Research article
DOI: https://doi.org/10.21202/jdtl.2023.17

Approaches to Regulating Relations in the Sphere of Developing and Using the Artificial Intelligence Technologies: Features and Practical Applicability

Olga S. Erahtina

Perm branch of National Research University "Higher School of Economics"
Perm, Russian Federation

Keywords

Artificial intelligence,
danger,
digital economy,
digital technologies,
law,
regulation,
risk management,
risk-oriented approach,
software,
technological approach

Abstract

Objective: to review the modern scientific approaches to regulating relations in the sphere of using the artificial intelligence technologies; to reveal the main features and limitations of using the risk-oriented and technological approaches in order to determine the directions of their further development.

Methods: the methodological basis of the research is a set of scientific cognition methods, including the general scientific dialectic method and the universal scientific methods (analysis and synthesis, comparison, summarization, structural-functional, and formal-logical methods).

Results: it was determined that the use of the risk-oriented approach implies building constructive models of risk management. A significant issue in using this approach is the bases of referring the artificial intelligence technologies to high-risk ones. When determining the risk level of using the artificial intelligence technologies, the following criteria should be applied: the type of artificial intelligence technology, its sphere of use, and the level of potential harm for the environment, health and other fundamental human rights.

In turn, the central issue of using the technological approach is the necessity and limits of regulation in the sphere of developing and using the artificial intelligence technologies. First, interference into this sphere must not create obstacles for developing technologies and innovations. Second, a natural reaction of a regulator towards newly emerging objects and subjects of turnover is the "imperfect law syndrome". At the same time, a false idea

about a lack of legal regulation may produce an opposite effect – duplication of legal norms. To solve the problem of duplicating legal requirements, it is necessary, first of all, to solve the issue of the need to regulate the artificial intelligence technologies or certain types of software applications.

Scientific novelty: a review was carried out of the main approaches to regulating relations in the sphere of developing and using the artificial intelligence technologies; the opportunities and limitations of their use are revealed; further directions of their development are proposed.

Practical significance: the main provisions and conclusions of the research can be used for determining the optimal approaches to regulating the sphere of digital technologies and for improving the legal regulation of the studied sphere of social relations.

For citation

Erahtina, O. S. (2023). Approaches to Regulating Relations in the Sphere of Developing and Using the Artificial Intelligence Technologies: Features and Practical Applicability. *Journal of Digital Technologies and Law, 1*(2), 421–437. https://doi.org/10.21202/jdtl.2023.17

Contents

Introduction
1. Risk-oriented approach
2. Technological approach
Conclusions
References

Introduction

Active development of technologies and systems of artificial intelligence generates scientific discussions about the necessity, limits and tasks of legal regulation in the sphere of information technologies. Scientists declare opposing views: from opinions about the need to establish a large number of obligatory requirements, mainly imposed on a developer (Smuha, 2021), to proposals to eliminate legal interference into the sphere of high technologies[1], so as not to impede innovations. The range of positions of scientists includes also more moderate voews: application of international and national standards (Zielke, 2020); implementation of voluntary certification (Ellul et al., 2021); soft regulation and self-regulation (Erdélyi & Goldsmith, 2018); establishing of explainable (Hamon et al., 2022) and ethical frameworks (Wagner, 2018).

[1] O'Sullivan, Andrea. (2017, October 24). *Don't Let Regulators Ruin AI*. https://www.technologyreview.com/2017/10/24/3937/dont-let-regulators-ruin-ai/

A Belgian researcher Nicolas Petit proposes the so called "regulatory trade-offs" achieved by balancing threats and opportunities created by the introduction of legal regulation[2]. He gives a number of examples of regulation impeding technological progress[3]. At the same time, he emphasizes that the lack of regulation may also hinder technological evolution. In particular, legal uncertainty negatively influences investments. According to Ryan Calo, undefined liability rules may bar investments into the open robotics markets and direct the caital flow towards narrow functionality of robots, where manufacturers may better manage risks, leaving open robotics underdeveloped (Calo, 2011).

Among the many approaches to legal regulation of relations in the sphere of using the artificial intelligence technologies one may specify the approach determining the general legal regime which is to stipulate the basic requirements to providing safety of the artificial intelligence systems. This regime should be applied to all such systems. Alongside with that, detailed requirements should be elaborated to development and use of the artificial intelligence in specific spheres (Ponkin & Redkina, 2018).

The high dynamics of the artificial intelligence technologies development and the multiple regulatory initiatives actualize the importance of interdisciplinary research aimed at revealing the optimal approaches to regulating the said sphere of public relations.

The article presents a complex analysis of two interdisciplinary approaches to regulating relations in the sphere of developing and using the artificial intelligence technologies, namely, the risk-oriented and the technological approaches; the features and limitations of their use are revealed; the directions of their further development are specified.

1. Risk-oriented approach

One of the approaches to regulating the artificial intelligence technologies actively discussed in science is a risk-oriented approach (Mikhaleva & Shubina, 2019; Gellert, 2021; Gonçalves, 2020). The idea of applying this approach was announced in the European Parliament Resolution on Civil Law Rules on Robotics of 2017[4]. Four years later, a draft Report of European Union stipulating the main rules on the artificial intelligence[5] proposed classification of the artificial intelligence systems based on the estimation of risk of their application. According to the said classification, all artificial intelligence systems were divided into four groups:

---

2 Petit, N. (2017, March 9). *Law and Regulation of Artificial Intelligence and Robots – Conceptual Framework and Normative Implications* (Working paper, pp. 6–7). http://dx.doi.org/10.2139/ssrn.2931339

3 *Ibid*. P. 12.

4 European Parliament. (2017, February 15). *Draft Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL))*. https://www.europarl.europa.eu/portal/en

5 European Parliament. (2021, April 21). *Regulation of the European Parliament and of the Council. Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*. https://www.europarl.europa.eu/portal/en

1) artificial intelligence systems with inadmissibly high risk level (first of all, the artificial intelligence systems used in military and defense sector, systems for manipulating human behavior and systems for forming social ratings);

2) artificial intelligence systems with high risk level[6];

3) artificial intelligence systems with limited risk level[7];

4) artificial intelligence systems with minimal risk level[8].

To estimate the risk level of artificial intelligence systems application, two main criteria are proposed: the degree of users' dependence on the decisions made by the system and the degree of its danger for life and health of citizens and violation of their fundamental rights.

The UE draft Regulation highlights the need to prohibit production and civil circulation of artificial intelligence systems, the use of which creates inadmissibly high risk of incurring harm. In turn, the developers, owners, and users of high-risk artificial intelligence systems, according to the draft regulation, must meet higher requirements to providing safety, keeping technical documentation and disclosing information[9]. To comply with the stipulated standards, quality management systems can be applied. The systems with limited or minimal risk level must, as a minimum, provide the opportunity to inform users about their interaction with artificial intelligence.

In general, the EU approach deserves support. At the same time, it requires further development.

First, it should be taken into account that the risk-oriented approach is the risk management system consisting of three main stages. At the first stage, one must identify, analyze and differentiate between the forecasted risks. At the second stage, one should estimate the risk level. At the third stage, one should determine the means of managing risks.

Given the variety of approaches to classification of risks (ideally, all these approaches must be taken into account), for the purposes of this article we may highlight:

– internal and external risks;

– systemic and non-systemic risks.

---

6 For example, robot assistants in surgery, management and exploitation of critical infrastructure.

7 For example, chat bots, virtual assistants, smart homes.

8 For example, videogames, spam filters.

9 When developing and using such systems, "principal requirements" should be met, such as requirements to the quality of data, documenting and traceability, human control, etc. In particular, prior to market placement or putting into operation, technical documentation must be compiled, which should reflect the system compliance to the set requirements and all the necessary information for estimating the system compliance (Article 11). The draft also requires elaborating systems so as to provide accounting during the system functioning (Article 12), as well as transparency of the AI system and information submission (Article 13), for the users of high-risk systems to be able to use them properly and to interpret the output data correctly. Human control must be provided during the entire lifecycle of the system, with the opportunity to interfere into the system functioning at any time and stop or fix it if needed.

Internal risks occur in an individual company; they can be forecasted, estimated and prevented in house. External risks (changes in the economic and political situation, natural disasters, environmental accidents, etc.) cannot be prevented in house.

Systemic risks threaten the market in general or certain spheres of business. Only experts may forecast their occurrence and estimate their consequences. They also cannot be prevented in house. As for non-systemic (commercial) risks, these are the risks of an individual company which it can and must minimize by its own efforts.

The concept of risk-oriented approach as interpreted in the European Parliament Resolution on Civil Law Rules on Robotics is aimed at managing internal and non-systemic risks while unattended external and systemic risks, which cannot be imputed to individual subjects of civil turnover. Identification of such risks is one of the main tasks to be solved at the first stage.

At the second stage, the risk level is determined (the probability of risk materialization and the volume of adverse consequences which may occur). At the first sight, the draft solves this task. However, the grounds for referring the artificial intelligence system to one of the four groups require further research. As was mentioned above, the draft Resolution proposes using the degree of users' dependence on the decisions made by the artificial intelligence as the criterion of the risk level, as well as the degree of danger the technology poses for the life and health of humans and the violation of their fundamental rights. In our opinion, the assessment of the valuation of the probability of risk materialization depends also on a number of other factors. First of all, these are characteristics of the technology. The main characteristics of the artificial intelligence are its autonomy (ability to make decisions independently, without human interference) and learnability (ability to master new skills and competencies). Depending on the sphere of application, one may distinguish several levels of the technology autonomy. For example, Appendix 10 to the Transport Strategy of the Russian Federation up to 2030 with the forecast up to 2035[10] defines five levels of autonomy of automobile transport, four levels of autonomy of railway transport and six levels of autonomy of water and marine transport.

By the criterion of learnability, the artificial intelligence may be unlearning, learning and self-learning. Apparently, highly autonomous and self-learning technologies must be referred to high-risk artificial intelligence systems, while unlearning technologies with the first or second levels of autonomy should be referred to the systems with minimal risk. However, the task of determining the risk level of an artificial intelligence technology based on its characteristic is not as simple as it may seem at the first glance. This is first, of all, due to the fact that, while estimating the risk level, one must take into account other characteristics of artificial intelligence besides autonomy and learnability. In particular, these are functionality (ability to perform one or more functions) and equipment with control means (Alekseev et al., 2020). Also, apparently, various combinations of these characteristics

[10] Adopted by the Order of the Government of the Russian Federation of 27.11.2021 No. 3363-r. https://base.garant.ru/403156321/

are possible. For example, the artificial intelligence technology may be highly autonomous, learning, perform two functions, and having no objective control means.

Scientific works also propose to use the sphere of application as the criterion for estimating the risk level of using artificial intelligence technologies. According to a group of researchers from University of Malta, legal regulation must be obligatory only for critical spheres of activity. At the same time, alongside with the sphere of using the artificial intelligence systems, one must assess the risk level of the activities it is used in (Ellul et al., 2021). One should agree with this conclusion. For example, in healthcare artificial intelligence technologies may be used to assist doctors in making diagnosis, prescribing medications, or performing operations. These types of activity may be referred to a high-risk category. At the same time, the artificial intelligence technologies are used for patient registering, processing and analyzing medical records, automated notifying of medical staff. These types of activity may be referred to a limited risk category.

Most authors refer the sphere of transport to the high-risk category. However, it should be taken account which types of activity are accompanied by the artificial intelligence. The artificial intelligence systems can be used to improve safety and efficiency of transportation, to manage passenger and cargo flows. At the same time, the artificial intelligence technologies are also used for rendering services of transporting cargo and passengers. While managing transport infrastructure refers to the high-risk category, servicing may be referred to the limited risk category.

Second, the question of risk management means requires further research, too. The draft pays the most attention to high-risk systems, actually, leaving unattended the artificial intelligence systems with limited risk. At the same time, special regulation (based on risk-oriented approach) must be implemented also to the artificial intelligence systems referring to this group.

We believe that risk management means will be different depending on the type of risk (internal or external, systemic or non-systemic risk) and the degree of risk of the artificial intelligence technology (high or intermediate).

Deserving attention is the “Basic model for determining criteria and categories of risk” adopted in 2017 by a project committee of the priority program “Reform of control and supervisory activity”[11]. The document defines such notions as “risk sources”, “risk factors”, “risk profile”, determines their types, offers the means of ranking the manageable risk factors of profiles (to determine the most significant of them) and the methodology

[11] “Basic model for determining criteria and categories of risk” (adopted by a protocol of the meeting of the project committee of 31.03.2017 No. 19(3)) (alongside with the “Requirements to justification of the proposed by federal executive bodies – participants of the priority program “Reform of control and supervisory activity” – risk categories (classes of danger) and risk criteria in relation to the types of state control (supervision) executed by them”).

of determining the volume of harm incurred and the probable frequency of potential negative consequences.

Although the above model was adopted in order to implement "smart checks" by supervisory bodies, to focus the checks on potentially most dangerous objects, the proposed methods for determining risk categories and criteria can be also used for assessing the risk level of using artificial intelligence technologies.

2. Technological approach

Recently scientific literature has been paying more and more attention to technological approach which focuses on the technology per se, its essential and specific characteristics. Viewing the development of technologies and innovations as the basic task of legal regulation, representatives of this approach, first of all, pose the question of the necessity and limits of regulation in the spheres of high technologies. Pondering over this issue, J. Ellul comes to the conclusion that legal regulation must focus not on the artificial intelligence, but on software. In his opinion, in case of critical software, for example, used in an aircraft, it does not matter if artificial intelligence is applied or not. Regulation should not touch upon a specific artificial intelligence technology; it should be broader and be implemented in relation to software in general. To prove this conclusion, Ellul gives one more example. When using artificial intelligence in banking or insurance systems which decide whether a specific credit or polis should be offered, regulation must be aimed at providing that clients are not discriminated. This requirement must be applied not only to the systems based on the artificial intelligence. It is quite feasible to program a decision making system, using methods not related to artificial intelligence (Ellul, 2022).

Supporting this viewpoint in general, we should take into account that artificial intelligence is an umbrella term. Normative-legal acts justly and consistently distinguish between the notions "computer program"[12], "artificial intelligence"[13] and "artificial intelligence technologies"[14].

[12] Article 1261 of the Russian Civil Code.

[13] Order of the President of the Russian Federation of October 10, 2019 No. 490 "On developing artificial intelligence in the Russian Federation", which introduces the National strategy of developing artificial intelligence up to 2030.

[14] Article 2 of Federal Law of April 24, 2020 No. 123-FZ "On making an experiment of establishing special regulation with a view of creating the necessary conditions for developing and introducing the artificial intelligence technologies in the Russian Federation subject – city of federal significance Moscow and introducing changes into Articles 6 and 10 of Federal Law "On personal data".

Note to clause 3.18 of the National Standard "Artificial intelligence systems. Classification of the artificial intelligence systems"[15] highlights that artificial intelligence as a complex of technological solutions includes information-communication infrastructure, software (including that using machine learning methods), processes and services of data processing, analysis and synthesis of solutions.

Scientific literature also raises the question whether artificial intelligence is a single object or an umbrella notion (Balashova, 2022). To solve this question, L. Yu. Vasilevskaya et al. propose including artificial intelligence into the list of complex intellectual rights objects, stipulated in Article 1240 of the Russian Civil Code. According to the authors, the structural elements of artificial intelligence are a software product (computer program); software (a set of programs); artificial neural networks (computer programs); algorithms, software as know-how; technical solutions as inventions; data bases (Vasilevskaya et al., 2021).

Thus, although a computer program is a core of the artificial intelligence technology, it is wrong to equate these notions. It is the distinctive features of artificial intelligence systems, their specific characteristics and the presence of structural elements being independent objects of civil rights that determine the features of legal regulation of relations in the sphere of their development and use.

Application of the technological approach is also aimed at preventing duplication of legal requirements in the spheres where they are already introduced. In this regard, J. Ellul poses one more question: should software for planning tasks in a calendar, for example, be more regulated than required by the current laws (for example, the law on personal data protection or consumer rights protection) (Ellul, 2022)? We believe that this question should be answered positively. Technological development changes the process of interaction of the turnover participants, and, consequently, the content of their rights and obligations. For example, Article 12 of the Law on consumer rights protection stipulates the obligation of the producer (executor, seller) to timely provide the consumer with the necessary and reliable information about the goods (works, services). At the same time, in the digital society information is provided, as a rule, in the digital form. Alongside with that, software appears which simplifies information search. A. I. Savelyev justly notes that in future, probably, a consumer will bear the risk of non-acquaintance with the information placed by the producer in publicly accessible sources (Savelyev, 2016). Moreover, a legislator introduces new subjects into the civil turnover. For example, in June 2018 the Law "On making changes in the 'Law of the Russian Federation on consumer rights protection' "[16] introduced special regulation of activity of an owner of information aggregator on goods (services).

---

[15] GOST R 59277-2020. National Standard of the Russian Federation. Artificial intelligence systems. Classification of the artificial intelligence systems. Date of introduction 01.03.2021.

[16] "On making changes in the 'Law of the Russian Federation on consumer rights protection'": Federal Law of 29.07.2018 No. 250-FZ. http://www.consultant.ru/document/cons_doc_LAW_303537/

Using the artificial intelligence technologies for processing and storing personal data is associated with risks of their leaking or incorrect interpretation. Since 1995, the European Parliament has been solving the problem of such risks management[17]. In 2016, the EU "Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data" proposed a model aimed at solving the task of improved personal data protection. Implementation of this model, in the opinion of the Regulation drafters, should promote forming a trustful attitude towards technologies[18].

The final question studied in J. Ellul's work is: must obligatory regulation be oriented directly towards technologies or towards a certain sphere or type of activity, during the implementation of which they are used (Ellul, 2022)? When answering this question, one should take into account that a risk of error is inherent in software of any complexity, regardless of it having elements of artificial intelligence or not. As software systems in general (not obligatory using artificial intelligence) "grow in complexity, interconnectedness, and geographical distribution, we will increasingly face unwanted emergent behavior" (Mogul, 2006). That is, interaction of a technology with the environment creates additional complexities and risks. To minimize such risks, it is necessary, first of all, to introduce quality standards of software[19]. Then, it is necessary to assess the risk level of the types of activity, during the implementation of which the technology is used (as was said in the first part of the article). If a certain type of activity refers to a high-risk group, a requirement must be stipulated about an obligatory application of the respective standard. Thus, obligatory regulation must be oriented not on technology but on the type of activity, during the implementation of which it is used.

Viewing the main questions raised by the representatives of the technological approach, one should consider a research by Ronald Leenes. The researcher from the Netherlands points out that it is rather difficult to identify gaps in the legal regulation of relations in the sphere of using technologies. First of all, one should define the essential and specific characteristics of the technology. While solving this task, should one focus on a specific technology, like unmanned automobiles, or consider a broader category, like unmanned vehicles?

---

17 On the protection of individuals with regard to the processing of personal data and on the free movement of such data: Directive 95/46/EC of October 24, 1995. (Directive 95/46/EC "On personal data").

18 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data: Regulation 2016/679 of April 27, 2016.

19 See, for example: GOST 28195-89. Assessing the quality of software. General provisions. Introduced on 01.07.1990; GOST 28806-90. Quality of software. Terms and definitions. Introduced on 01.01.1992; GOST R 51188-98. Protection of information. Testing software for the presence of computer viruses. Standard guidelines. Introduced on 01.07.1999.

According to Leenes, both approaches are disadvantageous. Focusing on a specific technology may result in a regulator concentrating on potentially accidental features of the technology. Otherwise, an excessive generalization may make the discussion abstract, hence useless. That is why, at the present stage, one should take a "social-technical prism" and, alongside with determining specific characteristics of the technology, reveal whose interests should be important and prioritized (Leenes, 2019).

At the second stage, it is necessary to solve the question of technology development, to which end reveal the potential risks and current problems associated with their use. Unfortunately, the categories of "risk" and "problem" are often confused in the scientific literature, making it hard to distinctly define the limits and tasks of legal regulation in the sphere of social relations under study. Assumingly, one of the main risks of using the artificial intelligence technologies is the possibility of it autonomously deviating from the target initially built in it. As a result if such risk materialization, certain negative consequences may occur, such as harm to life, health or property of the user, or disclosure of confidential information.

The need to distinguish between the "risk" and "problem" categories was pointed out by E. A. Voinikanis, E. V. Semenova and G. S. Tyulyaev. They mention such risks of using the artificial intelligence technologies as, in particular, the possibility of data de-anonymization, possibility of discrimination based on gender, race, nationality, or confession. They pose such problems as who is a right holder of artificial intelligence software, who is responsible for incurring harm to life or health when using artificial intelligence, etc. (Voinikanis et al., 2018).

At the third stage, one should define the forms and limits of state interference into the sphere of the artificial intelligence technologies. The means of risk management and solving the problems of minimizing the negative consequences of their materialization are different. For example, the means of risk management may include keeping a register during the system functioning and providing transparency of the decision-making process, so that the users may interpret the output data. In relation to high-risk system, post-marketing monitoring should also be introduced, in order to collect and analyze data about the system functioning after its launching into market.

If, despite the preventive control measures taken, the system malfunctions, law must provide the means for just distribution of negative consequences between its developer, user, and operator.

One should also take into account that the means of influencing the risks and problems are various and not always legal in form. At that, according to a just remark by M. Scherer (Scherer, 2016), traditional methods of legal regulation, such as, for example, licensing production, control over researches, possibility to apply delict liability are not quite suitable for risk management in the sphere of using artificial intelligence systems.

Conclusions

The use of risk-oriented approach implies building constructive models of risk management. The process of risk management consists of three main stages. At the first stage, it is necessary to identify and classify all risks related to using the artificial intelligence technologies in a certain sphere. The concept of risk-oriented approach, proposed by the European Parliament, focuses on internal and non-systemic risks. Accordingly, in order to develop this approach, it is necessary to research the external and systemic risks. At the second stage, it is necessary to assess the risk level of using a specific artificial intelligence technology. When making the assessment, several criteria should be used. Among them are the essential and specific characteristics of the technology, the sphere and type of activity, during implementation of which this technology is used. At the third stage, one should identify the means of risk management, which, in turn, are differentiated depending on the risk level of a specific technology. As one can see, the main objective of applying the risk-oriented approach consists in determining the means of risk management, associated with the use of the artificial intelligence technologies.

The technological approach is focused on the necessity and limits of regulation in the sphere of high technologies. The main stages of applying the technological approach are the following:

– determining the essential and specific characteristics of the technologies;

– revealing the potential risks and current problems of their use;

– determining the forms and limits of the state interference into the sphere of the artificial intelligence technologies.

It is the specific characteristics of the artificial intelligence technologies, such as autonomy and self-learning ability that determine the features of legal regulation of relations in the sphere of their development and use. At that, legal regulation should be oriented not on technology but on the type of activity, during the implementation of which it is used.

The research carried out also allows concluding that a universal approach to regulating relations in the sphere of technologies development and use is the technological approach. Although this approach needs further development, it may right now serve as the basis for forming the strategy of law-making activity. In turn, the risk-oriented approach is one of the main elements of the technological approach. Effective management of the accompanying risks will enable to minimize the potential negative consequences of using new technologies and will provide the sustainable development of the sphere of high technologies.

References

Alekseev, A. O., Erahtina, O. S., Kondratyeva K. S., & Nikitin, T. Ph. (2020). Approaches to civil legal liability of the artificial intelligence technologies developer: based on the classification. *Information Society*, *6*, 47–57. (In Russ.).

Balashova, A. I. (2022). Artificial intelligence in copyright and patent law: objects, subject structure of legal relations, terms of legal protection. *Zhurnal Suda po intellektual'nym pravam*, *2(36), 90–98.* (In Russ.).

Calo, R. (2011). *Open robotics. Maryland Law Review*, *70.3, 101–142*.

Ellul, J., Pace, G., McCarthy, S., Sammut, T., Brockdorf, J., & Scerri, M. (2021). Regulating artificial intelligence: a technology regulator's perspective. In: *Proceedings of the Eighteenth International conference on artificial intelligence and law* (pp. 190–194). https://doi.org/10.1145/3462757.3466093

Ellul, J. (2022). Should we regulate Artificial Intelligence or some uses of Software? *Discover Artificial Intelligence*, *2*(5). https://doi.org/10.1007/s44163-022-00021-9

Erdélyi, O. J., & Goldsmith, J. (2018). Regulating artifcial intelligence: proposal for a global solution. In *Proceedings of the 2018 AAAI/ACM conference on AI, ethics, and society* (pp. 95–101).

Gellert, R. (2021). The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual? *Journal of Ethics and Legal Technologies*, *3*(2), 15–33.

Gonçalves, M. E. (2020). The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research*, *23*(2), 139–152. https://doi.org/10.1080/13669877.2018.1517381

Hamon, R., Junklewitz, H., Sanchez, I., Malgieri, G., & De Hert, P. (2022). Bridging the gap between AI and explainability in the GDPR: towards trustworthiness-by-design in automated decision-making. *IEEE ComputIntell Mag.*, *17*(1), 72–85. https://doi.org/10.1109/mci.2021.3129960

Leenes, R. (2019). *Regulating New Technologies in Uncertain Times*. https://doi.org/10.1007/978-94-6265-279-8_2

Mikhaleva, E. S., & Shubina, E. A. (2019). Challenges and Prospects of the Legal Regulation of Robotics. *Actual Problems of Russian Law*, *1*(12), 26–35. (In Russ.). https://doi.org/10.17803/1994-1471.2019.109.12.026-035

Mogul, J. C. (2006). Emergent (mis)behavior vs. complex software systems. *ACM SIGOPS Oper. Syst. Rev.*, *40*(4), 293–304. https://doi.org/10.1145/1218063.1217964

Ponkin, I. V., & Redkina, A. I. (2018). Artificial Intelligence from the Point of View of Law. *RUDN Journal of Law*, *22*(1), 91–109. (In Russ.). https://doi.org/10.22363/2313-2337-2018-22-1-91-109

Savelyev, A. I. (2016). Directions of freedom of contract evolution under the influence of modern information technologies. In M. A. Rozhkova (head of authors' collective and editor-in-chief), *Svoboda dogovora*. Moscow: Statut. (In Russ.).

Scherer, M. U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, *29*(2), 353–400. https://doi.org/10.2139/ssrn.2609777

Smuha, N. A. (2021). From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence. *Law. Innov. Technol.*, *13*(1), 57–84. https://doi.org/10.1080/17579961.2021.1898300

Vasilevskaya, L. Yu., Poduzova, E. B., & Tasalov, F. A. (2021). *Digitalization of civil turnover: legal characteristics of "artificial intelligence' and "digital" subjects (civilistic research)* (In 5 Vol.). Moscow: Prospekt. (In Russ.).

Voinikanis, E. A., Semenova, E. V., & Tyulyaev, G. S. (2018). Artificial intelligence and law: challenges and possibilities of self-learning algorithms. *Proceedings of Voronezh State University. Series: Pravo*, *4*(35), 137–148. (In Russ.).

Wagner, B. (2018). Ethics as an escape from regulation: from ethics-washing to ethics-shopping. In *Being profiling: cogitas ergo sum* (pp. 86–90). Amsterdam: Amsterdam University Press. https://doi.org/10.1515/9789048550180-016

Zielke, T. (2020). Is artificial intelligence ready for standardization? In: *European conference on software process improvement* (pp. 259–274). Springer.

Author information

Olga S. Erahtina – Candidate of Sciences in Jurisprudence, Associate Professor, Department of Civil and Entrepreneurial Law, Perm branch of National Research University "Higher School of Economics"
Address: 38 Studencheskaya Str., 614070 Perm, Russian Federation
E-mail: oerahtina@hse.ru
ORCID ID: https://orcid.org/0000-0002-9041-3487
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/K-3149-2014
Google Scholar ID: https://scholar.google.ru/citations?hl=ru&user=WdwWB4kAAAAJ
RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=498773

Conflict of interests

The author declares no conflict of interests.

Financial disclosure

The research was not sponsored.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – February 10, 2023
Date of approval – April 23, 2023
Date of acceptance – June 16, 2023
Date of online placement – June 20, 2023

Научная статья
УДК 340.143:004.8
EDN: https://elibrary.ru/lbwsxw
DOI: https://doi.org/10.21202/jdtl.2023.17

Подходы к регулированию отношений в сфере разработки и применения технологий искусственного интеллекта: особенности и практическая применимость

Ольга Сергеевна Ерахтина

Пермский филиал Национального исследовательского университета «Высшая школа экономики»
г. Пермь, Российская Федерация

Ключевые слова

Искусственный интеллект,
опасность,
право,
программное обеспечение,
регулирование,
рискориентированный подход,
технологический подход,
управление рисками,
цифровая экономика,
цифровые технологии

Аннотация

Цель: обзор сложившихся в науке подходов к регулированию отношений в сфере применения технологий искусственного интеллекта, выявление основных особенностей и ограничений применения рискориентированного и технологического подходов для определения направлений их дальнейшего развития.

Методы: методологическую основу исследования составляет совокупность методов научного познания, в том числе общенаучный диалектический и универсальные научные методы (анализ и синтез, сравнение, обобщение, структурно-функциональный, формально-логический).

Результаты: определено, что применение рискориентированного подхода предполагает построение конструктивных моделей управления рисками. Значимым вопросом для применения данного подхода является вопрос об основаниях отнесения технологий искусственного интеллекта к высокорисковым. При определении уровня риска применения технологии искусственного интеллекта необходимо применять следующие критерии: тип технологии искусственного интеллекта, сферу ее применения, а также уровень ее потенциальной опасности для окружающей среды, здоровья, других фундаментальных прав граждан.

В свою очередь, центральным вопросом для применения технологического подхода является вопрос о необходимости и пределах регулирования сферы разработки и применения технологий искусственного интеллекта. Во-первых, вмешательство в данную сферу не должно создавать препятствий для развития технологий и инноваций.

Во-вторых, естественная реакция регулятора в ответ на появление новых объектов и субъектов оборота – «синдром несовершенного закона». Вместе с тем ложное представление об отсутствии правового регулирования может дать обратный эффект – дублирование правовых норм. В целях решения проблемы дублирования законодательных требований следует прежде всего решить вопрос о том, необходимо ли регулировать технологии искусственного интеллекта или некоторые виды использования программного обеспечения.

Научная новизна: проведен обзор основных подходов к регулированию отношений в сфере разработки и применения технологий искусственного интеллекта, выявлены возможности и ограничения их применения, предложены дальнейшие направления их развития.

Практическая значимость: основные положения и выводы исследования могут быть использованы для определения оптимальных подходов к регулированию сферы цифровых технологий, а также в целях совершенствования правового регулирования рассматриваемой области общественных отношений.

Для цитирования

Ерахтина, О. С. (2023). Подходы к регулированию отношений в сфере разработки и применения технологий искусственного интеллекта: особенности и практическая применимость. *Journal of Digital Technologies and Law*, *1*(2), 421–437. https://doi.org/10.21202/jdtl.2023.17

Список литературы

Алексеев, А. О., Ерахтина, О. С., Кондратьева, К. С., Никитин, Т. Ф. (2020). Подходы к гражданско-правовой ответственности разработчика технологий искусственного интеллекта: на основе классификации технологий. *Информационное общество*, *6*, 47–57. https://elibrary.ru/yldbab

Балашова, А. И. (2022). Искусственный интеллект в авторском и патентном праве: объекты, субъектный состав правоотношений, сроки правовой охраны. *Журнал Суда по интеллектуальным правам*, *2*(36), 90–98. EDN: https://elibrary.ru/apldua

Василевская, Л. Ю., Подузова, Е. Б., Тасалов, Ф. А. (2021). *Цифровизация гражданского оборота: правовая характеристика «искусственного интеллекта» и «цифровых» субъектов (цивилистическое исследование)* (в 5 т.). Москва: Проспект. https://elibrary.ru/nrjkdo

Войниканис, Е. А., Семенова, Е. В., Тюляев, Г. С. (2018). Искусственный интеллект и право. Вызовы и возможности самообучающихся алгоритмов. *Вестник Воронежского государственного университета. Серия: Право*, *4*(35), 137–148. https://elibrary.ru/yumlnz

Михалева, Е. С., Шубина, Е. А. (2019). Проблемы и перспективы правового регулирования робототехники. *Актуальные проблемы российского права*, *12*(109), 26–35. https://doi.org/10.17803/1994-1471.2019.109.12.026-035

Понкин, И. В., Редькина, А. И. (2018). Искусственный интеллект с точки зрения права. *Вестник РУДН. Серия: Юридические науки*, *22*(1), 91–109. https://doi.org/10.22363/2313-2337-2018-22-1-91-109

Савельев, А. И. (2016). Направления эволюции свободы договора под влиянием современных информационных технологий. В сб. М. А. Рожкова (рук. авт. кол. и отв. ред.), *Свобода договора*. Москва: Статут. https://elibrary.ru/xxoolt

Calo, R. (2011). Open robotics. *Maryland Law Review*, 70.3, *101–142*.

Ellul, J., Pace, G., McCarthy, S., Sammut, T., Brockdorf, J., & Scerri, M. (2021). Regulating artifcial intelligence: a technology regulator's perspective. In *Proceedings of the Eighteenth International conference on artifcial intelligence and law* (pp. 190–194). https://doi.org/10.1145/3462757.3466093

Ellul, J. (2022). Should we regulate Artificial Intelligence or some uses of Software? *Discover Artificial Intelligence*, *2*(5). https://doi.org/10.1007/s44163-022-00021-9

Erdélyi, O. J., & Goldsmith, J. (2018). Regulating artifcial intelligence: proposal for a global solution. In *Proceedings of the 2018 AAAI/ACM conference on AI, ethics, and society* (pp. 95–101).

Gellert, R. (2021). The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual? *Journal of Ethics and Legal Technologies*, *3*(2), 15–33.

Gonçalves, M. E. (2020). The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research*, *23*(2), 139–152. https://doi.org/10.1080/13669877.2018.1517381

Hamon, R., Junklewitz, H., Sanchez, I., Malgieri, G., & De Hert, P. (2022). Bridging the gap between AI and explainability in the GDPR: towards trustworthiness-by-design in automated decision-making. *IEEE Comput Intell Mag.*, *17*(1), 72–85. https://doi.org/10.1109/mci.2021.3129960

Leenes, R. (2019). *Regulating New Technologies in Uncertain Times*. https://doi.org/10.1007/978-94-6265-279-8_2

Mogul, J. C. (2006). Emergent (mis) behavior vs. complex software systems. *ACM SIGOPS Oper. Syst. Rev.*, *40*(4), 293–304. https://doi.org/10.1145/1218063.1217964

Scherer, M. U. (2016) Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, *29*(2), 353–400. https://doi.org/10.2139/ssrn.2609777

Smuha, N. A. (2021). From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence. *Law. Innov. Technol.*, *13*(1), 57–84. https://doi.org/10.1080/17579961.2021.1898300

Wagner, B. (2018). Ethics as an escape from regulation: from ethics-washing to ethics-shopping. In *Being profling: cogitas ergo sum* (pp. 86–90). Amsterdam: Amsterdam University Press. https://doi.org/10.1515/9789048550180-016

Zielke, T. (2020). Is artificial intelligence ready for standardization? In *European conference on software process improvement* (pp. 259–274). Springer.

Сведения об авторе

Ерахтина Ольга Сергеевна – кандидат юридических наук, доцент, доцент кафедры гражданского и предпринимательского права, Пермский филиал Национального исследовательского университета «Высшая школа экономики»
Адрес: 614070, Российская Федерация, г. Пермь, ул. Студенческая, 38
E-mail: oerahtina@hse.ru
ORCID ID: https://orcid.org/0000-0002-9041-3487
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/K-3149-2014
Google Scholar ID: https://scholar.google.ru/citations?hl=ru&user=WdwWB4kAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=498773

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 10 февраля 2023 г.
Дата одобрения после рецензирования – 23 апреля 2023 г.
Дата принятия к опубликованию – 16 июня 2023 г.
Дата онлайн-размещения – 20 июня 2023 г.