



Research article

UDC 34:004:346.6:004.8

EDN: <https://elibrary.ru/ruzmxxp>

DOI: <https://doi.org/10.21202/jdtl.2025.18>

Legal Mechanisms for Distributing the Responsibility for the Harm Caused by Artificial Intelligence Systems

Dmitriy Aleksandrovich Kazantsev

Chamber of Commerce and Industry of the Russian Federation, Moscow, Russia

Keywords

artificial intelligence,
autonomy,
delictual dispositive capacity,
digital technologies,
law,
legal liability,
legislation,
neural network,
risk-oriented approach,
robot

Abstract

Objective: to formulate proposals to form a system of subsidiary liability for harm resulting from the use of artificial intelligence systems.

Methods: the research is based on a comprehensive methodological basis, including the abstract logical method for theoretical understanding of the legal nature of artificial intelligence as an object of legal regulation; the method of comparison to analyze the Russian and European legislations on tort liability; generalization to systematize the existing concepts of responsibility distribution between subjects of law; and correlation analysis to identify the relationships between the typology of artificial intelligence systems and the mechanisms of legal responsibility for their functioning.

Results: the study summarizes and systematizes modern theoretical and legal concepts and regulations of the European Union and the Russian Federation on the distribution of subsidiary responsibility for the adverse effects of artificial intelligence. Potential subjects of responsibility were identified, as well as the key factors influencing the distribution of responsibility between them. A multidimensional matrix was developed for responsibility distribution between the subjects, taking into account their impact on the specific artificial intelligence system functioning and the systems typologization under the risk-based approach.

Scientific novelty: for the first time, an original concept is proposed, which combines the differentiation of the subjects' roles in terms of their real impact on the artificial intelligence results; the differentiation of artificial intelligence systems under the risk-based approach; and the system of legal

© Kazantsev D. A., 2025

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

presumptions of responsibility distribution corresponding to the above two classifications. The novelty lies in the creation of a multidimensional matrix of subsidiary liability, which allows taking into account many factors when determining the subject of responsibility in each specific case of harm caused by artificial intelligence systems, which differs significantly from existing unilateral approaches to this issue.

Practical significance: the research conclusions and suggestions can be used to develop the doctrine of subsidiary responsibility in the field of artificial intelligence use, to develop and modify the legal norms regulating artificial intelligence. The proposed multidimensional matrix of responsibility distribution can serve as a theoretical basis for improving judicial practice in cases of compensation for damage caused by artificial intelligence systems, as well as for creating an effective balance between stimulating the development of AI technologies and ensuring the protection of the rights and legitimate interests of individuals and legal entities.

For citation

Kazantsev, D. A. (2025). Legal Mechanisms for Distributing the Responsibility for the Harm Caused by Artificial Intelligence Systems. *Journal of Digital Technologies and Law*, 3(3), 446–471. <https://doi.org/10.21202/jdtl.2025.18>

Contents

Introduction

1. Robot and human: bases of delictual dispositive capacity
2. Prevention of violations in the field of using AI
3. Multidimensional matrix of subsidiary responsibility for AI functioning

Conclusions

References

Introduction

The increasing use of artificial intelligence systems in everyday life, as well as in various sectors of the economy and even public administration, makes neural networks and other forms of the so-called weak artificial intelligence not just an experimental tool, but also a factor in legal relations. An important and one of the most socially significant facets of these relationships is delict relationships – in other words, obligations arising as a result of harm caused by the use of artificial intelligence. In a broader discourse, it is necessary to resolve the issue of assigning and distributing responsibility for the adverse consequences of AI use.

Robotization of industries and the increasing use of artificial intelligence in various aspects of everyday life is shifting the issue of the legal consequences of a robot causing

harm to humans from theory to practice. The lack of appropriate regulation creates a legal vacuum, which can potentially create a situation of lack of responsibility for a whole group of offenses.

This, in turn, will inevitably entail the desire of individuals and legal entities to avoid, as far as possible, involvement in such legal relationships in which a potential violation of their rights and legitimate interests may have no consequences. Simply put, the unresolved legal liability of AI is one of the key factors in the depopularization of the daily use of digital technologies, and therefore an important obstacle to their development.

Even today, this issue has ceased to be theoretical-legal. Unfortunately, the robotization of industries, jobs, and services demonstrates very real examples of how the ill-conceived use of artificial intelligence damages not only the rights and legitimate interests of individuals or legal entities, but also damages human health, and in some cases even leads to deaths. For example, robotization of vehicles and delivery services, medical diagnostics and personal data processing, while remaining an absolute convenience and a promising way of improving the living standards, has costs in the form of significant risks to the life and health of citizens.

At a higher level of generalization, one may consider AI systems to be threats to basic civil rights. "The obvious dangers include: infringements on privacy by covert surveillance (the European Court of Human Rights has already heard a number of cases on covert surveillance of employees in the workplace); dependence of the exercise of constitutional rights on the will of other actors (for example, providers); inadequate confidentiality when processing digitized personal information; additional costs for purchasing technical means and devices (for example, mandatory use of electronic diaries of schoolchildren in large families); linking to an electronic address to obtain official or banking information, etc." (Kovler, 2022).

Working in the digital environment in general and the consequences of AI actions in particular cannot and should not remain outside legal regulation. The inadmissibility of using artificial intelligence to intentionally cause harm to people and organizations, as well as preventing and minimizing the risks of negative consequences of using artificial intelligence are among the fundamental principles of AI development both in the Russian Federation and abroad¹.

As the very first approximation, practice leads us to choosing one of several simple solutions regarding the future legal regulation of AI.

The first and, it would seem, the most obvious solution is a complete ban on the use of any artificial intelligence systems as potentially dangerous to humans. Today, this danger is no longer purely speculative. It has been proven in practice. This means that

¹ Decree of the Russian President No. 490 of 10.10.2019 (edited as Decree of the Russian President of 124 of 15.02.2024). (2024). Garant. <https://clck.ru/3NXX4N>

it is necessary to eliminate any such systems from use in order to eliminate this threat to human life and health.

However, today artificial intelligence is not only a risk factor, but also a factor in improving quality of life and convenience of work for people. In the information age, a ban on an information processing tool would be as destructive as, for example, a ban on using cars or airplanes on the grounds that traffic accidents and plane crashes occur with deplorable regularity.

The ban itself is by no means an ordinary, but an extreme, exclusive instrument of legal regulation. Simply put, if it is possible to do without a ban in the field of law, then it is better to do without prohibitions. Any ban is nothing more than a stated crisis of public relations in one area or another and an imperfect social and legal regulation.

This does not mean that prohibitions are completely unnecessary and all of them are destructive. It is only important to use this instrument of legal regulation with great care and only if its absence can generate objectively greater risks than its presence.

A good example is the differentiation of risk factors for the AI use provided in a document known as the EU Artificial Intelligence Act². According to this law, only those AI systems are subject to an unequivocal ban which are designed, for example, for biometric identification and categorization of people, building social rating systems, and the technologies that are directly aimed at destroying basic human and civil rights and freedoms. All other AI systems are subject only to more or less strict regulation, ranging from the maximum requirements for systems potentially capable of posing a threat to human life and health to the absence of any requirements for using AI in computer games.

Another extreme in solving the problem of legal regulation of the adverse effects of the AI use is to equate artificial intelligence technologies with force majeure circumstances or give them a similar status. At first glance, this is appropriate because the logic of information search and processing, even by weak AI, is not transparent to humans, which means that its solutions are far from predictable for humans.

However, the lack of full understanding does not mean that there is no possibility of influence. Continuing the analogy with a car, we can recall that in the 21st century, most motorists have rather vague understanding about the nuances of their car's design. Nevertheless, each of them is directly responsible for the consequences of managing the mechanism. In the same way, the impact on AI systems does not go beyond humans, even to the point of adjusting their algorithms in order to minimize the risk of erroneous decisions based on the results of big data processing.

In practice, any analogy between the work of an AI and a force majeure event will mean that there is no actual legal responsibility for the consequences of its work.

² European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act). EUR-Lex. <https://clck.ru/3NXX6n>

Meanwhile, the exclusion of such responsibility obviously creates a space for abuse, including the use of artificial intelligence to commit crimes that would go unpunished in this case.

Since neither a complete ban nor complete impunity of AI seem reasonable and possible, the third approach pushes us to include AI in the circle of legal responsibility subjects, at least in cases where a person objectively did not and could not participate in an erroneous malicious decision made by artificial intelligence. This approach deserves closer consideration from a legal point of view.

1. Robot and human: bases of delictual dispositive capacity

Law, at least in its current form, is anthropocentric. It is a regulatory system created by humans for relations in human society. The development of law is a reflection of social development, and the evolution of law is subordinated to the evolution of both society and the position of an individual in society. Even when we are dealing with a legal fiction, assigning responsibility to a legal entity, for example, practically means the occurrence of adverse consequences for specific individuals: managers, employees, owners, etc.

Apparently, legal regulation covers corporations, robots, other hardware and software systems, and mechanisms. Not limited to artifacts of human civilization, legal regulation in certain situations may even affect animals and plants (in particular, their breeding, turnover and handling). However, a non-human subject does not act as a subject of legal structures, not because of its “limitations” or “inferiority” in comparison with humans, but only because these structures emerged and were developing for many millennia precisely as a regulator of purely human behavior.

For example, the classical set of legal responsibility elements is commonly known to be a subject, a subjective side, an object and an objective side. While the presence of an object and an objective side is not eliminated by the fact of harm caused as a result of AI actions, the presence of the two remaining factors is debatable.

The European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics points to the increasing urgency of the liability for damage caused by artificial intelligence. At the same time, it notes that current legislation does not allow artificial intelligence to be liable even in cases where damage is caused to third parties³. Although the Resolution rather cautiously describes

³ European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). (2018). Official Journal of the European Union, 252–257. <https://clck.ru/3NXXAJ>

the prospects for the legal subjectivity of artificial intelligence, its draft dated May 31, 2016, formulated several approaches to consolidate “the legal nature of artificial intelligence: to treat it as physical persons, as legal entities, as animals or objects, or to create a new category with its own characteristics and consequences regarding the assignment of rights and obligations, including liability for damage”⁴.

Hence, the issue was raised at the regulatory level that the use of AI could create a high or even unacceptable risk to people’s lives, health, rights and legitimate interests, but this issue has not been resolved. Moreover, this risk is not determined by malicious AI actions. In this context, particularly relevant is the definition of “the legal nature of artificial intelligence: to treat it as physical persons, as legal entities, as animals or objects, or to create a new category with its own characteristics and consequences regarding the assignment of rights and obligations, including liability for damage”⁵.

Today, it seems premature to talk about assigning artificial intelligence the status of a legal entity. One has to agree that “the use of digital technologies using artificial intelligence at the current level of its development does not mean the emergence of new social relations that are qualitatively different from existing ones”. A similar opinion is: “Artificial intelligence does not act as a digital legal entity in relations on the turnover of digital rights in the operator’s information system. The operator uses digital technologies in entrepreneurship and applies elements of artificial intelligence in business models that do not generate digital legal relationships” (Andreev, 2021). In other words, artificial intelligence, being a tool for implementing traditional economic relations at a new technological level, does not generate fundamentally new legal relations so far.

This conclusion is also true from an ontological point of view. The skills of processing large amounts of information, including using self-learning technologies, do not create human-like thinking and consciousness. A fairly accurate and still relevant definition of AI is given in the above-mentioned Presidential Decree: “A set of technological solutions that allow simulating human cognitive functions (including self-learning and finding solutions without a predefined algorithm) and obtaining results comparable to at least the results of human intellectual activity when performing specific tasks”⁶. Today, the most realistic concept seems to be artificial intelligence as a software and hardware complex that has nothing in common with the human mind in terms of the essence of thinking, but is capable of solving generally similar or more complex tasks (Bokovnya et al., 2020).

⁴ Draft report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). (2016, May 31). Committee on Legal Affairs. <https://clck.ru/3NXXCu>

⁵ Nevejans, N. (2016). European Civil Law Rules in Robotics: Study. European Union. <https://clck.ru/3NXXFs>

⁶ Decree of the Russian President No. 490 of 10.10.2019 (edited as Decree of the Russian President of 15.02.2024 No. 124). (2024). Garant. <https://clck.ru/3NXXHJ>

Since similarity does not mean identity, assigning anthropomorphic features to a robot does not mean that it acquires identity with a human. Hence, given both the achieved technological and legal development, “obvious is the inconsistency of the proposal to recognize artificial intelligence as a legal personality similar to that of an individual, and despite using the human brain principles to build an artificial intelligence system, the principles of legal regulation of the human status cannot be applied to artificial intelligence” (Durneva, 2019).

Despite the rapid development of neural networks and robotics, the conclusion remains relevant that “giving robots (artificial intelligence systems) the legal entity status will not entail any explicit negative consequences in the foreseeable future. At the same time, the advantages of such a solution are not apparent compared to considering robots (artificial intelligence systems) as quasi-subjects of law. Based on Occam’s philosophical principle not to multiply entities unless absolutely necessary, we believe that the introduction of such a fundamentally new legal entity as a robot (artificial intelligence system) into the legal sphere is premature (although it is possible that such a need may arise)” (Channov, 2022). Assigning human rights to AI would be just a purely incorrect extrapolation of human properties to AI (Duffy & Hopkins, 2013), without taking into account the specifics of either humans or artificial intelligence.

Putting this as simple as possible, one may argue that today it seems premature to assign AI the status of a legal entity. Yes, in many aspects, AI is qualitatively superior to humans both in the speed of information processing and in the volume of information being processed. However, assigning anthropomorphic features to a robot does not mean that it acquires identity with a human. Similarly, assigning AI the legal status of a human would only be an extrapolation of human properties to AI, which accounts the specifics of neither humans nor artificial intelligence.

The very phenomenon of delictual dispositive capacity is inextricably linked with the concept of legal personality. To simplify matters as much as possible, only a legal entity can be legally responsible. A party that is not a subject of law is not legally responsible. However, in a situation where the cause of tort obligations was the actions of an AI, i. e. an entity not being a subject of law, it is still necessary to have a mechanism of legal liability. It is obvious that even in the case of harm caused by artificial intelligence the subject of legal responsibility will be the subject of law or several such entities.

At the same time, it is important to emphasize that the legal principle of proportionality requires the imposition of responsibility on those persons whose actions directly or indirectly caused the occurrence of tort obligations.

2. Prevention of violations in the field of using AI

The theoretical and legal comprehension of the tort consequences of using artificial intelligence should not be limited to working with *fait accompli* and assigning responsibility for them. Such an approach appears to be inherently insufficient. It is not only possible, but

also necessary that the mechanisms for prevention, or rather, minimizing the risk of harm caused by artificial intelligence be included in the theoretical and legal justification, and then applied regulation.

To do this, first of all, it is necessary to theoretically substantiate, practically test (and, where possible and necessary, also normalize) the correct balance between the roles of humans and artificial intelligence in the implementation of business processes in economic relations. Legal regulation, in turn, should be adequate to these fundamental approaches. First of all, we should recognize that it is unacceptable to entrust AI with making key decisions on issues affecting the rights and legitimate interests of individuals and legal entities in any relationship. Such decisions must remain the exclusive prerogative of humans wherever possible.

The point here is not only and not so much in the above-mentioned principle of anthropocentrism of law. More precisely, this circumstance is due to the fact that a person is involved in the range of potential consequences of the robot's activity not as a subject, but as an object. For example, if a decision is made about an emergency shutdown of a power plant or an emergency discharge of water from a reservoir, even the most advanced algorithm, in the absence of complex additional settings, will evaluate the purely economic consequences of each possible solution. It may well turn out that the sudden flooding of a nearby village will be considered economically feasible by artificial intelligence in this situation. For other reasons, but with the same fatal logic, a decision may be made to hit a pedestrian or turn off life support systems. Postulating such principles as "a robot must protect a human" and "a robot cannot harm a human" at the level of basic AI algorithms cannot mitigate this risk: too often linear logic, divorced from ethics, will push to protect one person by harming another.

This brings us back to the concept of the subjective side of the offense. A highly qualified development team can create an algorithm that allows, to a certain extent, including human interests as the highest priority in the robot's decision-making mechanism. But even this will not endow the robot with the moral and ethical properties of a human being, imitate moral experiences and a psycho-emotional attitude to the action performed. Existing AI systems have such specific characteristics as non-transparent decision-making, autonomy, self-learning, and unpredictability in some cases from the viewpoint of human logic (Llorca, 2023).

One should remember: the methods of human thinking qualitatively differ from those of information processing by conditional artificial intelligence. These are two different types of information processing, each with its own advantages and disadvantages. Even if there are similar goals, it is inappropriate to transfer the properties of one type to another. The discussion about the possibility of artificial intelligence having consciousness as such remains beyond the scope of this article, but it is hardly possible to expect a human-type consciousness from artificial intelligence.

Under these conditions, as a general rule, only a person, having proper expertise, developed ethical principles, and an anthropocentric axiology, can make decisions within the limits of their authority that affect the key rights and legitimate interests of another person. Therefore, today, artificial intelligence, as a general rule, can only be a source of data for an expert, and not a substitute for that expert. Moreover, the rule remains relevant: the less threats a potential AI error can pose to the life and health of individuals, the more appropriate it is to use AI.

If this rule is followed, fundamentally new legal structures are not required to regulate liability for harm resulting from the work of AI. The distribution of tort obligations may well be resolved using existing legal mechanisms. At the same time, the high autonomy of AI in decision-making, even if it does not place it among the subjects of law, requires thoughtful consideration of the AI specifics when adapting existing norms and principles of law. “Traditional approaches to legal responsibility attribution require significant adaptation, necessitating a more nuanced, multi-level framework that maintains clear accountability chains” (Tianran, 2024).

One of the most significant areas of adaptation is the regulation of responsibility in situations when it is impossible to preserve decision-making by humans, since AI autonomy is the very essence of automating this process.

A good example is a robotic taxi, an autopilot of a marine vessel, or a robot for microsurgical operations. The technological complexity of the tasks they perform directly determines the economic and practical expediency of removing a human from controlling these operations. Simply put, if there is a driver at the wheel, then a robot in such a taxi is no longer needed; and if a taxi is operated by a robot, then the presence of a driver negates the economic benefits of taxi robotization. It is for such situations that new legal mechanisms for regulating responsibility for the actions of artificial intelligence are relevant.

To a certain extent, in this situation, an analogy can be proposed between responsibility for the actions of an AI and those of an infant: both are not delictable but show high autonomy and limited predictability of their actions. A legal historian can even suggest an appeal to old, long-forgotten legal models. For example, the model of the relationship between paterfamilias and a slave in Roman law. Under this approach, “the legal status of AI becomes identical or close to that of Roman anthropomorphic collective organizations, or even more reduced – slaves, family members, children, including filius in potestate tua est” (Afanasyev, 2022). However, the simple principle “the master is legally responsible for all the actions of the slave” cannot be mechanically transferred to the model of distribution of responsibility for the consequences of the robot’s actions.

This does not mean that modern artificial intelligence is more complex in psycho-emotional terms than, for example, an ancient Roman gladiator. On the contrary, when

investigating the causes of a decision by artificial intelligence, we can more easily identify at least several key actors, and each of these subjects will be an individual, a legal entity, or a group of persons. “Relations using artificial intelligence are always relations between subjects of law or about objects of law. In any case, these are relationships that are initiated and programmed at one stage or another by a person – a subject of law with varying degrees of responsibility (including within the activities of legal entities). A person’s will to certain actions of artificial intelligence can be expressed in varying degrees: from the AI actions under the full control of a human will, to autonomous AI actions allowed and realized within their possible limits and consequences by a person (group of persons)” (Shakhnazarov, 2022).

This possibility, in turn, can and should become the basis for building a model of subsidiary responsibility (Laptev, 2019) for the actions of artificial intelligence between the subjects of law that could directly or indirectly influence such actions.

3. Multidimensional matrix of subsidiary responsibility for AI functioning

The issue of tort obligations arising from the activities of AI has been raised in theoretical-legal works for several years now (Bertolini, 2013). Special studies, as a rule, contain conclusions about subsidiary liability or a liability matrix; they serve as the basis on which the question of imposing adverse legal consequences is decided individually in each case, taking into account a set of facts (Bokovnya et al., 2020). This implies subjects such as the AI owner, user, developer, and third parties. It seems appropriate to base the matrix of distribution of legal responsibility for the consequences of AI actions on the balance of the rights, duties and responsibilities of these subjects.

Apparently, we cannot apply criminal or administrative penalties to AI. Any responsibility measure applied to AI will in any case entail adverse consequences for its user: for example, an administrative ban on AI operation for a certain period will mean costs not for the AI, but only for the entity that used this AI system in its business activities. “When considering AI liability, it is relevant to talk primarily about tort liability; that is, liability measures should be established as a reaction to the harm that AI can or does cause. At the same time, this is not always about linear responsibility, i.e. the responsibility of a person for the harm that they caused, but rather about combined responsibility, i.e. when, in addition to the harm-doer, other actors may be called to account” (Philipp, 2023).

A theoretical and legal solution to the issue of allocating responsibility for AI actions that have caused damage to individuals and/or legal entities is necessary as a basis for regulating the practical aspects of the consequences of such liability. “A fundamental issue underlying AI liability is responsibility fragmentation. Unlike traditional tools that function under direct human control, AI-driven systems operate autonomously based

on algorithmic decision-making. In product liability cases, manufacturers are generally held accountable for design flaws, but what happens when an AI system “learns” harmful behavior over time? Some legal scholars advocate for strict liability on manufacturers, similar to pharmaceutical industry regulations, while others propose shared responsibility models that include software developers, operators, and even end-users”⁷.

To resolve this issue, it is necessary, first of all, to identify a range of legal entities that are delictable and able to actually compensate for the damage caused by AI errors. For example, according to the long-held opinion of R. Leenes and F. Lucivero, the responsibility for the harm caused by AI lies with the person who programmed it or the person responsible for its operation, within the limits established by law (Leenes & Lucivero, 2014). At the same time, the principle of legal proportionality requires the existence of a causal relationship between the action (inaction) of such persons and the occurrence of the said harm. From this point of view, the following groups of potential subjects of responsibility can be distinguished:

1. AI developer.
2. AI owner.
3. AI user.
4. Third parties.

This list identifies the groups in which subgroups can be distinguished. For example, in practice, it is possible to separate AI customers from its developers; among third parties, one may distinguish those who had a direct impact on AI algorithms from those who posted false information in the public domain, which caused erroneous AI decisions, etc. In any case, by supplementing the generalized list above with two forms of guilt, one gets a two-dimensional matrix of subsidiary responsibility for the consequences of AI decisions (Table 1).

Table 1. Basic matrix of culpable responsibility for AI functioning

Subject of responsibility	Intent	Negligence
Developer		
Owner		
User		
Third parties		
Regulatory bodies		

Subsidiary liability is formed as a result of clarifying the presence and nature of guilt in each case. The matrix allows taking into account many factors: for example, whether the user followed the instructions of the developers during the AI operation; whether there were any restrictions in this particular AI model; whether they were brought to the

⁷ Upadhyay, Sh. (2025, March 6). Navigating Liability in Autonomous Robots: Legal and Ethical Challenges in Manufacturing and Military Applications. <https://clck.ru/3NXXNJ>

attention of the user; whether the AI system underwent proper training (and if not, whether the damage was caused by the fault of the developer or of the agent who provided data for training); to what extent the owner could control the AI operation or the user's actions, etc.

For example, based on the results of an expert examination (and, if necessary, investigative actions), it can be proved that adverse consequences have arisen due to fundamental design flaws. "When an artificial intelligence system is purchased embedded in other goods (for example, in a car), it seems unlikely that such contractual exclusions (for example, between the car manufacturer and the provider of artificial intelligence software) can be successfully transferred to the car buyer. At the same time, of interest is the idea of establishing the boundaries of developers' responsibility for defects in the creation of released artificial intelligence systems" (Kharitonova et al., 2022)⁸.

The thesis on the responsibility limits brings us to the question of legal presumptions in the field of regulating responsibility for AI actions. For example, one can distribute such presumptions of responsibility among the above-listed entities: "Primary responsibility rests with deploying organizations and system operators who maintain direct control over implementation, requiring them to ensure proper function, monitor performance, and implement necessary safeguards while maintaining comprehensive documentation. Secondary responsibility extends to system developers and manufacturers, encompassing technical standards compliance, safety features, and documentation requirements, including transparent decision-making processes and clear audit trails. Tertiary responsibility belongs to oversight bodies and regulatory authorities, who must establish standards, conduct regular audits, and maintain effective enforcement mechanisms. This layered framework ensures comprehensive coverage of responsibility while maintaining clear accountability chains throughout the system's lifecycle" (Tianran, 2024).

By supplementing our two-dimensional matrix with such presumptions, we obtain the following logic for allocating responsibility for AI actions (Table 2).

Table 2. Variant of the parity of responsibility for AI functioning

Order of bringing to responsibility	Guilt	
	Intent	Negligence
1. Owner		
2. Developer		
3. Customer		
4. User		
5. Regulatory and controlling bodies		
6. Information provider		
7. Third parties		

⁸ Naumov, V. B., Chekhovskaya, S. A., Braginet, A. Yu., & Mayorov, A. V. (2021). Legal aspects of using artificial intelligence: current problems and possible solutions: report of the Higher School of Economics. Moscow.

At the same time, “a high degree of AI autonomy cannot serve as a basis for reducing the responsibility of developers and manufacturers. If an AI developer has a greater degree of control over the functioning of an AI system than the system manufacturer, owner, or user, this should increase the developer’s responsibility for causing harm. This principle can be presented in a more universal interpretation: the degree of control over the AI system functioning is proportional to the responsibility for causing harm”⁹.

Without using presumptions, the issue of allocating responsibility for AI actions will indeed be difficult to resolve in many cases. However, such a linear distribution of presumptions seems to be a simplification. It is obvious to a practicing lawyer that this matrix cannot cover all possible combinations of responsibilities that potentially arise when using AI. Guiltless compensation for damages (both contractual and non-contractual) remains beyond it, as well as the design of the source of increased danger.

Yes, as a general rule of Part 2 of Article 1064 of the Russian Civil Code, a person who has caused harm is exempt from compensation if they prove that the harm was caused not through their fault. However, there are exceptions to this rule. One of them is established by Art. 1079 of the Civil Code: persons who own a source of increased danger are obliged to compensate for the damage caused, regardless of the presence or absence of guilt, if the damage was caused by this particular source of increased danger. The Supreme Court of the Russian Federation explains that a source of increased danger is “any activity that creates an increased likelihood of harm due to the inability of a person to fully control it”¹⁰.

Intuitively, AI falls under this definition, because it is autonomous in its decisions, is not fully controlled by humans, and is capable of harming individuals and legal entities. “The source of increased danger can be recognized through the following criteria: ‘activity’, ‘action’, and ‘harmfulness’. Having identified the necessary criteria, one has to find out whether the AI meets the specified requirements. The categories of ‘activities’ and ‘actions’ that pose a risk of harm are confirmed by the technically complex structure of the AI technology, as well as by the autonomous choice of a strategy for completing the task. The criterion of ‘harmfulness’ is revealed through the areas in which AI technology can be used. For example, the use of artificial intelligence in medicine in determining the diagnosis or in unmanned vehicle control presupposes the possibility of harming surrounding subjects. Thus, one may conclude that artificial intelligence can be recognized as a source of increased danger”¹¹.

⁹ Naumov, V. B., Chekhovskaya, S. A., Braginets, A. Yu., & Mayorov, A. V. (2021). Legal aspects of using artificial intelligence: current problems and possible solutions: report of the Higher School of Economics. Moscow..

¹⁰ On the application by courts of civil legislation, regulating relations on obligations due to harm to the life or health of a citizen: Resolution of the Plenum of the Supreme Court of the Russian Federation No. 1 of 26.01.2010, cl. 18.

¹¹ Pozdnyakova, M. (2025, April 3). Recognition of artificial intelligence as a source of increased danger: realities and prospects. Delovoy profil. <https://clck.ru/3NXXbo>

Indeed, “many AI systems (unmanned vehicles, drones, surgical robots, etc.) can be classified as sources of increased danger, and their use as activities that pose an increased risk to others” (Izhaev & Kuteynikov, 2024). This thesis is the starting point for concretizing the correct but abstract thesis about the individual decision on the subsidiary responsibility allocation in each specific case, taking into account a set of factors. “The incorporation of new AI systems into law will require considering their recognition as a source of increased danger” (Antonov, 2020); in this context, the owner of artificial intelligence appears to be the owner of a source of increased danger. By default, the owner is responsible for the adverse effects of artificial intelligence activities, but only until the guilt of other persons is proven.

Summarizing the above theses and partially complementing them, we may state that “according to the criterion of applying the existing legal regulation to harm caused by AI systems, the following approaches are possible:

- liability for harm caused by a source of increased danger;
- liability for damage caused due to defects (defects) of the product;
- guiltless liability for harm caused by extremely dangerous activities;
- analogy to the norms on liability for harm caused by animals. In particular, there are some similarities between robots and animals. For example, both robots and animals can act independently of their owners, perceive the environment and perform actions depending on it;
- analogy to the norms on liability for harm caused by employees. The employer’s liability for harm caused by an employee to third parties is related to the actions of the employee that caused harm, which they committed as part of work duties;
- analogy to the norms on liability for harm caused by children”¹².

All of these approaches are correct in their own way, but each of them can only be fully applied to individual AI use cases. After all, the concept of a source of increased danger today is no longer able to fully cover the practice of using AI. “Obviously, there are different types of AI systems, from robot vacuum cleaners to autonomous drones used in weapons. A large number of primitive AI systems will not have characteristics capable of causing any significant harm to humans. In this regard, the default usage of Art. 1079 of the Russian Civil Code and equating all AI systems to sources of increased danger is controversial. In part, we can agree with the expediency of detailing criteria for sources of increased danger in relation to AI systems. It should be borne in mind that in practice, the so-called activity approach can be used to determine the source of increased danger in

¹² Naumov, V. B., Chekhovskaya, S. A., Braginets, A. Yu., Mayorov, A. V. (2021). Legal aspects of using artificial intelligence: current problems and possible solutions: report of the Higher School of Economics. Moscow.

a particular situation. Its essence is reflected in the resolution of the Plenum of the Russian Supreme Court No. 138 dated 26.01.2010. The document states that within the meaning of Art. 1079 of the Russian Civil Code, as a source of increased danger is any activity that creates an increased likelihood of harm due to the inability of a person to fully control it, as well as activities related to the use, transportation, storage of objects, substances, and other industrial, economic, or other facilities with the same properties. This interpretation allows the court to determine on a case-by-case basis whether an AI system is a source of increased danger” (Izhaev & Kuteynikov, 2024).

Hence, not every AI system is a source of increased danger. This means that the application of the presumptions briefly listed above is subject-object in nature. In other words, it depends not only on the status of the legal responsibility subject, but also on AI system as the object, whose work results imply responsibility.

Here we return to the risk-based classification of the EU AI Act, mentioned at the very beginning of this article. To implement a risk-based approach, the Act identifies four groups of AI systems, which vary depending on the purpose:

1. Unacceptable risk category: biometric identification and categorization of people, social rating system, etc.;
2. High risk category: the use of AI which may create a direct threat to human life and health, for example, in transport or medicine;
3. Low risk category: the use of chatbots, the use of neural networks to create information content;
4. Minimum risk category: video games, assistants, recommendation systems.

The classification certainly deserves further development. For example, within the group of high-risk systems, it is worth separating systems with a risk to life and health, on the one hand, and systems with a risk to the property interests of individuals and legal entities, on the other. General purpose and specialized systems can be distinguished within low-risk systems. In any case, when allocating subsidiary responsibility, it is necessary to take into account not only the impact that tort-related subjects of law have on AI functioning, but also the nature of the specific AI system.

For example, “in cases where harm is caused by a high-risk AI system, it is advisable to use strict developer responsibility. This is due to the fact that such AI systems, by their very nature, can have a significant negative impact on human rights and freedoms, and therefore the latter should have increased protection guarantees” (Izhaev & Kuteynikov, 2024). The implementation of this approach shifts the discourse from the concept of a source of increased danger towards establishing its own system of presumptions for each group of AI systems, distinguished according to the risk-oriented principle.

As a result, we have a multidimensional matrix that takes into account at least the following parameters:

1. The role of a delictable legal entity in AI functioning;
2. The form of guilt and the existence of grounds for guiltless responsibility;
3. The category of the AI system from the viewpoint of the risk-oriented approach.

In such a multidimensional matrix, we are no longer limited to categorical statements that “the owner is primarily responsible for AI” or “the developer is responsible for AI, and we hold everyone else accountable only after the absence of the developer’s guilt is proven”.

Yes, such a multidimensional matrix is complicated. However, it is the only opportunity to achieve the balance of rights and duties and to maintain the balance of economic interests. After all, while the complete absence of legal regulation of liability can impede the AI industry development, excessive under-elaborated regulation is quite capable of creating similar problems. Simply put, if we presume the responsibility of the owner for the AI actions, then no one will want to buy such systems. If developers are held accountable by default, then few people will want to develop them.

One should agree that “in the light of the possible imposition of responsibility on developers, it is necessary, at least at the initial stages, to provide a balanced system of immunities for them, adding mandatory liability insurance, as well as registration of AI systems. If AI is recognized as a subject, it is possible to establish a regime of combined responsibility, when both the AI creator and owner or another subject can bear subsidiary responsibility”¹³. It seems that such subsidiary responsibility can be implemented most effectively within the framework of the multidimensional matrix proposed above.

Despite its complexity, the multidimensional matrix will allow not only to include all cases of AI use in the legal regulation, but also to take into account the variability, changeability and specific combinations of various algorithms. For example, an AI owner becomes the first candidate for subsidiary liability in the event of harm due to the use of “general-purpose AI systems, which are characterized by the ability to solve a wide range of tasks. As a general rule, they should be defined as low-risk AI systems. However, if they are used in high-risk products as a result of ‘fine-tuning’, then such systems should also be recognized as high-risk with corresponding consequences in resolving disputes arising from harm” (Philipp, 2023). As for high-risk systems, the presumption of responsibility can be placed primarily on customers and developers.

Conclusions

Law as a phenomenon and legal institutions as its manifestations do not develop in a vacuum of purely theoretical constructions, but only in the developing practice of economic relations. In this sense, the theoretical understanding of technical and economic realities follows the

¹³ Naumov, V. B., Chekhovskaya, S. A., Braginets, A. Yu., Mayorov, A. V. (2021). Legal aspects of using artificial intelligence: current problems and possible solutions: report of the Higher School of Economics. Moscow.

emergence of these realities. However, without theoretical understanding, neither systemic cognition nor professional regulation of new relationships are possible.

Today, due to the level of technology development and the involvement of innovative technologies in economic relations, the issue of AI responsibility is no longer only theoretical-legal but is rather of practical importance. Robots today can not only benefit, but also cause harm to both individuals and legal entities. Moreover, “the use of algorithmic systems poses particular threats to personal and political rights – the right to privacy, freedom of expression, and the right to participate in state governance through democratic procedures. In addition, due to the fact that algorithms and artificial intelligence technologies based on them process information from the external environment, the rights of personal data subjects should be under special protection in an algorithmic society” (Pibaev & Simonova, 2020).

The lack of special regulation creates a legal vacuum, which potentially means that there is no responsibility for a group of offenses. This, in turn, is a key factor in the depopularization of using digital technologies, and therefore an important obstacle to their development. However, ill-conceived regulation can become the same, if not a more significant obstacle to using AI in everyday and industrial matters.

The first but important step towards practical regulation should be the theoretical-legal elaboration of issues of responsibility for the consequences of AI use. “There is still no clear understanding of how to resolve the problems of imposing non-contractual civil liability for harm caused by AI systems. On the one hand, regulation should stimulate the AI sector development and not contain excessively burdensome provisions for developers and professional operators. On the other hand, it is necessary to ensure a high level of protection of the rights of humans and society, since the latter will obviously be the weak side in such disputes. Thus, it is obvious that searching for optimal and adequate approaches to the legal regulation of legal liability is urgent” (Izhaev & Kuteynikov, 2024).

Today, the issue of responsibility for the consequences of AI actions can be resolved positively, since the intentional or at least careless fault of “artificial intelligence intermediaries (developers and users) in the event of harm by an artificial intelligence system can be quite probable, legally and expertly provable” (Ivliev & Egorova, 2022). This means that the principle of “delineating the responsibilities of organizations that develop and use artificial intelligence technologies based on the nature and degree of harm caused” already seems feasible¹⁴.

¹⁴ Decree of the Russian President No. 490 of 10.10.2019 (edited as Decree of the Russian President of 15.02.2024 No. 124). (2024). Garant. <https://clck.ru/3NXXig>

However, the possibility of a positive solution to the issue does not mean that it is easy to solve. First of all, it is necessary to rely on the following fundamental assumptions:

1. The current levels of development of both law and artificial intelligence technologies do not allow considering a robot as a subject of legal relations or of legal responsibility.

2. The impossibility of recognizing the delictability of artificial intelligence does not mean that it must be recognized as force majeure or that it cannot be held responsible for the consequences of artificial intelligence actions.

3. Responsibility for the consequences of AI actions is distributed between its creators, owners, users and other persons involved in using the robot, in the extent that they affect the results of the artificial intelligence functioning.

4. The combination of liability, including subsidiary liability, in each specific case depends both on the type of the AI system and on whose actions influenced the AI's decision which resulted in the tort obligations.

For example, "the user or owner may be held liable if the instructions for using artificial intelligence are violated, especially in situations where the user was informed of specific requirements for the system operation. If we are talking about the user or the owner, then the model of responsibility for harm caused by a source of increased danger is the closest to this type of relationship. The data provider is responsible if the damage occurred when the system was still being trained, or if low-quality data was provided. It should also be borne in mind that the artificial intelligence system can be released with an open source code. In this case, experts speak of holding programmers accountable. Also, in some cases, if the damage is caused by deep-seated problems of the artificial intelligence system, the question arises of holding the designer or manufacturer of the artificial intelligence system accountable. Since artificial intelligence systems often operate in the aforementioned 'black box' paradigm, in some cases it may be impossible to identify the person by whose will or negligence the harm was caused" (Shakhnazarov, 2022)¹⁵.

In these circumstances, a positive solution to the issue of subsidiary liability is impossible without applying the legal structures that are close (but not necessarily identical) to the concept of a source of increased danger. At the same time, it seems that such a structure, applicable in the field of responsibility for AI decisions, should not be limited only to the guiltless responsibility.

Somewhat simplifying, we can propose a system of responsibility presumption. Within this system, the guilt of each of the delictable legal entities is investigated in a top-down manner. Only in the case when it is objectively impossible to establish guilt, guiltless responsibility is applied.

¹⁵ Naumov, V. B., Chekhovskaya, S. A., Braginets, A. Yu., & Mayorov, A. V. (2021). Legal aspects of using artificial intelligence: current problems and possible solutions: report of the Higher School of Economics. Moscow.

At the same time, the hierarchy of presumptions depends on the AI category within a risk-based approach. According to it, at least the following categories of AI can be distinguished:

1. High-risk AI that can pose a threat to human life and health;
2. High-risk AI that can pose a threat to the property of individuals and legal entities;
3. High-risk AI that can create a threat of disclosure of personal data and other information with limited access;
4. Medium-risk AI that can pose a threat to the proper conduct of business operations;
5. Medium-risk AI that can pose a threat to production processes and the functioning of infrastructure facilities;
6. Medium-risk AI of general purpose;
7. Low-risk AI.

For each of these categories, an individual system of responsibility presumptions is built for the following subjects:

1. AI owner;
2. AI customer;
3. AI developer;
4. AI user;
5. Regulatory and controlling bodies;
6. Providers of information for AI;
7. Third parties.

The proposed multidimensional matrix of responsibility for harm caused by AI actions is schematically presented in Table 3, where, for each cell in the indicated order, the question of intentional or negligent guilt is first investigated and then the possibility of guiltless liability.

Table 3. Multidimensional matrix of responsibility for AI functioning

Categories of AI systems	Subjects of responsibility						
	Owner	Customer	Developer	User	Regulatory bodies	Information provider	Third parties
High-risk AI that can pose a threat to human life and health	3	1	2	6	4	5	7
High-risk AI that can pose a threat to the property of individuals and legal entities	3	1	2	4	5	6	7
High-risk AI that can create a threat of disclosure of personal data and other information with limited access	4	1	2	3	6	5	7
Medium-risk AI that can pose a threat to the proper conduct of business operations	1	4	5	2	3	6	7
Medium-risk AI that can pose a threat to production processes and the functioning of infrastructure facilities	1	3	4	2	6	5	7
Medium-risk AI of general purpose	1	4	3	2	5	7	6
Low-risk AI	4	3	2	1	5	7	6

Thus, the formal inability to impose a punishment or other measure of legal responsibility on a robot today does not at all prevent the full inclusion of relations using artificial intelligence technologies in the sphere of legal regulation, including in terms of the legal consequences of harm. These innovative technologies require significant development of legal regulation, but they do not create either new legal institutions or fundamentally new legal structures. This means that with a proper approach to the essential understanding of the technological component, such regulation can be successfully implemented within the existing legal system.

References

- Afanasyev, S. F. (2022). On the problem of substantive and procedural legal personality of artificial intelligence. *Vestnik Grazhdanskogo Protsessa*, 3, 12–31. <https://doi.org/10.24031/2226-0781-2022-12-3-12-31>
- Andreev, V. K. (2021). Acquiring and exercising rights of a legal entity with the use of artificial intelligence. *Predprinimatelskoe Pravo*, 4, 11–17. <https://doi.org/10.18572/1999-4788-2021-4-11-17>
- Antonov, A. A. (2020). Artificial intelligence as a source of increased danger. *Yurist*, 7, 69–74. <https://doi.org/10.18572/1812-3929-2020-7-69-74>
- Bertolini, A. (2013). Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules. *Law, Innovation and Technology*, 5. <https://doi.org/10.5235/17579961.5.2.214>
- Bokovnya, A. Y. et al. (2020). Legal Approaches to Artificial Intelligence Concept and Essence Definition. *Revista San Gregorio*, 41, 115–121. <https://doi.org/10.36097/rsan.v1i41.1489>
- Channov, S. E. (2022). Robot (artificial intelligence system) as a subject (quasi-subject) of law. *Actual Problems of Russian Law*, 12, 94–109. <https://doi.org/10.17803/1994-1471.2022.145.12.094-109>
- Duffy, S. H., & Hopkins, J. P. (2013). Sit, Stay, Drive: The Future of Autonomous Car Liability. *SMU Science & Technology Law Review*, 16.
- Durneva, P. N. (2019). Artificial intelligence: an analysis from the standpoint of the classical legal capacity theory. *Grazhdanskoe Pravo*, 5, 30–35. <https://doi.org/10.18572/2070-2140-2019-5-30-33>
- Ivliev, G. P., & Egorova, M. A. (2022). Legal issues of the legal status of artificial intelligence and products created by artificial intelligence systems. *Zhurnal Rossiyskogo Prava*, 6, 32–46. <https://doi.org/10.12737/jrl.2022.060>
- Izhaev, O. A., & Kuteynikov, D. L. (2024). Artificial intelligence systems and non-contractual civil liability: a risk-based approach. *Lex russica*, 77(6), 23–34. <https://doi.org/10.17803/1729-5920.2024.211.6.023-034>
- Kharitonova, Yu. S., Savina, V. S., & Pagnini, F. (2022). Civil liability in the development and application of artificial intelligence and robotic systems: basic approaches. *Vestnik Permskogo Universiteta. Yuridicheskie Nauki*, 58, 683–708. <https://doi.org/10.17072/1995-4190-2021-58-683-708>
- Kovler, A. I. (2022). Anthropology of human rights in the digital age (experience of comparative legal method). *Zhurnal Rossiyskogo Prava*, 12, 5–29. <https://doi.org/10.12737/jrl.2022.125>
- Laptev, V. A. (2019). Artificial intelligence and liability for its work. *Law. Journal of the Higher School of Economics*, 2, 79–102. <https://doi.org/10.17-323/2072-8166.2019.2.79.102>
- Leenes, R., & Lucivero, F. (2014). Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design. *Law, Innovation and Technology*, 6(2), 194–222.
- Llorca, D. F. (2023). Liability Regimes in the Age of AI: a Use-Case Driven Analysis of the Burden of Proof. *Journal of Artificial Intelligence Research*, 76, 613–644. <https://doi.org/10.48550/arXiv.2211.01817>
- Philipp, H. (2023). The European AI liability directives – Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, 51, 1–42. <https://doi.org/10.1016/j.clsr.2023.105871>

- Pibaev, I. A., & Simonova, S. V. (2020). Algorithms in the mechanism of implementation of constitutional rights and freedoms: challenges in the digital age. *Sravnitelnoye Konstitutsionnoye Obozreniye*, 6, 31–50. <https://doi.org/10.21128/1812-7126-2020-6-31-50>
- Shakhnazarov, B. A. (2022). Legal regulation of relations using artificial intelligence. *Actualniye Problemy Rossiyskogo Prava*, 9, 63–72. <https://doi.org/10.17803/1994-1471.2022.142.9.063-072>
- Tianran, L. (2024). Research on Legal Responsibility Attribution for Autonomous Systems: An AI Governance Perspective. *Science of Law Journal*, 3(7), 166–174. <https://doi.org/10.23977/law.2024.030722>

Author information



Dmitriy A. Kazantsev – Cand. Sci. (Law), member of the Council for developing purchases, Chamber of Commerce and Industry of the Russian Federation, Moscow, Russia

Address: 6/1c1 Ilyinka Str., 109012, Moscow, Russia

E-mail: info@dkazantsev.ru

ORCID ID: <https://orcid.org/0000-0003-2182-5776>

RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1149755

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – May 22, 2025

Date of approval – June 4, 2025

Date of acceptance – September 25, 2025

Date of online placement – September 30, 2025



Научная статья

УДК 34:004:346.6:004.8

EDN: <https://elibrary.ru/ruzmxxp>

DOI: <https://doi.org/10.21202/jdtl.2025.18>

Правовые механизмы распределения ответственности за вред, причиненный системами искусственного интеллекта

Дмитрий Александрович Казанцев

Торгово-промышленная палата Российской Федерации, Москва, Россия

Ключевые слова

автономность,
деликтоспособность,
законодательство,
искусственный интеллект,
нейронная сеть,
право,
рискориентированный
подход,
робот,
цифровые технологии,
юридическая
ответственность

Аннотация

Цель: формулировка предложений по формированию системы субсидиарной ответственности субъектов за вред, ставший результатом использования систем искусственного интеллекта.

Методы: исследование базируется на комплексной методологической основе, включающей применение абстрактно-логического метода для теоретического осмысления правовой природы искусственного интеллекта как объекта правового регулирования, метода сравнения для анализа подходов российского и европейского законодательства к регулированию деликтной ответственности, методов обобщения для систематизации существующих концепций распределения ответственности между субъектами права, а также корреляционного анализа для выявления взаимосвязей между типологией систем искусственного интеллекта и механизмами правовой ответственности за их функционирование.

Результаты: в ходе исследования обобщены и систематизированы современные теоретико-правовые представления и нормативные акты Европейского союза и Российской Федерации о вариантах распределения субсидиарной ответственности за неблагоприятные последствия работы искусственного интеллекта. Определены потенциальные субъекты ответственности и выявлены ключевые факторы, влияющие на распределение ответственности между ними. Разработана многомерная матрица распределения ответственности между субъектами, учитывающая влияние каждого из них на работу конкретной системы искусственного интеллекта и типологизацию самих систем с точки зрения рискориентированного подхода.

Научная новизна: в работе впервые предложена авторская концепция, сочетающая дифференциацию ролей субъектов с точки зрения их реального влияния на результаты работы искусственного интеллекта, дифференциацию самих систем искусственного интеллекта согласно

© Казанцев Д. А., 2025

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

рискоориентированному подходу и соответствующую двум указанным классификациям систему правовых презумпций распределения ответственности. Новизна заключается в создании многомерной матрицы субсидиарной ответственности, которая позволяет учитывать множество факторов при определении субъекта ответственности в каждом конкретном случае причинения вреда системами искусственного интеллекта, что существенно отличается от существующих односторонних подходов к данной проблематике.

Практическая значимость: выводы и предложения исследования могут быть использованы для развития доктрины субсидиарной ответственности в области использования искусственного интеллекта, разработки и модификации норм права, посвященных регулированию искусственного интеллекта. Предложенная многомерная матрица распределения ответственности может служить теоретическим основанием для совершенствования судебной практики по делам о возмещении вреда, причиненного системами искусственного интеллекта, а также для создания эффективного баланса между стимулированием развития ИИ-технологий и обеспечением защиты прав и законных интересов физических и юридических лиц.

Для цитирования

Казанцев, Д. А. (2025). Правовые механизмы распределения ответственности за вред, причиненный системами искусственного интеллекта. *Journal of Digital Technologies and Law*, 3(3), 446–471. <https://doi.org/10.21202/jdtl.2025.18>

Список литературы

- Андреев, В. К. (2021). Приобретение и осуществление прав юридического лица с использованием искусственного интеллекта. *Предпринимательское право*, 4, 11–17. EDN: <https://elibrary.ru/nnesjs>. DOI: <https://doi.org/10.18572/1999-4788-2021-4-11-17>
- Антонов, А. А. (2020). Искусственный интеллект как источник повышенной опасности. *Юрист*, 7, 69–74. EDN: <https://elibrary.ru/dwhttx>. DOI: <https://doi.org/10.18572/1812-3929-2020-7-69-74>
- Афанасьев, С. Ф. (2022). К проблеме материальной и процессуальной правосубъектности искусственного интеллекта. *Вестник гражданского процесса*, 3, 12–31. EDN: <https://elibrary.ru/fjaogm>. DOI: <https://doi.org/10.24031/2226-0781-2022-12-3-12-31>
- Дурнева, П. Н. (2019). Искусственный интеллект: анализ с точки зрения классической теории правосубъектности. *Гражданское право*, 5, 30–35. EDN: <https://elibrary.ru/nckitd>. DOI: <https://doi.org/10.18572/2070-2140-2019-5-30-33>
- Ивлиев, Г. П., Егорова, М. А. (2022). Юридическая проблематика правового статуса искусственного интеллекта и продуктов, созданных системами искусственного интеллекта. *Журнал российского права*, 6, 32–46. EDN: <https://elibrary.ru/anagtu>. DOI: <https://doi.org/10.12737/jrl.2022.060>
- Ижаев, О. А., Кутейников, Д. Л. (2024). Системы искусственного интеллекта и внедоговорная гражданско-правовая ответственность: риск-ориентированный подход. *Lex russica*, 77(6), 23–34. EDN: <https://elibrary.ru/xvabso>. DOI: <https://doi.org/10.17803/1729-5920.2024.211.6.023-034>
- Ковлер, А. И. (2022). Антропология прав человека в цифровую эпоху (опыт сравнительного анализа). *Журнал российского права*, 12, 5–29. EDN: <https://elibrary.ru/drklnh>. DOI: <https://doi.org/10.12737/jrl.2022.125>
- Лаптев, В. А. (2019). Понятие искусственного интеллекта и юридическая ответственность за его работу. *Право. Журнал Высшей школы экономики*, 2, 79–102. EDN: <https://elibrary.ru/gqatho>. DOI: <https://doi.org/10.17-323/2072-8166.2019.2.79.102>
- Пибаев, И. А., Симонова, С. В. (2020). Алгоритмы в механизме реализации конституционных прав и свобод: вызовы цифровой эпохи. *Сравнительное конституционное обозрение*, 6, 31–50. EDN: <https://elibrary.ru/zmmnic>. DOI: <https://doi.org/10.21128/1812-7126-2020-6-31-50>

- Харитонов, Ю. С., Савина, В. С., Паньини, Ф. (2022). Гражданско-правовая ответственность при разработке и применении систем искусственного интеллекта и робототехники: основные подходы. *Вестник Пермского университета. Юридические науки*, 58, 683–708. EDN: <https://elibrary.ru/ppvmzr>. DOI: <https://doi.org/10.17072/1995-4190-2021-58-683-708>
- Чаннов, С. Е. (2022). Робот (система искусственного интеллекта) как субъект (квазисубъект) права. *Актуальные проблемы российского права*, 12, 94–109. EDN: <https://elibrary.ru/memsif>. DOI: <https://doi.org/10.17803/1994-1471.2022.145.12.094-109>
- Шахназаров, Б. А. (2022). Правовое регулирование отношений с использованием искусственного интеллекта. *Актуальные проблемы российского права*, 9, 63–72. EDN: <https://elibrary.ru/yownjo>. DOI: <https://doi.org/10.17803/1994-1471.2022.142.9.063-072>
- Bertolini, A. (2013). Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules. *Law, Innovation and Technology*, 5. <https://doi.org/10.5235/17579961.5.2.214>
- Vokovnya, A. Y. et al. (2020). Legal Approaches to Artificial Intelligence Concept and Essence Definition. *Revista San Gregorio*, 41, 115–121. <https://doi.org/10.36097/rsan.v1i41.1489>
- Duffy, S. H., & Hopkins, J. P. (2013). Sit, Stay, Drive: The Future of Autonomous Car Liability. *SMU Science & Technology Law Review*, 16.
- Leenes, R., & Lucivero, F. (2014). Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design. *Law, Innovation and Technology*, 6(2), 194–222.
- Llorca, D. F. (2023). Liability Regimes in the Age of AI: a Use-Case Driven Analysis of the Burden of Proof. *Journal of Artificial Intelligence Research*, 76, 613–644. <https://doi.org/10.48550/arXiv.2211.01817>
- Philipp, H. (2023). The European AI liability directives – Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, 51, 1–42. <https://doi.org/10.1016/j.clsr.2023.105871>
- Tianran, L. (2024). Research on Legal Responsibility Attribution for Autonomous Systems: An AI Governance Perspective. *Science of Law Journal*, 3(7), 166–174. <https://doi.org/10.23977/law.2024.030722>

Сведения об авторе



Казанцев Дмитрий Александрович – кандидат юридических наук, член Совета по развитию закупок, Торгово-промышленная палата Российской Федерации
Адрес: 109012, Россия, г. Москва, ул. Ильинка, 6/1с1
E-mail: info@dkazantsev.ru
ORCID ID: <https://orcid.org/0000-0003-2182-5776>
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1149755

Конфликт интересов

Автор сообщает 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: 10.19.31 / Право на информацию

Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 22 мая 2025 г.

Дата одобрения после рецензирования – 4 июня 2025 г.

Дата принятия к опубликованию – 25 сентября 2025 г.

Дата онлайн-размещения – 30 сентября 2025 г.