is one of the few domestic examples. It is a collection of biological samples (DNA, blood, tissues, cells, etc.) gathered at the Tomsk NIMC medical genetics research institute.[17]

Experience has shown that digitalising healthcare can have negative consequences. It does not eliminate the possibility of medical errors, poor-quality medical services or data leakage. This necessitates development of better technologies and compliance with all applicable national laws and regulations. For instance, the use of synthetic data in AI-based research and diagnostics can lead to issues of "synthetic confidence": an unfounded trust in models that are trained using artificial datasets which do not reflect clinical validity or demographic realities. To ensure full accountability, effective precautions must be taken when using medical AI, including training data standards, vulnerability testing throughout the development process and disclosing the origin of synthetic data. These measures guarantee the integrity and fairness of data in clinical applications and establish new standards for the responsible and equitable use of synthetic data in healthcare [Koul A., Duran D., 2025: 2–5].

Digital technologies cannot eliminate adverse outcomes, such as adverse drug reactions or errors in medication administration. Unsafe treatment methods may arise at different stages of the process, such as erroneous drug prescriptions (e.g. mismatch to the patient's age and condition, incorrect dosage, contraindications, and lack of attention to

[15] Collection of Legislation of the Russian Federation. 2023. No 1. (Part 1). P. 19.

[16] Collection of Legislation of the Russian Federation. 2016. No 26. (Part I). P. 3849.

[17] Available at: URL: https://www.medgenetics.ru/institut/bank/ (accessed: 13.11.2025)

drug interactions), errors in the issuing and prescribing process, and improper monitoring of treatment [Insani W. et al., 2025: 27]. The application of biotechnology is associated with possible risks, including adverse health effects, which are an inevitable consequence of disease treatment and prevention.[18]

In addition to the above risks, there are also ethical issues, for example regarding AI technology as defined in the Code of Ethics for the Use of Artificial Intelligence in Healthcare.[19] These include increased risk of harm to health due to potential errors in processing of data and AI-generated conclusions (recommendations); cybersecurity issues, including unauthorised interference with AI algorithms or access to patient's personal data, etc.

This exacerbates the problem of liability for medical errors involving AI, at a time when judicial and enforcement practices are still in their infancy. Doctors are criminally liable and medical institutions are civilly liable for inadequate medical services. As S. Grishin and C. Odintsov have noted [Grishin S., Odintsov C., 2024: 43–50], applying tort liability to determine the guilt of a doctor who used AI technology is not an indisputable solution. Neural networks are more accurate than doctors. However, the final decision is made by a doctor, not AI.

In accordance with the Responsible Infinitor doctrine [Kamensky S., 2020: 9], which holds employers liable for inadvertently harming employees while they are performing work duties, the medical organisation is liable for its managers' failure to adequately train employees and monitor AI usage. However, attributing responsibility to AI would require the recognition of its legal personality, which is contrary to current legislation. At the same time, according to several researchers [Magrani E., 2019: 7– v8]; [Ivanova A., 2021: 155], the widespread use of AI could result in doctors becoming less skilled and losing their diagnostic abilities. We must also consider AI's 'hallucinations' when making decisions or diagnoses, as these can also lead to medical errors. Liability is one of the most pressing issues in digital medicine, and the use of AI

[18] WEF. Global Risks Report. January 2025. P. 53–55. Available at: URL: https://www.weforum.org/ publications/global-risks-report-2025 (accessed: 13.11.2025)

[19] Approved by the Interdepartmental Working Group of the Ministry of Health on the creation, development and implementation in clinical practice of medical products and services using artificial intelligence technologies, meeting minutes No. 90/18-0/117. 14 February 2025. Available at: URL: https://portal.egisz.rosminzdrav.ru/default/06/kodeks-etiki-primenenia-iskusstvennogo-intellekta-v-sfere-ohrany-zdorov-a-1.pdf (accessed: 13.11.2025)

and other digital technologies introduces further risks and threats. This complicates the structure of legal relations and, consequently, the liability of those involved.

That said that advances in digital medicine within the fields of biomedicine and biotechnology are leading to new legal regulations, such as the concepts of neural and biological law, etc. [Kravets I., 2022: 130].

Developing a legal framework for digital healthcare primarily involves creating regulations for the use of technology in digitalising medical activities and assistance. This includes establishing an optimal mechanism for experimental legal regimes for specific medical activities, with a view to subsequently applying the results to legal regulation. Examples include introducing an electronic graphic signature for providing or refusing informed consent to medical intervention and applying technologies to collect and process information on patients' health status and diagnoses.

Digitalisation also affects document management. New methods and technologies are employed during implementation and to establish electronic communications between healthcare institutions and the regulator. For example, amendments to Federal Law No. 61-FZ of 12 April 2010 (as amended on 29 December 2025) "On the handling of medicines"[20] provide for most registration and circulation procedures for medicines to be transferred to an electronic format via the federal portal Gosuslugi and the USIS. The law permits patient consent for participation in clinical trials to be drafted in electronic or paper form. Additionally, the development and use of advanced medicines necessitated the introduction of the term "advanced medicinal product" into the law. This refers to a gene therapy medicinal product or a medicinal preparation based on somatic cells or tissue engineering.

Conclusion

Digital technologies present unique opportunities for the development of healthcare and legal regulation. They are a vital part of sustainable health systems and a driving force behind their development. A national digitalisation strategy is necessary to create a digital health ecosystem. This will bring together financial, organisational, human and technological resources and ensure coordination among the many

[20] Collection of Legislation of the Russian Federation. 2010. No. 16. P. 1815.

stakeholders of the digital healthcare system, helping to establish priorities, standards and systems for digital IT architecture and facilitating their integration.

Digital healthcare is about delivering outcomes that benefit both patients and society. The concept of digital health is implemented with the following requirements in mind:

— an approach to healthcare based on biological data;

— the use of digital tools to track treatment outcomes and improve access to healthcare;

— expanding opportunities for telemedicine and other online healthcare services;

— improving funding methods to reduce costs.

Biometric data is particularly important as it provides a clear picture of access issues and enables targeted support for patients. The wide use of telemedicine and robotic devices (e.g. robot surgeons and helpers) improves interaction between patients and doctors, regardless of their location, while mobile tools improve prevention. It is clear that a new legal sphere — digital health care is emerging rapidly at the intersection of technology and healthcare. Because innovations in medical technology mentioned transform the industry seriously, the need for a comprehensive regulatory system governing digital medicine is growing stronger. Therefore, it would be sensible to create a special section on digital health issues within the Federal Law No. 323-FZ of 21 November 2011, that would include provisions about the goals and objectives of digital medicine, its development strategy, and on its principles and directions.

References

1. Azarfar G. et al. (2025) Responsible adoption of multimodal artificial intelligence in health care: promises and challenges. *The Lancet Digital Health*, vol. 7, no. 12, pp. 100917. DOI: 10.1016/j.landig.2025.100917

2. Backman J. et al. (2021) Exome sequencing and analysis of 454,787 UK Biobank participants. *Nature*, vol. 599, pp. 628–634. doi:10.1038/s41586-021-04103-z

3. Bogdanovskaya I. Yu., Vasiakina E., Volos A., Danilov N.A., Yegorova E., Salikhov D., Kalyatin V., Karpenko O. (2025) Artificial intelligence and law: from theory to practice. *Legal Issues in the Digital Age,* vol. 6, no. 1, pp. 124–148. DOI: 10.17323/2713-2749.2025.1.124.148

4. Bontempi D. et al. (2025) Face Age, a deep learning system to estimate biological age from face photographs to improve prognostication: a model development and validation study. *The Lancet Digital Health,* vol. 7, no. 6, p. 100870.

5. Cao X., Liu T. et al. (2024) Recent advances in nanozyme-based sensing technology for antioxidant detection. *Sensors*, vol. 24, no.20, p. 6616.

6. Cortes A., Johnston I. et al. (2025) The UK Biobank Whole-Genome Sequencing Consortium. Whole-genome sequencing of 490,640 UK Biobank participants. *Nature*, vol. 645, pp. 670–692. https://doi.org/10.1038/s41586-025-09272-9

7. Florea L., Diamond D. (2022) Sensors and "the internet of biochemical things". *Frontiers in Sensors*, vol. 3, pp. 1–7. https://doi.org/10.3389/fsens.2022.1010212

8. Garg M., Karpinski M. et al. (2024) Disease prediction with multi-omics and biomarkers empowers case–control genetic discoveries in the UK Biobank. *Nature Genetics*, vol. 56, pp. 1821–1831. https://doi.org/10.1038/s41588-024-01898-19.

9. Grishin S.M., Odintsov S.V. (2024) E-Health trends and practice of handling disputes on medical services using digital technologies. *Problemy ekonomiki i praktiki*=Issues of Economics and Practice, no. 5, pp. 43–50 (in Russ.)

10. Insani W. et al. (2025) Digital health technology interventions for improving medication safety: systematic review of economic evaluations. *Journal of Medical Internet Research,* pp. 1–16. DOI: 10.2196/65546

11. Ivanova A. P. (2021) Legal aspects of use of artificial intelligence in the field of health. *Sotsialnye i gumanitarnyie nauki. Otechesvennaya i zarubezhnaya literatura. Gosudarstvo i pravo. Referativnyi zhurnal*=Social and Humanitarian Sciences. Domestic and Foreign Publications. State and Law. Journal of Abstracts, no. 1, pp. 151–159 (in Russ.)

12. Kamensky S. (2020) Artificial Intelligence and technology in health care: overview and possible legal implications. *De Pual Journal of Health Care Law,* vol. 21, no. 3, pp. 4–12.

13. Koul A., Duran D. et al. (2025) Synthetic data, synthetic trust: navigating data challenges in the digital revolution. *The Lancet Digital Health,* vol. 7, no. 11, pp. 1–7. DOI: 10.1016/j.landig.2025.100924

14. Kravets I.A. (2022) Bioneuronconstitutionalism and dignity: theoretical foundations, dialogue of ethical and legal requirements and perspectives of interaction. *Zhurnal rossiyskogo prava*=Journal of Russian Law, no. 6. pp. 5–31 (in Russ.) DOI: 10.12737/jrl.2022.059.

15. Lee B., Ghovanloo M. (2019) An overview of data telemetry in inductively powered implantable biomedical devices. *IEEE Communications Magazine,* vol. 57, no. 2, pp. 74–80. DOI:10.1109/MCOM.2018.1800052

16. Lino C., Barrias S. et al. (2022) Biosensors as diagnostic tools in clinical applications. *Biochimica et Biophysica Acta–Reviews on Cancer*, vol. 77, no. 3, pp. 188726.

17. Magrani E. (2019) New perspectives on ethics and the laws of artificial intelligence. *Internet Policy Review*, vol. 8, no. 3, pp. 4–10. DOI:10.14763/2019.3.1420

18. Maity D. et al. (2023) Blood-Glucose-Powered Metabolic Fuel Cell for Self-Sufficient Bioelectronics. *Advanced Materials*, vol. 35, no. 21, pp. 1–14. DOI:10.1002/adma.202300890

19. Maleina M.N. (2020) Legal status of the biobank (bank of human biological materials). *Pravo. Zhurnal Vysshey shkoly ekonomiki*=Law. Journal of the Higher School of Economics, vol. 13, no. 1, pp. 99–100 (in Russ.)

20. Maleina M.N. (2023) Legal regulation of the use of medical robotic surgeons in the complex of digital technologies. *Meditsinskoye pravo*=Medicine Law, no. 1, pp. 2–5 (in Russ.)

21. Mokhov A.A. (2021) Biobanks and biobank activities require adequate legal protection. In: Bioeconomy: doctrine, legislation, practice. Moscow: Prospekt, pp. 339–349 (in Russ.)

22. Nusinovici S. et al. (2022) Retinal photograph-based deep learning predicts biological age, and stratifies morbidity and mortality risk. *Age and* Ageing, no. 4, pp. 1–9.

23. Ostanina E.A. (2023) Biobank as a legal category. *Yuridicheskiy zhurnal Samarskogo gosudarstvernnogo universiteta*=Legal Journal of the Samara State University, no. 2, pp. 66–67 (in Russ.)

24. Pugachev P.S., Gusev A.V. et al. (2021) Global trends in digital transformation of the health care industry. *Natsionalnoye zdravookhraneniye*=National Healthcare, no. 2, pp. 5-12 (in Russ.)

25. Osadchuk M.A. et al. (2020) Legal regulation in digital medicine. *Journal of Advanced Research in Law and Economics*, vol. 11, no. 1, pp. 148–155.

26. Raghu V., Weiss J. et al. (2021) Deep learning to estimate biological age from chest radiographs. *Journal of American College Cardiology,* vol. 14, pp. 2226–2236.

27. Ringeva M., Armel F. et al. (2025) Advancing health care with digital twins: meta-review of applications and implementation challenges. *Journal of Medical Internet Research,* vol. 27, p. 44. https://www.jmir.org/2025/1/e69544

28. Schroer D., Simon S., Trommer G. (2023) Medtech's generative Al opportunity. Available at: URL: https://www.bcg.com/publications/2023/generative-ai-in-medtech

29. Sheremetyeva N.V. (2024) Legal regulation and protection of the application of robotics and artificial intelligence in medical activities. *Meditsinskoye pravo*=Medicine Law, no. 3, pp. 40-43 (in Russ.)

30. Sen A. et al. (2024) Recent trends in nanozyme research and their potential therapeutic applications. *Current Research in Biotechnology,* vol. 7, p. 100205. https://doi.org/10.1016/j.crbiot.2024.100205

31. Sizov G. (2024) Digital transformation of primary health care in Moscow. *Natsionalnoye zdravookhraneniye*=National Healthcare, no. 3, pp. 41–52 (in Russ.)

32. Tarasenko C. et al. (2025) Methodology for assessing the digital maturity of medical organizations. *Vrach i informatcionnye tekhnologii*=Physician and Information Technologies, no. 3, pp. 76–89 (in Russ.)

33. Thirumala M., Monika S. (2024) Transforming healthcare: the power and potential of digital medicine. *Future Science OA*, vol. 10, no. 1, p. 2430357. DOI: 10.1080/20565623.2024.2430357

34.Voshev D.V. (2023) Review of methodologies and models for assessing digital maturity in primary health care bodies. *Nauka molodykh*=Science of Youthful, no. 4, pp. 615–627 (in Russ.)

35. Zalatan J., Petrini L., Geiger R. (2024) Engineering bacteria for cancer immunotherapy. *Current Opinion in Biotechnology,* vol. 85, pp. 1–13. DOI: 10.1016/j.copbio.2023.103061

36. Zargartalebi H., Mirzaie S. et al. (2024) Active-reset protein sensors enable continuous in vivo monitoring of inflammation. *Science*, vol. 386, pp. 1146–1153.

37. Zhou H., Baptista-Hon D. at al. (2024) Concepts and applications of digital twins in healthcare and medicine. *International Consortium of Digital Twins in Medicine,* vol. 5, no. 9, p. 101028. https://doi.org/10.1016/j.patter.2024.101028

Information about the author:
A.A. Kartskhiya — Doctor of Sciences (Law), Associate Professor.

The article was submitted to editorial office 22.11.2025; approved after reviewing 22.12.2025; accepted for publication 19.01.2026.

Legal Issues in the Digital Age. 2026. Vol. 7, no. 1.
Вопросы права в цифровую эпоху. 2026. Том 7. № 1.

E-Government And Cybersecurity

Research article
JEL: K00
UDK: 004:34(063)
DOI:10.17323/2713-2749.2026.1.121.140

Legal Specifics of Corporate Implementation of IoT Systems in the Republic of Tatarstan

Kyrill R. Kirushin, Danil I. Safin

[1,2] Naberezhnye Chelny State Pedagogical University, 28 Nizametdinov Str., Republic of Tatarstan 423806, Russia,

[1] k.kirushin@mail.ru, https://orcid.org/0000-0002-8958-3673

[2] danil-safin-2018@mail.ru, https://orcid.org/0000-0002-2375-5225

Abstract

Implementing technologies of Internet of Things (IoT) across core economic sectors of Russia's regions, including industry, utilities, logistics and health, entails considerable legal challenges for the security of data to be processed. The article provides a comprehensive analysis of the legal specifics of corporate implementation of IoT systems in Tatarstan as one of the leaders of digital transformation in Russia. The research was undertaken to identify legal problems arising from processing smart device data and make evidence-based proposals to improve regional regulatory and enforcement mechanisms. Methodologically, the study relies on analysis of federal and regional statutory regulation for protection of information and personal data, consolidation and systematization of regional legal practice in 2020–2024 as well as empirical research of corporate bylaws including model data processing consents and legal awareness for workers. It was found that digitization of economic sectors in Tatarstan leaves out major legal gaps including uncertain legal regime applicable to IoT-generated data, lack of provisions regulating such data flows, and fragmented technical protection standards. The authors propose a number of measures including a risk-differentiated IoT data regulation framework based on contextual anonymization, as well as model data processing requirements to be introduced to the regional law. A special focus is made on providing justification for the model for differentiation of administrative liability for offences in the area under study. The study's

practical value lies in shaping legal mechanisms to minimize legal risks for operators and to balance technological development with protection of data subjects' rights. The solutions proposed may be applicable both in Tatarstan and any other constituent territory faced with similar legal issues in the context of digital transformation of the economy.

Keywords

Internet of Things; personal data; Tatarstan; regional legislation; IoT systems; smart devices; data protection; administrative liability.

Acknowledgments: the paper is published within the project of supporting the publications of the authors of Russian educational and research organizations in the Higher School of Economics academic publications.

For citation: Kirushin K.R., Safin D.I. (2026) Legal Specifics of Corporate Implementation of IoT Systems in the Republic of Tatarstan. *Legal Issues in the Digital Age,* vol. 7, no. 1, pp. 121–140. DOI:10.17323/2713-2749.2026.1.121.140

Background

The digital economic transformation processes in the Republic of Tatarstan are becoming markedly systemic, especially at the regional level. This trend needs in careful analysis since it assumes compliance with a set of statutory requirements which regulate processing and protection of data, operation of critical information infrastructure, and security of information in the context of expanding digitization. Personal data protection and processing are basically regulated at the federal level particularly by Federal Law No. 152-FZ "On Personal Data"[1]. However, with general principles established at the federal level, these provisions require the involvement of constituent territories to be made specific, especially at the sectoral and regional level.

As follows from the study of IoT personal data regulation in Tatarstan, certain segments of industry, utilities, logistics and health demonstrate a high level of IoT implementation. In this regard, a study of regional enforcement practices and room for regulatory improvement (as part of powers available to constituent territories) on the example of these segments will allow to develop valuable proposals both for Tatarstan and other regions of the Russian Federation.

[1] Federal Law No. 152-FZ "On Personal Data" of 27 July 2006 (as amended) // Collected Laws of Russia, 2006. No. 31. Art. 3451 // SPS Consultant Plus.

1. Analysis of IoT Implementation Practices and Legal Challenges in Tatarstan's Key Sectors

Focusing on industry as a priority segment for IoT implementation, it is to be noted that Tatarstan's mechanical engineering and oil & gas companies showcase the most advanced practices of smart technology integration, with KAMAZ and "Zavod imeni Sergo" Integrated Works deploying complex industrial IoT platforms for continuous collection and analysis of data generated by their process equipment[2]. Introducing vibration and temperature sensors, power consumption meters, while allowing to streamline production processes, gives rise to new legal challenges related to classifying and protecting collected data. The main challenge results from legal uncertainty: telemetric data may at the same time have attributes of personal data (such as where a machine is linked to an operator), business secret (production efficiency parameters) as well as technical information not subject to any special protection regime.

A lack of clear criteria for delimitating these regimes in the federal law makes it hard for companies to identify adequate protection policies, only to create a risk of liability for non-compliance. Under the federal law and that of the Republic of Tatarstan, a large part of such data may be defined as business secret or restricted access data thus requiring corporate bylaws to be developed to regulate how they are processed, stored and transferred[3].

Regulating oil & gas telemetric data across the Republic of Tatarstan merits special attention. As follows from the practices of major companies such as Tatneft and Nisznekmskneftekhim[4], the systems for remote monitoring of oil wells and pipelines to measure pressure, fluid

[2] KAMAZ to gain 20% in capacity utilization through artificial intelligence implementation. Available at: URL:https://vestikamaza.ru/posts/kamaz_planiruet_na_20_podnyat_zagruzku_oborudovaniya_pri_pomoshhi_iskusstvennogo_intellekta/ (accessed: 20.11.2025); R. Khasanov: "Everybody wants a recirculator. But it is Germany where lamps come from...". Available at: URL: https://www.business-gazeta.ru/article/467380 (accessed: 20.11.2025)

[3] Ministry of Industry and Trade of Tatarstan. Order No. 44-OD "On approving personal data processing policy of the Ministry of Trade and Industry of Tatarstan" of 15 March 2023 // SPS Consultant Plus.

[4] Tatneft to form IT cluster. Available at: URL: https://rg.ru/2018/12/11/reg-pfo/tatneft-formiruet-it-klaster.html (accessed: 20.11.2025); SIBUR to save RUB 6.5 billion from introduction of digital technologies in 2024. Available at: URL: https://op-ex.ru/post_news/sibur-poluchil-ekonomicheskij-effekt-65-mlrd-rublej-ot-vnedreniya-czifrovyh-tehnologij-v-2024-godu/ (accessed: 17.11. 2024)

composition and corrosion processes will generate a flow of information which is economically valuable but at the same time potentially vulnerable from the perspective of data security. In this case the legal problem is sectoral rather than individual.

Since the oil & gas sector is part of the critical information infrastructure, its operators are to comply with Federal Law No. 187-FZ "On Security of the Critical Information Infrastructure"[5] that have laid down additional requirements to data protection not always accounting for the specifics of data automatically collected by IoT devices. Companies have to put in place multi-tiered protection arrangements which combine encryption technologies with different legal instruments (such as non-disclosure agreements, counterparty confidentiality agreements) and bylaws on data access management.

In Tatarstan's utilities sector, IoT technologies are implemented primarily as part of the smart city concept which assumes massive digitization of metering and resource management systems. In metropolitan centres like Kazan, Naberezhnye Chelny and Almetyevsk, automated energy metering systems (AEMS) are being deployed, with intelligent meters transmitting power, water and heat readings across wireless communication networks. From the legal perspective, operating such systems raises a number of important issues related to legal nature of collected data[6]. In particular, readings of meters linked to residential space can be regarded as personal data, only to oblige AEMS operators to comply with the requirement to seek consent of data subjects, provide for their right to access and rectify information, and to implement technical protection policies[7]. The above steps are envisaged by regulations such as FTECS Order No. 21 "On approving the list and contents of organizational and technical policies for the security of personal data processed by information systems" of 18 February 2013[8] and FSS Order

[5] Federal Law No. 187-FZ "On Security of the Critical Information Infrastructure of the Russian Federation" of 26 July 2017 (as amended) // Collected Laws of Russia. 2017. No. 31. Art. 4724.

[6] Ministry of Construction, Architecture and Utilities of Tatarstan. Order No. 35/o "On approving the Provision for processing personal data of the Ministry workers" of 12 March 2018 // SPS Consultant Plus.

[7] Federal Law No. 152-FZ of 27 July 2006 // Collected Laws of Russia. 2006. No. 31. Article 3451.

[8] FTECS Order No. 21 of 18 February 2013 " On approving the list and contents of organizational and technical policies for the security of personal data processed by personal information systems" // SPS Consultant Plus.

No. 524 "On approving encryption (cryptography) based data protection requirements for state information systems" of 24 October 2022[9]. The doctrine highlights that compliance with the said technical policies including certification of protective technologies is a prerequisite of personal data security [Melnikov P.A., 2018: 182].

With Tatarstan's strategic position as the key transportation hub of the Volga Region, the logistical sector demonstrates a high degree of readiness to implement IoT technologies. At the Kazan multimodal logistical center and the Sviyazhsk port facilities GPS/GLONASS trackers are widely used for cargo traffic monitoring, RFID markers for warehouse inventory automation, and micro-climate sensors for refrigerated containers[10]. Operating these systems requires compliance with cross-border data transfer provisions, especially for shipments to member states of the Eurasian Economic Union. Under Article 12, Federal Law No. 152-FZ[11], personal data is not allowed to cross borders unless adequate protection is ensured.

In Tatarstan's health system, IoT technologies are implemented as part of the regional project "Building a shared digital loop in health based on the universal health information system" which assumes integrated remote patient monitoring systems and automated drug dispensing[12]. Platforms deployed at Tatarstan's health institutions enable data from portable devices (glucometers, blood pressure meters, pulsometers) to be uploaded to patient health records[13]. Processing such data calls for higher protection requirements since health data is part of the special category of personal data under Article 10 of Federal Law No. 152-FZ. Moreover, the use of IoT applications raises a number of issues related to the data subject's consent to data processing and user profiling based on

[9] FSS Order No. 524 of 24 October 2022 "On approving encryption (cryptography) based data protection requirements for state information systems" // SPS Consultant Plus.

[10] Irek Salikhov's quiet triumph: how the Sviyazhsk logistical center comes alive. Available at: URL: https://www.business-gazeta.ru/article/553001 (accessed: 20.11.2025)

[11] Federal Law No. 152-FZ of 27 July 2006 // Collected Laws of Russia. 2006. No. 31. Article 3451.

[12] Cabinet of Ministers Resolution No. 431 "On approving the Provision on the state information system "E-Health Care" in the Republic of Tatarstan" of 11 May 2022 // SPS ConsultantPlus.

[13] One thousand people on remote health monitoring in Tatarstan. Available at: URL: https://tass.ru/v-strane/17890215 (accessed: 31.10. 2025)

collected data, only to call for more clear legal regulation [Linkov V.V., Semyonov E.Yu., 2020: 193].

The emerging practice shows that health institutions are to seek the patient's consent in writing to process health data; use certified encryption technologies for data transfer; make the data available only to authorized personnel; and maintain personal data access logs. Cases of data processing consent being recalled by the patient, as well as limits of unsolicited personal data processing in cases envisaged by law for delivering aid may be especially challenging [Lyutsko V.V., Sveredyuk M.G., Stupak V.S., 2021: 506–508].

In analyzing the regulatory framework for implementing IoT in Tatarstan it is worth noting its multi-tiered structure, with Federal Laws No. 152-FZ, No. 187-FZ and No. 149-FZ "On Information, Information Technologies and Data Protection" as the key regulators at the federal level supported at the regional level by the 2030 Socioeconomic Development Strategy of Tatarstan, Tatarstan Cabinet of Ministers Resolution No. 748 "On approving the Strategy for digital transformation of economic sectors, social services and public governance in Tatarstan" of 18 March 2021, Smart City Program approved by the Cabinet of Ministers; departmental acts by the Ministry of Digitization of Public Governance, Information Technologies and Communications etc. Meanwhile, there is a considerable deficit of specialized provisions to regulate specific aspects of IoT operation. In fact, the legal status of IoT-generated data has not been clarified; procedure for distribution of liability between the system operator, equipment vendor and user has not been regulated nor common requirements to cross-border transfer of telemetric data established.

Empirical study reveals a number of legal problems: as a result of uncertain regime, the same data can be simultaneously qualified as personal data, business secret or classified information (with different interpretation of data likely to create the risk of unjustified disclosure resulting in administrative and criminal liability); a lack of common technical standards for encryption and authentication increases IoT vulnerability as confirmed by hacks of smart meters in the utilities sector; and fragmented regulatory requirements obstruct the development of shared corporate policies for data security forcing companies to draft their own bylaws not always in conformity with federal law.

Due to technical constraints of connected devices (low power consumption, small shape, limited computing resources), the traditional

methods of protection, such as encryption and authentication, need to be considerably adapted, something that complicates the emergence of shared security systems [Polegenko A.M., 2018: 42]. Meanwhile, personal data vulnerability, abuse of information technologies and inadequate informatization of individuals are the main challenges for the exercise of individual rights in the context of digitization [Zinovieva E.A., 2022: 98].

The Republic of Tatarstan showcases advanced approaches to minimize IoT-related legal risks. In 2024, the Center for Competencies in IoT Cybersecurity was set up on the basis of Kazan's IT-park to develop compliant model contracts for IoT system operators; perform data system audits for compliance with personal data law; and organize education programs on legal aspects of cybersecurity. With legal sandboxes introduced in the Elabuga special economic zone, certification of IoT devices is facilitated while maintaining requirements to data protection which allows to expedite the dissemination of innovative practices and to minimize legal barriers[14].

Thus, the IoT implementation in Tatarstan, while being characterized by high technological maturity and active government support, presents considerable legal challenges. Going forward will require regulations to specify requirements to IoT data processing; harmonizing sectoral standards with the federal law; developing mechanisms for cross-border data transfer within the EAEU; capacity building in the area of legal regulation of cybersecurity. Unless these challenges are addressed, any massive implementation of IoT technologies is likely to increase the legal risks related to the breach of data confidentiality, integrity and accessibility, something that will require a responsible corporate approach to compliance with regulatory requirements.

2. Judicial Practice of Protecting IoT-collected Personal Data (2020–2024)

The analysis of Tatarstan's judicial practice in 2020-2024 reveals a gradual emergence of sustainable approaches to resolution of disputes related to processing of IoT-collected personal data. Characteristically, a majority of cases were brought by individuals whose rights were vio-

[14] SOLLERS Plant in the Alabuga SEZ has implemented IoT and Big Data technologies to streamline production. Available at: URL: https://dzen.ru/a/aFFfn38a1G6hKUve (accessed: 20.11.2025)

lated through unauthorized collection, storage or transfer of data generated by smart devices (such as household sensors and corporate monitoring systems).

Claims for unauthorized IoT data transfer to a third party constitute a typical category. In one arbitration case, the plaintiff proved that the operator of a smart door phone system would transfer CCTV data to marketing agencies without house residents' consent. With reference to Article 7 and 9 of Federal Law No. 152-FZ, the court has recognized the operator's actions as illegal, required to stop data transfer and collected 50 000 roubles in moral damages. As an important legal conclusion, IoT camera footage was recognized personal data subject to specific protection[15].

Under another case related to a breach in biometric data processing, criminal charges were brought against a network of fitness clubs which used smart bracelets to collect data on clients' heart rate and physical activity. As established by court, the biometric data processing consent was general and, contrary to requirements of part 4, Article 9 of Federal Law No. 152-FZ, did not specify the purpose and dates. The court ruling provided for deletion of illegally collected data and assigned a penalty of 30.000 roubles for violation of the consent procedure[16].

Another question addressed by judicial practice is assessment of technological protection of personal data as exemplified by an arbitration claim against a vendor of smart speakers whose units would transfer audio recordings to servers without notifying users. The court has invoked a need to comply with FTECS Order No. 21 of 18 February 2013[17] that required protection from unauthorized access. The ruling included an order to refine the software and a penalty of 70.000 RUB[18].

Inadequate public awareness of the nature of IoT-collected data; regulatory gaps related to cross-border transfer of device-generated data; a lack of harmonized encryption standards for low-power IoT sensors;

[15] Supreme Court of Tatarstan. Ruling No. A33-12456/2022 of 04 October 2022 // SPS Consultant Plus.

[16] Documents of criminal case No. 2-345/2023 // Archive of Vakhit District Court of Kazan, Tatarstan.

[17] FTECS No. 21 "On approving the list and contents of organizational and technical policies for the security of personal data processed by personal information systems" of 18 February 2013 // SPS Consultant Plus.

[18] Supreme Court of Tatarstan. Ruling No. A33-2345/2024 of 12 November 2024 // SPS Consultant Plus.

and problems of proving causal relationships between the operator's behavior and damage are still among the key problems identified by judicial practice. Nationwide, judicial practice also reveals typical categories of offences such as unsolicited transfer of personal data to third parties, denial of information and unauthorized access to data, only to confirm that the identified problems are systemic [Miller I.P., 2017: 387–388]. Meanwhile, the regional experience finds new ways to protect IoT-generated personal data (such as enhancing the role of expert cybersecurity reviews in examining administrative and civil claims; shaping the precedents for collective protection of rights).

The analysis of Tatarstan's judicial practice reveals a trend for tougher legal protection of personal data subjects in the context of digitization of everyday life and production. In handling IoT-related disputes, courts will qualify smart device data (including audio and video streams) as subject to the personal data regime. It is notable that this practice is largely driven by individuals. While this suggests higher legal awareness of digital privacy, the still remaining gaps in regulation and security standards complicate the process of proving. Regional courts demonstrate readiness to apply not only sectoral law but also technical regulations in assessing adequacy of protection policies which is indicative of a shift from formal approach to intrinsic assessment of abuse. This allows to conclude that the regional judicial practice is not only apt to promptly respond to technological challenges but also contributes to identify new opportunities for better protection of rights of personal data subjects in the digital age.

3. The Issues and Organizational Model of Legal Awareness for Workers in Context of IoT Expansion

In context of wide-ranging digital economic transformation of Tatarstan, IoT technologies are systemically introduced at scale, with smart sensors integrated consistently into production processes at industrial companies, facial recognition enabled CCTC systems deployed at state organizations and business centers, and portable devices widely harnessed in corporate health programs. This technological dynamics results in an acute and ever growing need for workers' legal awareness of how to protect personal data collected by IoT devices.

To appreciate scrupulously the context of IoT implementation in Tatarstan, one should turn to the data reported by the Ministry of Digital Development of Public Governance, IT and Communications. Accord-

ing to their statistics, a number of major projects extensively involving IoT technologies were implemented in the republic in 2023– 2024[19]. These included the digitization of utilities with smart sensors installed at residential buildings in Kazan and Naberezhnye Chelny; implementation of video analytics systems at oil & gas companies; deployment of smart offices at executive government agencies; and the use of portable devices at large companies as part of their corporate health care programs.

As follows from the practice, personal data leaks are mostly often caused by human factor, only to confirm a need for systemic development of skills of those authorized to process data, and a need for the development of corporate regulations [Veprev S.B., Nesterovich S.A., 2021: 154–155]. These initiatives inevitably entail massive collection of various personal data – such as biometric (fingerprints, facial recognition), geopositioning (tracking movements across production facilities), behavioral (analyzing workplace activities), and physiological (cardiac rate etc.). Moreover, under Article 3, Federal Law No. 152-FZ, any information that allows to identify a natural person, is subject to binding legal protection. This will impose serious obligations on corporate entities to ensure confidentiality and security of the data they collect.

Regional rule-making experience, particularly in the Altai Region, shows that specifying the requirements to standard processing consent regionally will allow to fill the gaps in federal law for better protection of data subjects [Kovalenko K.E., Kovalenko N.E., 2020: 128]. The flaw that stands out in the first place is unclearly formulated purpose of data processing. Documents abound with generalized, fuzzy phrases (such as "to ensure the facility's security", "to optimize work processes") which do not mention any data usage scenarios. For example, it is not explained how the data may be used to analyze staff performance at large companies such as PJSC KAMAZ or JSC TANEKO; it is not stated how long the data will be stored (including at regional data processing centers); and no list of persons authorized to access the collected data is provided (including at Tatarstan's subcontracted IT companies)[20].

[19] Monitoring regional law for digital economic development across the ARIR. Available at: URL: https://cesi.tatarstan.ru/file/pub/pub_1613527.pdf (accessed: 20.11.2025)

[20] PJSC KAMAZ personal data processing policy. Available at: URL: https://kamaz.ru/about/policy/politika-personalnykh-dannyh/; JSC TANEKO personal data processing policy. Available at: URL: https://taneco.tatneft.ru/politika_v_otnoshenii_obrabotki_pnd.pdf (accessed: 08.11.2025)

Workers' low awareness of the technology behind regional IoT platforms is a matter of special concern. In most cases, they do not have detailed information on operating principles of integrated systems (for example, when they interact with the Smart City platform), data anonymization methods used by local IT providers, and data leakage protection mechanisms in the context of cross-regional exchange. Such information asymmetry considerably narrows the room for informed decision making with regard to consent to process personal data.

Legal awareness for Tatarstan's workers on protecting IoT-collected personal data should take into account a number of specific factors shaped by the regional context. In the first place, it should account for sectoral specifics: training for oil & gas workers (TANEKO, Nizhnekamskneftekhim) should be focused on protecting data collected by industrial security systems while that for government workers on compliance with data processing requirements within the framework of Smart City projects. The language factor is important: training documents should be available both in Russian and Tatar since production teams are multinational. Moreover, it is crucial for awareness programs to incorporate explanations of regional regulations (such as Cabinet of Ministers resolutions on the use of IoT systems at municipal agencies). Review of regional practices of the Federal Service for IT Supervision is also of considerable value: it is crucial for workers to be aware of typical violations identified in the course of inspections in Tatarstan such as a lack of data protection bylaws at small businesses.

In building a system for legal awareness, it is expedient to rely on a number of core principles that can be usefully classified as follows:

— contextuality: detailed explanation of what data is exactly collected (for example, access control to the Cabinet of Ministers' buildings, smart bus sensors in Kazan; portable devices at facilities of the special economic zone);

— risk visualization: using visual aids (bilingual infographics), and regional case studies including data leakage incidents, for example, at health institutions in Tatarstan;

— interactivity: trainings imitating typical situations (for example, the course of action when regional authorities require access to data or when suspicious IoT activity is identified at JSC Tatneft facilities);

— regularity: annual training workshops focused on the latest amendments including requirements of the Ministry of Digital Development

taking into account the implementation of new IoT technologies (such as facial recognition systems in Kazan's metro).

A model of four consecutive interrelated stages is proposed for a corporate system of legal awareness to be systemically implemented in Tatarstan. In our view, these stages should cover: diagnostics, content processing, implementation and performance evaluation.

Diagnostics should cover comprehensive audit of IoT devices in use always taking into account the register of regional IT solutions, and an analysis whether the data processing consents comply with requirements of Federal Law No. 152-FZ and Cabinet of Ministers resolutions. As an important point, diagnostics should identify "blind spots" in workers' awareness via questionnaires in Russian and Tatar.

At the educational content stage, bilingual checklists should be designed for detailed explanation of the essential technical terms such as "anonymization" and "tokenization". It is useful to have video guidance to demonstrate how to deal with privacy settings of IoT devices widely used in Tatarstan (for example, smart home sensors supplied by local providers). A special focus should be on case studies to be developed with a view to regionally registered incidents to make trainings as much practical and practice-oriented as possible.

The implementation stage assumes the delivery of induction courses for new personnel adjusted for sectoral specifics. Thematic webinars for division managers should be organized in this vein for a detailed discussion of requirements by the regional Ministry of Digital Development and of the latest regulatory amendments. Meanwhile, it is possible to use simulation games for adequate response to typical incidents (such as utilities sensor data leakage). A multi-tiered approach will allow to cover all worker categories taking into account how they deal with IoT devices as part of their functional responsibilities under the employment contract.

The final stage is evaluating performance of awareness trainings which can be done through comprehensive testing of workers' knowledge in Russian and Tatar, monitoring the dynamics of requests to the corporate data protection service, and analyzing changes to the number and nature of offences identified by the regional office of the Federal Service for IT Supervision. Regular collection and analysis of these indicators will allow to timely adjust the contents and methods of awareness training based on the identified knowledge gaps and relevant needs of the workers in question.

Thus, legal awareness of protecting IoT-collected personal data for workers in Tatarstan requires a comprehensive approach to account for the region's sectoral specifics (oil & gas, public services, utilities); a need for bilingual presentation of learning materials covering regional case studies; importance of cooperation with the regional government (Ministry of Digital Development and regional office of the Federal Service for IT Supervision); and a need for regular program update to account for dynamic development of the regional digital infrastructure.

4. Improving Legal Mechanisms to Protect IoT-generated Data

Explosive progress of digital technologies and widespread introduction of IoT devices make the improvement of the regulatory framework for protecting personal data a matter of urgency. In demonstrating a leading edge in digitization, Tatarstan is facing legal challenges characteristic of the whole Federation. This objectively calls for a need to improve the regional legal mechanisms. Many countries already have in place regulatory policies for security and protection of IoT-related personal data including special laws & standards, something that confirms a need in similar approaches to be pursued in Russia [Kuchkovskaya N.V., 2023: 353–354].

While constituent territories may adopt regulations within their competence to specify federal requirements, Tatarstan may and should develop its own regulatory framework with reliance on Article 4, Federal Law No. 152-FZ which allows for departmental and regional regulations to be adopted on specific issues. Instead of being a duplicate or substitute, this framework should specify the federal law with regard to specific aspects of processing IoT-generated data and sectoral specifics of the regional economy (industry, utilities, health care). In the modern environment, personal data are increasingly generated without direct human involvement. As a unique feature, such data are generated at scale and can contain information on user behavioral patterns, something that calls for legal mechanism to regulate how they are processed and protected.

A system for monitoring personal data security in the IoT infrastructure is of critical importance. Such system should comprise the mechanisms for regular audit of protective capabilities, assessment of security risks, incident analysis and choice of preventive policies, and also for producing statistical reports on data protection status. In the context of digital economic development, it is increasingly important to ensure

public control over personal data processing in the IoT environment. It is necessary to set up control units, develop system security methodologies, define review frequency and identify criteria of compliance with security requirements [Drilenko D.V., Fedyaev S.M., 2025: 133–134].

In the modern context of economic digitization and explosive implementation of IoT technologies, it is crucial to develop a system regulating how IoT-collected data are processed, stored and transferred. As a leader in digitization, Tatarstan is in need of a regional regulation that accounts for data processing specifics in the context of smart systems implemented at scale.

In the modern landscape of digital technological change and widespread IoT implementation across Tatarstan, it is becoming a priority to improve the mechanisms of administrative liability for breaching personal data security. The system of legal provisions needs to adapt to the specifics of IoT infrastructure and new categories of offences. The analysis of regulations points to a lack of regulatory framework to qualify administrative violations regarding IoT-related personal data processing. A need to account for specific aspects of IoT technologies in establishing liability is also stated in modern studies of the legal nature of IoT [Zabaikin Yu.V., Lunkin D.A., 2023: 331–332]. Provisions of the Code of Administrative Offences (hereinafter CAO) such as Article 13.11 ("Violations of Russia's personal data law") are of general nature and do not account for technological specifics of automated data collection. The latest amendments such as adding Article ст. 272.1 to Russia's Criminal Code (CCR) and new elements to CAO Article 13.11 to provide for turnover-based fines suggest a trend towards harsher liability of operators for data leakages. However, the IoT specifics is still out of the legislator's focus [Kovalev S.D., 2024: 272–273].

It has a sense thus to propose to differentiate administrative liability for violating personal data protection. We understand a differentiated system of administrative liability in the IoT context as containing the qualifying attributes of constitutive elements that allow to delimitate liability depending on: amount of processed data (large-scale collection); data type (biometric, geopositioning); implications (damage to critical infrastructure); subject of liability (operator, vendor). Any extension of the grounds for unsolicited data processing including references to operator legitimate interests should be accompanied by clearly defined criteria and restrictive interpretation to avoid unjustified invasion of privacy [Davymoka S.V., 2025: 448–449].

The regulatory scope of such system is principally important. Under Russian Federation Constitution (para "k", part 1, Article 72), both the federation and its constituent territories have the competence over administrative and administrative procedure law. Meanwhile, establishing constituent elements (dispositions and sanctions) is a prerogative of the federal legislator. Thus, rather than developing regional-level constituent elements of IoT-related offences (something that would extend beyond its competence), Tatarstan should work to exercise the right to legislative initiative and draft proposals to amend federal law, and to specify the procedure for invoking liability in regional regulations as part of the powers available to any constituent territory. To implement this idea, we propose the following steps on the example of Tatarstan:

— drafting model procedures for IoT operators to cooperate with supervisory authorities including for investigating incidents and building the evidence base;

— approving regional methodological guidance for judges and officers of the Federal Service for IT Supervision to qualify IoT-related offences in accounting for sectoral specifics (such as unauthorized collection of biometric data in smart city systems);

— proposing to differentiate constituent elements of administrative offences by adding qualifying attributes to the CAO to account for specifics of IoT systems (it is particularly proposed to add aggravating circumstances (constituent elements) to CAO Article 13.11 such as "processing personal data automatically generated by devices (telemetric data) without notifying the data subject"; "unsolicited cross-border transfer of IoT data collected at critical information infrastructure facilities"; "failure by the operator to timely notify of any incident causing leakage of biometric personal data from IoT systems");

— implementing corrective mechanisms (warnings, instructions) available within the regional competence to promptly respond to IoT system vulnerabilities identified at utilities and health organizations.

Moreover, a major vector is improving legal awareness and local rule-making so that data operators can themselves minimize the risk of non-compliance already at the stage of IoT system design.

Thus, the proposed administrative liability system has two levels: the federal level (establishing differentiated constituent elements of offences in the CAO) and the regional level (developing methodological guidance for enforcement agencies, cooperation procedures and preventive

policies). Implementing the proposed steps with a view to respective scopes of competence will allow to put in place a useful mechanism of administrative prosecution for violations of personal data protection by IoT systems in accounting for their specifics, something that will contribute to better protection of personal data subjects' rights in the context of development of digital technologies.

5. The Concept of Special Legal Regime for IoT Data Processing

The analysis of enforcement practices and identified regulatory gaps points to a need for comprehensive approach to data protection. Such approach, in our view, should assume the improvement of liability mechanisms and the development of a principally new concept of regulating data as such.

In contrast to the general personal data regime governed by the Federal Law "On Personal Data", the proposed regime is to account for operational features of IoT technologies including continuous collection of data at scale, their close links with critical information infrastructure facilities, and highly automated processing without direct human involvement. This article proposes basic elements of such a regime as adapted to the regional level exemplified by Tatarstan. Integrating data protection principles into the international regulatory framework and establishing clear rules for ethical use of AI (such as transparency, accountability, equity and non-discrimination) is crucial for developing a global standard for responsible use of new technologies [Amramova A.G., 2024: 48–50].

Thus, the "contextual anonymization" principle can be the first element of the proposed regime. Unlike total anonymization capable of rendering data useless for achieving the goals in industry or utilities, the proposed rule will allow to process the collected data (telemetry, meter readings) in an anonymized form to generate statistics and optimize processes. Moreover, the said data could be "reversibly de-anonymized" through the use of encryption and strictly audited procedure solely in cases explicitly envisaged by law, such as accident investigation at critical data infrastructure facilities or justified request by judicial authorities. Implementing this principle will allow to remove a conflict whereby the same information can be simultaneously regarded as a business secret and potential personal data.

Differentiating the legal status of data could be the second element. It is thus proposed to qualify IoT-generated data by the extent of risk

for data subject rights by adopting regional level regulations or initiating amendments at the federal level. Low risk data are proposed to include meter readings at residential buildings and aggregated device utilization statistics unrelated to operator where basic protection requirements apply. Medium risk data include corporate vehicle geopositioning, system access control and telemetry linked to operator workplace, something that requires stronger authentication and encryption. High risk data comprise biometric information such as facial recognition and fingerprints, as well as health indicators generated by portable devices where the strongest protection – such as encryption, operation licensing and secure storage – will apply. Using biometric data involves a number of major threats such as room for data manipulations, hidden surveillance and introduction of social rating systems, only to require special care on the part of the legislator [Zhirnova N.A., Kovaleva N.N., 2024: 112–115].

Finally, developing and introducing a regional-level standard for responsible implementation of IoT technologies can provide the third element of the proposed concept. With the powers afforded to constituent territories by Article 4, Federal Law "On Personal Data" and considering the successful experience of the Alabuga special economic zone, it would be expedient that Tatarstan's Cabinet of Ministers adopts a resolution to approve "Model requirements to organizing data processing in departmental and municipal IoT systems". The document can contain mandatory wordings of data processing consents to specify the purpose of such processing and remove fuzzy language revealed by analysis of bylaws. Moreover, it could provide minimum technical standards of encryption for various types of devices depending on their energy consumption, and a procedure for cooperation between IoT system operators and the Federal Service for IT Supervision (regional office) and the Ministry of Digital Development in the event of incident including period of notice and composition of an investigation commission.

Implementing the above elements at the regional level will shape a regulatory environment to minimize the risks revealed by analysis of judicial practice without waiting for the process of amendments to federal law that may be lengthy.

Conclusions

So, Tatarstan showcases a high extent of economic digitization as confirmed by widespread implementation of IoT technologies in in-

dustry, utilities, logistics and health. The region's major companies are actively integrating smart systems into their production and managerial processes. The analysis of regulations shows that while the federal regulatory framework (in the first place Federal Law No. 152-FZ) provides a brickwork for personal data protection, it needs to adapt to the specifics of data processing in the IoT context. Considerable regulatory gaps (uncertainty of legal regime applicable to data, lack of common standard) are found on the federal level. Against this backdrop, the role of regional law is to promptly specify federal provisions via sectoral rules, develop model documents (consents, policies) and to improve legal awareness. The measures proposed by the study relying on regional practices in Tatarstan and accounting for federal provisions can be upscaled given compliance with federal law and in light of subsequent implementation of the best regional practices in federal regulations and sectoral standards for use elsewhere in the Russian Federation to minimize legal risks associated with IoT technologies.

A study of IoT implementation practices in the region's key economic sectors allowed to identify a number of systemic problems. In particular, it was found that corporate bylaws failed to comply with personal data protection requirements, only to put data subjects' rights increasingly at risk. This problem is especially acute in the utilities sector and at small businesses in the logistics sector. While the judicial practice in Tatarstan reveals a trend towards sustainable approaches to resolution of personal data related disputes, legal mechanisms need further improvement. The analysis of court rulings suggests a need for harsher liability for violating personal data protection, with secure preventive arrangements to be developed. The study contains proposals for regulatory improvements substantiating a two-tiered model to differentiate administrative liability related to personal data offences; proposing and detailing the concept of special legal regime for IoT-generated data. The steps proposed in the study can be useful not only in Tatarstan but also in other regions facing similar problems.

References

1. Abramova A.G. (2024) New technologies and their importance for personal data protection (Internet of Things, Artificial Intelligence). *Vestnik Rossiysko-Armyanskogo (Slavyanskogo) universiteta: gumanitarnye i obshchestvennye nauki*=Bulletin of the Russian-Armenian Slavic University, no. 2, pp. 44–52 (in Russ.)

2. Davymoka S.V. (2025) The rights and legitimate interests of the personal data operator. *Sovremenniy ucheniy*=Contemporary Researcher, no. 7, pp. 446–450 (in Russ.)

3. Drilenko D.V., Fedyaev S.M. (2025) Legal regulation of context-dependent IoT sensors and machine vision technologies: conflict of Federal Law No. 152-FZ and Federal Law No. 572-FZ in biometric data processing (regulatory analysis and empirical study of judicial practice in 2018–2025). *Nauchnye trudy Kubanskogo gosudarstvennogo tekhnologicheskogo universiteta*=Proceedings of the Kuban State Technological University, no. 5, pp. 123–139 (in Russ.)

4. Kovalenko K.E., Kovalenko N.E. (2020) Correlation of federal and regional legislation in the field of personal data protection. Evolutsiya rossiyskogo prava. Papers of proceedings of international conference of young scientists and students. Yekaterinburg: Ural State Law University Press, pp. 127–128 (in Russ.)

5. Kovalev S.D. (2024) Overview of recent changes in the Federal Law "On Personal Data". *Agrarnoe i zemelnoe pravo*=Agrarian and Family Law, no. 12, pp. 272–274 (in Russ.)

6. Kuchkovskaya N.V. (2023) Evolution of IoT law. *Voprosy rossiyskogo i mezhdunarodnogo prava*=Issues of the Russian and International Law, vol. 13, no. 4, pp. 350–356 (in Russ.)

7. Linkov V.V., Semenov E.Yu. (2020) Legal issues of personal data protection in integrating the Internet of Things into everyday life. *Zakon i pravo*=Law and Legislation, no.10, pp. 193–195 (in Russ.)

8. Lyutsko V.V., Sveredyuk M.G., Stupak V.S. (2021) The patient's withdrawal of personal data processing consent from a health institution: legitimacy & possible regulation. *Sovremennye problemy zdravookhraneniya i meditsinskoy statistiki*, =Contemporary Issues of Healthcare and Medical Statistics, no. 4, pp. 502–514 (in Russ.)

9. Melnikov P.A. (2018) Analyzing Russia's regulatory framework for personal data protection. Innovative potential of youth: social, environmental and economic sustainability. Proceedings of the international youth research conference. Yekaterinburg: Ural Federal University Press, pp. 179–183 (in Russ.)

10. Miller I.P. Legal aspects of using personal data when using electronic services. Urban Environment Safety. Proceedings of international conference. Omsk: Omsk State Technical University Press, pp. 385–389 (in Russ.)

11. Polegenko A.M. (2018) Peculiarities of information protection in the Internet of Things. *International Journal of Open Information Technologies,* vol. 6, no. 10, pp. 41–45.

12. Veprev S.B., Nesterovich S.A. (2021) Measures for improving the security of personal data in the Internet. Information Security: yesterday, today, tomorrow. Collection of articles based on proceedings of international scholar and practical conference. Moscow: Russian State Humanitarian University Press, pp. 153–158 (in Russ.)

13. Zabaikin Yu.V., Lunkin D.A. (2023) Internet of Things: legal aspects of use. *Voprosy rossiyskogo i mezhdunarodnogo prava*=Issues of Russian and International Law, vol. 13, no. 4-1, pp. 329–335 (in Russ.)

14. Zhirnova N.A., Kovaleva N.N. (2024) Personal data confidentiality problems in artificial intelligence systems. *Zhurnal rossiyskogo prava*=Journal of Russian Law, vol. 28, no. 7, pp. 109–121 (in Russ.)

15. Zinovieva E.A. (2022) Exercising individual rights and freedoms in the context of digitalization. *Problemy ekonomiki i yuridicheskoy praktiki*=Issues of Economics and Legal Practice, vol. 18, no. 4, pp. 94–99 (in Russ.)

Information about the authors:

K.R. Kirushin – Candidate of Sciences (Law), Senior Lecturer.
D.I. Safin – Assistant.

The article was submitted to editorial office 24.12.2025; approved after reviewing 28.01.2026; accepted for publication 28.01.2026.

Legal Issues in the Digital Age. 2026. Vol. 7, no. 1.
Вопросы права в цифровую эпоху. 2026. Том 7. № 1 .

Research article
JEL: K 14
УДК: 343.71
DOI:10.17323/2713-2749.2026.1.141.163

Criminal Law Compliance with Cyber Resilience Testing of Information Systems (Penetration Testing and Bug Bounty)

Evgeny Aleksandrovich Russkevich

Kutafin Moscow State Law University, 9/2 Sadovaya-Kudrinskaya Str., Moscow 123342, Russia,

russkevich@mail.ru, https://orcid.org/0000-0003-4587-8258

Abstract

The increasing dependence of individuals, society, and the state on digital technologies is driving a growing demand for computer system security services. A distinct cybersecurity market has already emerged in Russia, with estimated turnover in the multi-billion dollar range (at the end of 2024, the market size was 593.4 billion rubles). One significant segment of the industry is the provision of services related to comprehensive and in-depth testing of information systems for resistance to cyberattacks (penetration testing). At the same time, the practice of crowdsourcing information system security analysis (bug bounty) is rapidly developing, allowing anyone to participate in testing an information system and, if a vulnerability is discovered, receive a reward. The goal of this research is to develop theoretical recommendations and proposals for mitigating criminal risks arising during cybersecurity testing of information systems. The research is based on the application of general scientific and specialized methods (analysis, synthesis, induction, formal legal, abstract logical, etc.). In the absence of specific legal regulation, “ethical hackers” searching for vulnerabilities in information systems undoubtedly expose themselves to the risk of criminal prosecution. Therefore, addressing this issue requires defining a legal framework for cybersecurity testing of information systems. The paper concludes that, when testing the security of a computer system, a specialist possessing the necessary knowledge and relying on proven methods and tools strives to achieve

a socially beneficial result. However, they always accept (even if only to a small degree) the risk of system failure with subsequent possible negative consequences, such as an emergency shutdown of automated process control systems, equipment failure, data destruction or blocking, etc. Such behavior by a specialist, as well as the corresponding consequences, fully complies with the provisions of criminal law on justified risk (Article 41 of the Criminal Code of the Russian Federation). Based on the research, the article offers several recommendations for mitigating the criminal risks of cybersecurity testing of information systems.

Keywords

pentesting; bug bounty; computer crimes; criminal compliance; cybersecurity; white hat hackers.

For citation: Russkevich E.A. (2026) Criminal Law Compliance with Cyber Resilience Testing of Information Systems (Penetration Testing and Big Bounty). *Legal Issues in the Digital Age,* vol. 7, no. 1, pp. 141–163. DOI:10.17323/2713-2749.2026.1.141.163

Introduction

Penetration testing is a contemporary practice in securing digital infrastructure against computer attacks. Broadly speaking, a penetration test involves assessing a system's security by identifying and exploiting vulnerabilities using hacking techniques [Reddy P.S., Pelletier J.M., 2022: 1117–1125].

Over time, this has emerged as a distinct segment of the information security market. According to MarketsandMarkets studies, the global penetration testing market was valued at USD 1.7 billion in 2024 and is projected to grow to USD 3.9 billion by 2029. As cybercrime becomes more sophisticated and technologically advanced, users will require sophisticated penetration testing tools to stay one step ahead of rapidly evolving digital threats. High standards of data protection will drive demand for reliable penetration testing solutions. The penetration testing market is expected to continue its upward trajectory, driven by the rise in cybercrime and increasingly stringent regulatory legislation on information security[1].

The penetration testing process involves assessing the security of an IT infrastructure against current threats by analysing its architecture and identifying vulnerabilities. It is important it can only be effectively imple-

[1] Penetration Testing Market Size, Size, Growth & Latest Trends. Available at: URL: https://www.marketsandmarkets.com/Market-Reports/penetration-testing-market-13422019.html (дата обращения: 05.09.2025)

mented by conducting "test hacking", whereby the system being tested must demonstrate its ability to withstand malicious attacks in real-world conditions. In the worst-case scenario, the tester discovers that the IT asset has failed the security check and has been compromised. In this case, the report provides an explanation and lists the identified vulnerabilities.[2]

The doctrine notes the key difference between unauthorised access ("hacking") and penetration testing is that hackers breach a system to obtain sensitive information and cause damage, whereas penetration testing specialists identify security vulnerabilities that could be exploited and help you address them [Tudosi A.-D., Graur A., Balan D.G., Potorac A.D., 2023].

Penetration testing is important for assessing the security of long-standing information infrastructure assets that may be outdated in the face of current threats. It is also extremely useful when a client or prospective user of a digital service wants to verify the security of the product presented by the developers.

The concept of a bug bounty is based on the idea that a skilled individual hacker could find unconventional ways to breach even the highest security levels. A company is capable to invest heavily in information security and employ highly skilled specialists, but it does not guarantee protection against penetration. Therefore, the right approach is to be proactive and identify issues before they arise. An open bug bounty programme with a pre-announced reward is specifically designed for this purpose [Laszka A., Zhao M., Malbari A., Grossklags J., 2018: 138–159].

The obvious advantage of a bug bounty over a penetration test is that it involves an unlimited number of information security specialists [Kuehn A., Mueller M., 2014]. Furthermore, payment is offered not for the test itself, but as a reward for identifying a vulnerability. Consequently, from a financial perspective, a bug bounty programme is a highly effective tool for testing a system's cyber resilience. While engaging hundreds or even thousands of specialists with various skill levels, the organiser only pays for results. It should also be noted that bug bounties help companies recruit talented information security professionals.

According to available analytical sources, the popularity of bug bounty is growing in Russia: "Over the course of 2024, the client base of bug bounty platforms has diversified, with organisations from sectors beyond

[2] Pentest Results 2023. Available at: URL: https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2023/#id1 (accessed: 02.09.2025)

technology, banking, retail and IT now joining their ranks. Bug bounty programmes are now being used by insurance companies, information security firms, software developers (including those creating domestic products as part of import substitution programmes), logistics companies, delivery services, bookmakers and regional government bodies in the Russian Federation. Furthermore, smaller companies, for whom information security is not a top priority, have shown an ever-growing interest in bug bounty programmes. These companies choose bug bounties as the most effective and convenient way to improve security."[3]

According to experts, the most significant barrier to the full development of the penetration testing industry is the risk of criminal prosecution for unauthorised access to protected computer data and systems [Fiorinelli G., Zucca V., 2024]. Research into the legal risks of this activity has already been published in in foreign literature [Park S., Albert K., 2020].

In Russian doctrine legal risks associated with organising and conducting penetration tests and bug bounty programmes have barely been explored. As has been rightly pointed out in a number of publications, the absence of clear legal frameworks and rules governing cyber testing poses significant risks for organisers and participants alike [Smorodina E.P., Burtsev R.D., Zinchenko D.R., Netrebin A.E., 2023: 116–122].

1. Criminal Law Risks Associated with Penetration Testing

In Russia some organisations are required by law to carry out regular penetration testing. For example, according to Bank of Russia Regulation No. 821-P of 17 August 2023, "On requirements for ensuring information security when carrying out money transfers, and on the procedure for the Bank of Russia to monitor compliance with these requirements", money transfer operators, bank payment agents, information exchange service operators, payment infrastructure service operators, and electronic platform operators must carry out annual testing. This is to identify potential points of penetration into their information infrastructure, and analyse its vulnerabilities.[4]

[3] The Russian IT market and its role in the global industry, 2024 results and forecasts for 2025. Available at: URL: https://www.ptsecurity.com/ru-ru/research/analytics/rossijskij-rynok-ib-i-ego-rol-v-mirovoj-industrii-itogi-2024-goda-i-prognozy-na-2025/#id22 (accessed: 03.09. 2025)

[4] See: Bulletin of the Bank of Russia, No. 76, 21 December 2023.

In accordance with Government Order No. 1911-r of 28 August 2019, "On the Approval of the Concept for the Creation of a Unified State Cloud Platform", the information security system of the state-run unified cloud platform must undergo an annual independent internal and external audit of the information security measures and state of protection in place, including vulnerability assessments and penetration testing. These audits must be carried out by organisations licensed by the Federal Service for Technical and Export Control.[5]

Information security standards emphasise that using a penetration tester (usually a contractor) to assess a system's security by attempting to breach it, with the knowledge and consent of the relevant official within the organisation, is one of the prerequisites for building trust in the security programme. As IT systems become more complex, maintaining security becomes increasingly difficult. Penetration testing groups can help to identify weaknesses.[6]

Although penetration testing has become fairly routine in cyber resilience monitoring, specific criminal law risks remain. These risks manifest as "the risk of being subjected to criminal prosecution without lawful substantive grounds for doing so, or to various restrictions arising from a preliminary or final assessment of an act as a criminal offence, whether overturned or not" [Zhalinsky A.E., 2009: 242].

Current issues relating to the regulatory framework and legal risks of penetration testing are frequently discussed in Russian literature on information security auditing. This approach could be reasonable if "audit" simply meant an independent review of a particular activity in the broadest sense of the word. Scholars point out in particular that "The current regulatory framework does not fully define aspects such as the objectives and audit methodologies, the rights and obligations of those subject to audit, and the procedures for recording and reporting the results of information system audits to management and owners. Amendments to the Federal Law "On Auditing" regarding the inclusion of information security audits of business entities among other services, as well as the development of state audit standards, will help to standardise this type of activity" [Safonova M.F., Krivoshey D.N., 2024: 644–664].

[5] See: Collection of Laws of the Russian Federation, 09 September 2019, No. 36, Page 5066.

[6] See: GOST R ISO/TO 13569-2007. National Standard of the Russian Federation. Financial Services. Guidelines on Information Security (approved by Order No. 514-st of Rostekhregulirovanie dated 27 December 2007).

In the context of penetration testing, the risks associated with criminal law stem from various factors, including the lack of a uniform interpretation of the elements constituting criminal offences in the field of computer information, in both theory and practice. More specifically, an unwarranted criminal prosecution in the context of a penetration test is likely due to the following:

— A penetration test involves bypassing the technical and software security measures of a digital resource. This corresponds to the criteria for unauthorised access to legally protected computer information (Article 272 of the Russian Criminal Code).

— The tools used by testers to carry out simulated cyber-attacks may exhibit characteristics of malicious software as defined in Article 273 of the Code;

— When carrying out testing, the tester may gain access to confidential information affecting the rights and freedoms of various individuals. This in itself may constitute grounds for criminal prosecution under Article 137 (invasion of privacy), Article 138 (breach of the confidentiality of correspondence or communications), and Article 272-1 (unlawful handling of computer data containing personal information) of the Russian Criminal Code.

— As with any other professional activity, penetration testing can have adverse consequences, such as workplace injuries, damage to expensive equipment, etc. These may be due to both low skill levels or outright negligence in performing one's duties;

— If an information security incident occurs, the question may arise as to whether the tester should be held criminally liable under Article 274 or Part 3 of Article 274-1 of the Russian Criminal Code for negligently performing duties relating to the security audit of an information and communications infrastructure facility.

The risk of criminal liability associated with unauthorised access to computer data is generally eliminated by the copyright holder's consent to perform penetration testing. As Article 272 of the Russian Criminal Code stipulates liability for unauthorised access to computer data protected by law, the existence of such consent indicates that the access was authorised and therefore lawful. However, it is important to note that this consent relates to a specific test concerning a strictly defined resource or resources, and for a limited period of time, in terms of its content and methodology. If the tester fails to comply with any of these

conditions, they will no longer be able to claim that their access to computer data was lawful.

It is also important to note that such consent must be given by an authorised party in the correct format. The issue here is not just that the absence of a formal written agreement would make it impossible for an information security professional to prove they were acting on behalf of the resource owner, but also that they were acting in their interests. Authorised access can only be granted by the owner of the information system, or by other individuals within the scope of their authorised powers. For instance, a branch manager cannot grant access to the company-wide information network [Pupillo A., Ferreira A., Varisco G., 2018].

In this regard, it is possible that a tester may have acted in good faith regarding the lawfulness of their actions where consent was given by an unauthorised party. As IT specialists generally lack a legal background, they are unable to consider all the nuances of corporate governance. Such a misunderstanding could therefore be grounds for classifying the act as causing harm through negligence (Article 28 of the Russian Criminal Code).

Any consent given for penetration testing must clearly define its scope. In the context of information security vulnerability testing and analysis of information infrastructure assets, the scope refers to the list of assets for which such testing and analysis must be carried out.[7] A cybersecurity specialist breaching the testing conditions in this regard also leads to the conclusion that their actions were generally unlawful, with the offence falling under either Article 272 or Article 274-1 of the Russian Criminal Code.

The criminal law risks associated with penetration testing are equally significant, in terms of potential criminal prosecution for actions involving malicious computer programs or data. When analysing the legality of software used to commit high-tech crimes, the doctrine notes one should also take into account the existence of legitimate software that can be used for criminal purposes. This category includes programmes such as those grouped under the heading "penetration testing". These programmes simulate unauthorised access to a computer system. Due to the lack of clear legal regulation regarding the status of such software, creating and using it may be deemed unlawful, despite it effectively serving the purpose of ensuring information security [Polyakov V.V., 2024: 435–453].

[7] See: Bank of Russia Guidelines on Penetration Testing and Information Security Vulnerability Analysis of Information Infrastructure Facilities of Financial Market Organisations (approved by the Bank of Russia on 22 January 2025 No. 2-MR) // Consultant Plus Legal Information System.

In Paragraph 2, Clause 8 of Resolution No. 37 of 15 December 2022, titled "On Issues of Judicial Practice in Criminal Cases Concerning Offences in the Field of Computer Information, as Well as Other Offences Committed Using Electronic and Telecommunication Networks, Including the Internet", the Plenum of the Supreme Court of the Russian Federation has formulated a definition of malicious programmes and other computer data. This definition is based on the criterion that such programmes and data are designed to exert unauthorised and concealed influence on data and to neutralise the means of protecting it.[8]

This approach defines a programme as malicious based on its functional purpose, namely, to exert unlawful influence over computer data and systems. It follows from a literal interpretation of Article 273 of the Russian Federation Criminal Code and is the most widely endorsed approach in legal science and the most commonly applied in legal practice.

It has a sense to emphasize that the malicious nature of a programme is a legal matter falling within the remit of judicial and investigative authorities. Computer-based technical analysis describes the programme's general operating algorithm. While an expert's conclusions are decisive, they are not conclusive when it comes to determining whether a programme is malicious.

Indicators of malicious software that may be identified during a forensic computer examination include:

— functionality designed to destroy, block, modify or copy user information, or to circumvent security measures;

— installation without the user's consent;

— operation in a mode hidden from the user;

— performing operations on computer data without the user's consent.

An analysis of judicial practice shows: the question of whether a computer programme is harmful is a matter of debate and is characterised by legal uncertainty. For example, in one case, the court notes: «The defence counsel's assertions that the programmes 'BeaconDNS', 'beacon_dns_admin', and 'dns-bot-js', created by Zh., are not malicious but are equivalent to legitimate penetration testing programmes, have been created on the instructions of an employer providing services in the field of information security software development, and therefore

[8] See: Bulletin of the RF Supreme Court. No. 3, March, 2023.

cannot bypass security measures, copy information from a remote computer without authorisation, or be installed on it without the owner's knowledge since this would have required the creation of an additional programme, which Zh. did not do, were investigated during the judicial inquiry and were not substantiated'

Also an analysis of practice shows the question of whether a computer programme is harmful is a matter of debate characterised by legal uncertainty. For example, in one case, the court has noted that: "The defence counsel's assertions that the programmes "BeaconDNS", "beacon_dns_admin", and "dns-bot-js", created by Zh., are not malicious, but are equivalent to legitimate penetration testing programmes; that they were created on the instructions of an employer providing services in the field of information security software development; and that they cannot bypass security measures, copy information from a remote computer without authorisation, or be installed on it without the owner's knowledge, since this would have required the creation of an additional programme, that Zh. did not do, were investigated during the judicial inquiry and were not substantiated."[9]

The manual for the information security course state: "Vulnerabilities can be identified manually using the information obtained and vulnerability databases." However, this is a very long and laborious process. An alternative is to use vulnerability scanners, which not only help to identify known vulnerabilities in installed software and operating systems, but also detect outdated encryption protocols" [Begaev A.N., Begaev S.N., Fedotov V.A., 2018].

At the same time, examination of practice shows using specialised software to scan information infrastructure assets for the purpose of identifying vulnerabilities may be classified under Article 273 of the RF Criminal Code: "...S., using the aforementioned laptop and an internet connection provided by an internet service provider... launched a programme... and accessed a remote government website... for the purpose of subsequently scanning it for vulnerabilities using the programme... S. did not have the copyright holder's consent to do so[10].

[9] Sentence of the Frunze district court of Vladimir of 29 October, 2021 in case No. 1-23/2021 // Consultant Plus Legal Information System. Cassation Order No. 77-4/2023 of 13 January 2023 issued by the Second Court of Cassation of General Jurisdiction upheld this judgment.

[10] Ruling of the Komintern District Court of Voronezh of 27 September 2022 in Case No. 1-751/2022.

In a similar case, the court has handed down a ruling that classified the programme as malicious, but this time under Part 1 of Article 274-1 of the Criminal Code: "It has been established that M., whilst at home..., acting intentionally and with the aim of testing his software skills, knowing full well that the resource <...>, which has the domain name <...>, forms part of the University's information and telecommunications network, that is to say, constitutes part of critical information infrastructure, on his mobile telephone of the brand <...> opened a digital window for the freely available software designed to conduct network security audits of information resources — including those on public telecommunications networks–that software had previously been installed on the specified mobile phone, and entered the University's email address into the software... M. then launched the specified software using additional scripts..., employing the software to check for vulnerabilities on the website...".[11]

Cases of criminal prosecution for the use of scanning software are not isolated incidents.[12] In all cases, the prosecution's key argument was that such actions — using a scanning programme to identify vulnerabilities in an information infrastructure asset—were carried out without the owner's (administrator's) consent, i.e. there was no contractual agreement in place for the testing.

Examining practice reveals that referencing the dual purpose of a computer programme does not exempt a person from liability under Article 273 of the Russian Criminal Code.[13]

Resolution No. 37 of the Plenum of the Supreme Court of Russia of 15 December 2022 sets out that using such a programme or information on one's own computer devices, or with the consent of the owner, does not constitute a criminal offence if it is not done with the intention of gaining unauthorised access to legally protected computer data, and if it does not result in the unauthorised destruction, blocking, modification or copying of such data, or the neutralisation of its security measures.

[11] Ruling to discontinue criminal proceedings following the imposition of a court fine by the Kuibyshevsky District Court of Omsk on 19 January 2024 in case No. 1-21/2024 (1-398/2023).

[12] See: Appeal ruling of the Omsk Regional Court dated 20 February 2023 in case No. 22-491/2023; Sentence of the Ryazhsky District Court of the Ryazan Region of 29 December 2020 in case No. 1-163/2020; Sentence of the Kargopol District Court of the Kurgan Region of 26 November 2020 in Case No. 1-91/2020.

[13] Sentence of the Magadan City Court of the Magadan Region of 6 July 2022 in Case No. 1-195/2022 // Consultant Plus Legal Information System.

This applies, for example, to educational purposes or testing computer systems to assess the vulnerability of computer information security measures to which the individual has lawful access, as well as to the creation of such programmes for these purposes.

The Supreme Court's legal position has clarified the classification of actions taken by IT specialists involving computer programmes capable of circumventing technical protection measures. It is important to note that the clarification in question makes no mention of distribution. Distribution involves deliberately granting access to such objects in any form to a specific person or an unlimited number of persons. Consenting to receive malicious software does not preclude criminal liability for distribution under Article 273 of the Criminal Code. Since, according to the Supreme Court's position, criminal liability is not only excluded for authorised use, but also for the creation of malicious software for the purpose of testing a system's security, it is reasonable to assume that this interpretation may also apply to distribution.

However, this issue has not yet been definitively resolved in theory or judicial practice. The following example from legal practice illustrates this: "During the court hearing, the defendant S. partially admitted to the charge of committing the specified offence, explaining that he had been running a computer programme... However, this programme is not malicious software, but rather a website testing programme that can be used to identify vulnerabilities in websites."

When reaching its decision on the case and assessing the evidence as a whole, the court made the following statement: "The court regards the defendant S.'s testimony denying guilt in relation to the alleged offence with scepticism. This is because it is contradicted by the evidence presented by the prosecution and the established facts. Therefore, the court deems it to be unreliable. It is regarded as a chosen line of defence aimed at avoiding criminal liability for the offence committed. As such, it cannot influence the court's conclusions regarding S.'s guilt in the act with which he is charged."[14]

It appears that a key factor in the court's decision was the fact that the defendant distributed a computer programme exhibiting malicious characteristics without carrying out any specific testing activities at the

[14] Sentence of the Akhtubinsky District Court of the Astrakhan Region of 19 September 2022, No. 1-207/2022; Ruling of the Fourth Court of Cassation of General Jurisdiction of 13 June 2023, No. 77-2043/2023 has upheld this judgment.

time of the offence. The programme was implemented via a specialised platform on the condition that it could be used for an information security audit.

Overall, it is considered that the risk of criminal liability arising from the use and distribution of such scanning programmes, carried out with the consent of the information system owner and for the purpose of testing the vulnerability of computer information security measures, should be assessed as low. Article 11 of the 2024 United Nations Convention against Cybercrime, "Misuse of Devices", explicitly states that it is not an offence to receive, produce, sell, acquire for use, import, distribute, or otherwise provide or possess computer programmes, information, or devices without the intention of committing any of the offences recognised under Articles 7–10 of the Convention (unauthorised access, interception, interference with electronic data, or interference with an information and communications system) within the framework of authorised testing or the protection of an information and communications system.[15]

According to the penetration testing methodology, after gaining access to vulnerable services and escalating privileges to the highest level, the tester must gather evidence of the intrusion for inclusion in the final report for the client company [Eryshov V.G., Larionets K.A., 2022: 209–210]. In this context, if an individual comes into contact with various kinds of sensitive information, they may be held liable under Russian criminal law for handling confidential information unlawfully.

It is important that it is not recommended to use real data obtained from actual business processes for certain documents in the test environment. Where testing requires data as close as possible to real-world data, it is recommended that test datasets be generated by irreversibly anonymising, masking and/or distorting information obtained from the implementation of banking business processes. Under the legislation of the Russian Federation, the organisation's internal documents and/or contracts with clients and counterparties, it is not recommended to use any data in testing which is subject to confidentiality requirements.[16]

---

[15] See: The Convention approved by UN General Assembly Resolution 79/243 of 24 December 2024 and opened for signature in October 2025. Available at: URL: https://docs.un.org/ru/A/RES/79/243 (accessed: 04.11. 2025)

[16] See: Bank of Russia Recommendations on Standardisation "Ensuring Information Security in Bodies within the Banking System of the Russian Federation. Ensuring Information Security at the Various Stages of the Life Cycle of Automated

From the perspective of mitigating the risk of criminal liability faced by a penetration tester when handling restricted-access information, this recommendation appears to be the most preferable. As an alternative, if access to actual data is anticipated, the specialist's rights and obligations must be set out in as much detail as possible in the contract for information security audit services.

When conducting penetration testing on an information infrastructure asset, the tester is liable for any adverse consequences causally linked to the impact on the computer system resulting from the work being carried out. Available research findings indicate that, after budget constraints, the next factor hindering regular penetration testing is the risk of disrupting business continuity. The primary task of an organisation's information security department is to ensure the smooth running of business operations. For this reason, information security managers are wary of penetration tests, as many have experienced operational downtime.[17]

It is important to note here that penetration testing inherently involves the possibility of adverse consequences for the information infrastructure being tested. For example, GOST R 58143-2018 stipulates: "Test scenarios based on the incorrect, intentional or unintentional use of external objects or components dependent on the object under assessment must simulate software failures in order to identify security errors and potential vulnerabilities." Testers must also simulate atypical actions designed to undermine the assumptions made during software development about the software's state and that of its operating environment. The effect of the error may not be immediately apparent, and the consequences of the error may be difficult to detect outside the scope of the assessment. The result may take the form of an error message or a complete failure of the system under test."[18]

The relevant national standard provisions explicitly acknowledge the possibility of unforeseen adverse consequences arising from penetration

---

Banking Systems" RS BR IBBs-2.6-2014 (brought into force by Order of the Bank of Russia No. R-556 of 10 July 2014) // Consultant Plus Legal Information System.

[17] Is there a need for automated penetration testing? / Available at: URL: https://www.ptsecurity.com/ru-ru/research/analytics/est-li-neobhodimost-v-avtomatizacii-testirovaniya-na-proniknovenie/#id19 (accessed: 03.09. 2025)

[18] See: GOST P 58143-2018. National Standard of the Russian Federation. Information Technology. Methods and Means of Ensuring Security. A detailed analysis of software vulnerabilities in accordance with GOST R ISO/IEC 15408 and GOST R ISO/IEC 18045. Part 2. Penetration testing (approved and brought into force by Order of Rosstandart No. set of 24 May 2018).

testing. This allows us to conclude that, provided a professional conducts the testing in accordance with the target system's known operating conditions and uses attack templates developed in accordance with generally accepted national and/or international sources, liability for such consequences must be excluded.

The relevant national standard provisions explicitly acknowledge the possibility of unforeseen adverse consequences arising from penetration testing. Therefore, provided a professional conducts the testing in accordance with the target system's known operating conditions and uses attack templates developed in accordance with generally accepted national and/or international sources, we can conclude that they cannot be held liable for such consequences.

However, if such testing was carried out in a manner that endangered the lives and health of many people or was in clear breach of the basic rules and procedures governing penetration testing, it would be a different matter. In this context, the tester may be liable for criminal negligence under Section 274 or Section 274-1 of the Criminal Code.

In certain cases, the person responsible for conducting information security audits within an organisation may also be held liable for criminal negligence. This usually applies to situations involving the assessment of staff members responsible for conducting internal information security audits. This approach has already been confirmed in contemporary judicial practice. For instance, in a case involving an offence under Part 3 of Article 274-1 of the Criminal Code, the court stated: "...being fully aware that he was responsible for identifying, analysing and monitoring vulnerabilities in the security systems of the information system ..., as well as for responding to computer incidents, failed to fulfil his duties to monitor audit logs in the event log of the information panel...".[19]

Let author believe a company's information security specialist should only be held liable for criminal negligence in the event of a cyber incident involving a clear breach of professional duty, as described above. In each such case, it must be conclusively established that the IT specialist had a genuine, not just hypothetical, opportunity to prevent adverse consequences for the organisation's information infrastructure.

The court may take into account the voluntary disclosure of the results of unauthorised penetration testing when considering redress for

[19] Sentence of the Kyzyl City Court of the Republic of Tuva of 23 August 2024 in Case No. 1-1309/2024.

the harm caused by the offence and deciding on exemption from criminal liability. The following decision serves as an example: "The court has established that S. has been charged with a moderately severe crime, has no previous convictions, has fully admitted his guilt in relation to the offence with which he has been charged, is relatively young, has actively assisted in the detection and investigation of the crime and that there have been no adverse consequences, including any actual damage to the victim's business or reputation, as a result of S.'s unlawful activities. An apology has been offered to the victim in the form of a letter and a scanned copy of a report detailing the risks and vulnerabilities identified in the system with a view to strengthening its information security. The department has accepted the apology offered by S. and has no further claims against the defendant."[20]

This court ruling should be upheld. By disclosing all information obtained as a result of a cyberattack, the owner of the information resource can significantly improve information security levels. In this respect, behaviour that is originally unlawful can have a positive outcome, eliminating the system's vulnerabilities to current cyber threats.

2. Criminal Law Risks Associated with Running open Competitions to Identify Vulnerabilities in Software, web Applications and Computer Systems (Bug Bounty)

The criminal law risks associated with the crowdsourced method of assessing the cyber resilience of information infrastructure assets (bug bounty) are largely the same as those analysed in relation to penetration testing. This enables us to concentrate on the particular issues that characterise this method of identifying vulnerabilities in computer systems, which is becoming increasingly popular in Russia year on year.

In Russia there are no specific regulations governing the organisation and conduct of programmes (competitions) open to an unlimited number of participants (researchers) for testing the security of information products and/or systems against unauthorised access. A legislative initiative put forward by the Russian Ministry of Digital Development, Communications and Mass Media in 2023 came to nothing.

[20] Ruling of the Komintern District Court of Voronezh of 27 September 2022 to discontinue criminal proceedings on the grounds of active repentance in case No. 1-751/2022.

Examining legislation in other countries reveals examples of how the process of obtaining information about vulnerabilities in computer systems is regulated through bug bounty programmes. The European Union's Cyber Resilience Act, for example, stipulates: "Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Part II, point (5), of Annex I to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources."[21] The relevant annex stipulates: in addition to carrying out effective and regular security testing of products containing digital components, manufacturers are required to implement and ensure compliance with a coordinated vulnerability disclosure policy.

On 15 February 2023 specific regulations concerning participants in bug bounty programmes came into force in Belgium under the Belgian Act on the Protection of Whistle-blowers of 28 November 2022. Under the Act individuals disclosing information about vulnerabilities to the Belgian Cyber Security Centre will not be considered to have committed an offence in connection with the actions necessary to report the vulnerability, provided the following conditions are met:

The individual/legal entity must demonstrate that they have submitted a written vulnerability report to the Belgian Cyber Security Centre and the relevant organisation (the system owner) immediately, in accordance with the procedure set out in detail on the Belgian Cyber Security Centre's website. Such reports cannot be submitted once criminal proceedings have commenced.

— the researcher must act without criminal intent.

— the person making the report must not go beyond what is necessary and proportionate to confirm the existence of a potential vulnerability. These guidelines are available on the Belgian Cyber Security Centre's website.

— the researcher must not publicly disclose information about the vulnerability without the consent of the Belgian Cyber Security Centre.

These provisions apply to all organizations in Belgium, including those without their own bug bounty programme. Commenting on the significance of the new law, experts noted: "Until now, ethical hacking,

[21] Cyber Resilience Act / Available at: URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847 (accessed: 09.06. 2025)

even when carried out with the best of intentions, was punishable under Belgian criminal law. As a result, an ethical hacker who reported a security vulnerability in an organisation's systems risked facing criminal charges. The new legislation eliminates this risk, and we hope it will lead to more vulnerabilities being detected and reported to organisations, enabling them to improve the security of their systems."[22]

On a positive note, it is worth mentioning that there have been no convictions of participants (testers) or organisers of bug bounty programmes in Russian judicial practice. However, this does not mean that there are no risks of criminal prosecution in this area whatsoever. According to research, criminal law risks are the main factor hindering the development of this information security practice, accounting for 35% of all responses [Kadam R., Roy B., Deepak S. T., Singh R., 2025: 3219–3229].

A typical bug bounty programme is characterised by legal uncertainty surrounding the lawfulness of a tester's actions when they circumvent the technical and software security measures of an information product and/or system. Unlike a penetration test, no agreement is entered into with the programme participant (the tester). Accepting the programme's terms and conditions cannot perhaps be regarded as an agreement on the part of the researcher participating in the programme. In any case, this is a matter of debate.

Foreign publications also note that participants in bug bounty programmes are at the highest risk of facing criminal prosecution for unauthorised access to computer data. However, if such access is granted in strict accordance with the established rules for cyber testing, it should be regarded as lawful [Vostoupal J., Stupka V., Harasta J., Kasl F., Loutocky P., Malinka K., 2024]. Where a participant has unlawfully circumvented technical and software security measures due to a misinterpretation of the bug bounty rules, such an act is regarded as negligent data or system interference.[23]

[22] New Belgian legal framework gives safe harbour to ethical hackers and bug bounty hunters. Available at: URL: https://www.intigriti.com/blog/news/new-belgian-legal-framework-gives-safe-harbor-to-ethical-hackers-and-bug-bounty-hunters (accessed: 15.08.2025)

[23] For example, Article 232 of the Czech Criminal Code provides for liability for negligently interfering with the operation of computer equipment. It is important to note that liability only arises where substantial damage is caused to another person's property. The destructive impact on data, hardware or software alone does not constitute evidence of a criminal offence. Available at: URL: https://rm.coe.int/czech-criminal-code-in-english-as-amended-in-2023/1680b5e324 (accessed: 12.09. 2025)

Under Russian criminal law, such actions by a participant in cyber testing constitute a breach of access rules within the meaning of Article 274 of the RF Criminal Code. However, liability only arises if the act results in the destruction, blocking, modification or copying of computer data, causing substantial damage (in excess of 1 million Rubles).

In the absence of clear legal regulation it is unacceptable to present a bug bounty programme as an invitation to carry out cyber-attacks on a particular information system with the owner's consent while disregarding the interests of users. It is necessary to bear in mind such systems may contain sensitive information belonging to third parties. Allowing this poses a risk of significant harm to the rights and legitimate interests of others, including with regard to privacy, confidentiality of correspondence and trade secrets. Furthermore, the bug bounty scheme itself does not enable the organiser to monitor the behaviour of all testers. Having gained access under the programme, the latter may engage in unlawful activities, such as passing on sensitive information to third parties or using it for personal gain [Kinis U., 2018: 508–522].

This is precisely why organisers of current bug bounty programmes quite rightly stipulate researchers are prohibited from:

— accessing, altering or deleting other users' data;

— disclosing any confidential information inadvertently obtained during the vulnerability search;

— interfering with other users' accounts;

— exploiting the identified vulnerability for personal gain;

— attempting to gain access to accounts, user data within information systems or any other confidential data beyond what is strictly necessary to demonstrate the identified vulnerability;

— carrying out the targeted extraction of users' personal data from the internal systems of web services and applications, as well as from other information resources not specified in the technical specifications. Bug bounty organisers rightly assume that any actions involving information within the system under test, such as alteration, modification, deletion or replacement, are only permitted in relation to data associated with the participant's own account (a specially created test account) or another user's account with their consent. [24]

[24] See, for example: the 'Information Resources of the Nizhny Novgorod Region' bug bounty programme. Available at: URL: https://bugbounty.standoff365.

Therefore, it is unacceptable to make confirmation of the identified vulnerability dependent on whether the tester has copied confidential information (e.g. users' personal data). This poses a direct risk of criminal prosecution under Article 272-1 of the Russian Federation Criminal Code for unlawful acts involving computer data containing personal data, such as use, transfer, collection and storage. In this context the organisers' actions may themselves be classified under Part 6 of Article 272-1 as knowingly creating and maintaining an online resource intended for unlawful acts relating to computer data containing personal data. Therefore, a bug bounty programme may only be organised using client accounts that have been specifically created for this purpose (consent for the processing of personal data must include the possibility of granting access to such data during penetration testing).

The provision allowing funds to be transferred without the customer's consent is also unacceptable, as it poses a risk of criminal prosecution under Para. D, Part 3 of Article 158 of the Russian Criminal Code. While the value of the property taken may be insignificant (up to 2,500 Rubles), the offence meets the criteria for aggravated theft: from the victim's bank account. In this case, it would be advisable to adopt a different approach that explicitly indicates either that the withdrawal was made with consideration (for example, the tester tops up the participant's account and only then transfers funds from it), or that the loss was negligible, and no financial gain was involved (for example, the tester carries out a symbolic transaction for one Ruble).

When considering the criminal law risks associated with bug bounties, the Joe Sullivan case is an obvious point of reference. Sullivan, Uber's former head of security, has paid the two hackers who breached the company's infrastructure in 2016 the reward they had demanded. He concealed the incident affected more than 50 million passengers and 600,000 Uber drivers, from the regulatory authorities. At the same time, he authorised a pay-out of USD 100,000 under the company's bug bounty programme, despite the fact that the maximum pay-out under that programme was only USD 10,000. The hackers had threatened to release stolen confidential user data if the sum was not paid. Sullivan was found guilty of obstructing justice and concealing a serious crime.[25]

---

com/programs/nnov (accessed: 09.09. 2025)

[25] Former Uber Security Chief Found Guilty of Hiding Hack From Authorities. Available at: URL: https://www.nytimes.com/2022/10/05/technology/uber-security-chief-joe-sullivan-verdict.html (accessed: 09.08. 2025)

The ruling in the Sullivan case was met with considerable criticism from information security experts: "This ruling deprives private organisations of the ability to manage their own computer systems, as it interprets the Computer Fraud and Abuse Act (CFAA) in such a way that it prohibits them from retrospectively granting access to their systems. Under this interpretation, security researchers acting in good faith who identify and report vulnerabilities responsibly to companies may still face criminal prosecution if they gained access to the system before obtaining official authorisation. This decision is completely at odds with modern cybersecurity practices and increased the risk to organisations, information security managers and national security."[26]

Under Russian criminal law, such actions by an individual with managerial authority in a commercial organisation constitute an abuse of authority (Article 201 of the Russian Criminal Code). The individual may also face criminal charges for embezzling the organisation's property (Article 160 of it).

However, it is important to note the following caveat. The obligation to report information security incidents only applies to operators of critical information infrastructure in the Russian Federation. The relevant law requires such operators to:

Immediately notify the federal executive authority responsible for ensuring the functioning of the state system for the detection, prevention, and mitigation of the consequences of cyber-attacks on the information resources of the Russian Federation of any cyber-attacks or cyber incidents.

Assist officials of the aforementioned authority in detecting, preventing, and mitigating the consequences of cyber-attacks, and in establishing the causes and circumstances of cyber incidents.

Respond to cyber incidents in accordance with the procedure approved by the aforementioned authority.[27]

The provisions of the law in question are generally intended to promote transparency and cooperation. Hiding cyber incidents gives crimi-

[26] See: A Court Ruling on Bug Bounties Just Made the Internet Less Safe. Available at: URL: https://www.infosecurity-magazine.com/opinions/court-ruling-bug-bounties-internet/ (accessed: 25.08. 2025)

[27] Article 9 of Federal Law No. 187-FZ of 26 July 2017 (as amended on 7 April 2025) On the Security of Critical Information Infrastructure of the Russian Federation // Consultant Plus Legal Information System.

nals an advantage by enabling them to carry out new cyber-attacks. The practice of concealing information security issues is well-known. Companies are reluctant to report incidents involving the leakage of user data. This results in reputational damage and inevitable financial losses. In our opinion, the failure of the relevant entities to fulfil the aforementioned obligations poses an objective threat to the security of the Russian Federation's critical information infrastructure and to the rights and freedoms of individuals and organisations.

The above implies that concealing information about information security incidents involving facilities not part of Russia's critical information infrastructure cannot lead to criminal prosecution for abuse of authority (Article 201 of the Russian Criminal Code).

Finally, it is worth noting the obvious risk of criminal prosecution in cases where a participant in a cyber testing programme misleads the organiser. Traditionally, the rules governing bug bounty programmes stipulate information regarding vulnerabilities in a computer system must be obtained without the use of insider information or assistance from the organising company's employees. If information is obtained in a way that enables a participant to falsify a report and receive undue remuneration, this may be classified as fraud under Article 159 of the Russian Criminal Code.

Conclusion

Modern cybersecurity practices make extensive use of penetration testing and bug bounty programmes. These approaches enable organisations to identify vulnerabilities in advance while also allowing security researchers develop their professional skills.

In the absence of specific legislation, an "ethical hacker" searching for vulnerabilities in information systems is undoubtedly exposing themselves to the risk of criminal prosecution. This article analysis suggests a clear definition of the legal framework governing the testing of information systems for cyber resilience is required to fully address the associated risks. It should encompass targeted penetration testing conducted within the scope of individual contractual agreements and public tenders, as well as procedures for reporting vulnerabilities discovered by individuals acting independently.

Currently, the mitigation of criminal law risks faced by information security specialists is governed by the Supreme Court of the Russian Federation's specific rulings and doctrinal interpretations.

Overally speaking, government policy in this area should ultimately be directed towards a single overarching objective — to promote the identification and appropriate disclosure of information about vulnerabilities as widely as possible, in order to ensure the security of information infrastructure assets[28]. This can be achieved through educational and awareness-raising campaigns, reward schemes and public recognition of socially beneficial hacking, for example. Not only is it necessary to establish a legal framework for the activities of "ethical hackers", but it is also necessary to engage with them on an ideological level.

References

1. Begaev A.N., Begaev S.N., Fedotov V.A. (2018) Penetration Testing. Saint Petersburg: ITMO University, 45 p. (in Russ.)

2. Eryshov V.G., Larionets K.A. (2022) Main Stages, Methodologies, and Tools for Conducting Penetration Testing. In: Collection of Papers of the 2nd International Scholar Conference on Processing, Transmission, and Protection of Information in Computer Systems. S. l., no Publ., pp. 209–210 (in Russ.)

3. Fiorinelli G., Zucca V. (2024) Is the Road to Hell Paved with Good Intentions? A Criminological and Criminal Law Analysis of Prospective Regulation for Ethical Hacking in Italy and the EU. In: Proceedings of the 8th Italian Conference on Cyber Security. Available at: https://ceur-ws.org/Vol-3731/paper45.pdf

4. Kadam R., Roy B., Deepak S. T., Singh R. (2025) Bug Bounty Programs: A Comprehensive Meta-Analytical Review of Strategies, Challenges, and Future Directions. *International Research Journal on Advanced Engineering Hub,* vol. 3, pp. 3219–3229. https://doi.org/10.47392/IRJAEH.2025.0473

5. Kinis U. (2018) From Responsible Disclosure Policy towards State Regulated Responsible Vulnerability Disclosure Procedure: the Latvian approach. *Computer Law & Security Review,* vol. 34, no. 3, pp. 508–522. https://doi.org/10.1016/j.clsr.2017.11.003

6. Kuehn A., Mueller M. (2014) Analyzing Bug Bounty Programs: an Institutional Perspective on the Economics of Software Vulnerabilities. 2014 TPRC Conference Paper. Available at: http://dx.doi.org/10.2139/ssrn.2418812

[28] The rules of one of the programs contain prohibitions on: 1) working in the company for the sake of legitimate access to the company's systems and the implementation of unacceptable events; 2) bribery of employees of the company or collusion with them; the use of other voluntary assistance of the company's current employees (covering up the actions of the researcher, facilitating access or the occurrence of an unacceptable event, voluntary provision of equipment); 3) the use of any means of influencing the company's employees; 4) bribery, other influence on service providers or counterparties of the company, collusion with them. See: Tom Tailor Bug Bounty Program. Available at: URL: https://bugbounty. standoff365.com/programs/tom-tailor (accessed: 12.09.2025)

7. Laszka A., Zhao M., Malbari A., Grossklags J. (2018) The Rules of Engagement for Bug Bounty Programs. In: Financial Cryptography and Data Security International Conference Papers. Berlin: Springer, pp. 138–159. https://doi.org/10.1007/978-3-662-58387-6_8

8. Park S., Albert K. (2020) A Researcher's Guide to Some Legal Risks of Security Research. *The Cyberlaw Clinic at Harvard Law School*, 31 p. Available at: https://clinic.cyber.harvard.edu/wp-content/uploads/2024/08/Security-Researchers-Guide-8-2-24.pdf

9. Polyakov V.V. (2024) Forensic Classification of Means of High-Tech Crimes. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta. Pravo*=Bulletin of the Saint Petersburg State University. Law, no. 2, pp. 435–453 (in Russ.)

10. Pupillo A., Ferreira A., Varisco G. (2018) Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges. In: CEPS Task Force Reports. Brussels: Centre for European Policy Studies. Available at: https://www.researchgate.net/publication/337195978_Software_Vulnerability_Disclosure_in_Europe_Technologies_Policies_and_Legal_Challenges_Recommendations_from_a_Report_of_a_CEPS_Task_Force/citations

11. Reddy P., Pelletier J. (2022) The Pentest Method for Business Intelligence. In: Papers of the Jubilee International Convention on Information, Communication and Electronic Technology, pp. 1117–1125. https://doi.org/10.23919/MIPRO55190.2022.9803788

12. Safonova M.F., Krivoshey D.N. (2024) Audit of Information and Cybersecurity: Regulatory Framework and Operational Problems. *Mezhdunarodnyj bukhgalterskij uchet*=International Accounting, no. 6, pp. 644–664 (in Russ.)

13. Smorodina E.P., Burtsev R.D., Zinchenko D.R., Netrebin A.E. (2023) Economic and Legal Basics of Ethical Hacking in the Russian Federation. *Cifrovaya i otraslevaya ehkonomika*=Digital and Industrial Economics, no. 2, pp. 116–122 (in Russ.)

14. Tudosi A.-D., Graur A., Balan D., Potorac A.D. (2023) Research on Security Weakness Using Penetration Testing in a Distributed Firewall. *Sensors,* vol. 23, no. 5, p. 2683. https://doi.org/10.3390/s23052683

15. Vostoupal J., Stupka V., Harasta J., Kasl F., Loutocky P., Malinka K. (2024) The Legal Aspects of Cybersecurity Vulnerability Disclosure: to the NIS 2 and beyond. *Computer Law & Security Review.* vol. 53, https://doi.org/10.1016/j.clsr.2024.105988

16. Zhalinsky A.E. (2009) *Criminal Law in Anticipation of Change: Theoretical and Instrumental Analysis.* 2 nd ed. Moscow: Prospekt, 400 p. (in Russ.)

Information about the author:

E.A. Russkevich — Doctor of Sciences (Law).

The article was submitted to editorial office 31.10.2025; approved after reviewing 24.12.2025; accepted for publication 15.01.2026.

Legal Issues in the **DIGITAL AGE**

AUTHORS GUIDELINES

The submitted articles should be original, not published before in other printed editions. The articles should be topical, contain novelty, have conclusions on research and follow the guidelines given below. If an article has an inappropriate layout, it is returned to the article for fine-tuning. Articles are submitted Word-processed to the address: lawjournal@hse.ru

Article Length

Articles should be between 60,000 and 80,000 characters. The size of reviews and the reviews of foreign legislation should not exceed 20,000 characters.

The text should be in Times New Roman 14 pt, 11 pt for footnotes, 1.5 spaced; numbering of footnotes is consecutive.

Article Title

The title should be concise and informative.

Author Details

The details about the authors include:

- Full name of each author
- Complete name of the organization — affiliation of each author and the complete postal address
- Position, rank, academic degree of each author
- E-mail address of each author

Abstract

The abstract of the size from 150 to 200 words is to be consistent (follow the logic to describe the results of the research), reflect the key features of the article (subject matter, aim, methods and conclusions).

The information contained in the title should not be duplicated in the abstract. Historical references unless they represent the body of the paper as well as the description of the works published before and the facts of common knowledge are not included into the abstract.

Keywords

Please provide keywords from 6 to 10 units. The keywords or phrases are separated with semicolons.

References

The references are arranged as follows: [Smith J., 2015: 65]. See for details http://law-journal.hse.ru.

A reference list should be attached to the article.

Footnotes

The footnotes include legal acts and cases are to be given paginaly.

The articles are peer-reviewed. The authors may study the content of the reviews. If the review is negative, the author is provided with a motivated rejection.