ARTICLE

Responsibility in the Field of Artificial Intelligence Systems Usage: Features of Private and Public Law Regulation

Ilya R. Khmelevskoi,

University of Tyumen (Tyumen, Russian Federation)

https://orcid.org/0009-0007-2787-1358

Nikita A. Kalashnikov,

University of Tyumen (Tyumen, Russian Federation)

https://orcid.org/0009-0006-6657-7939

https://doi.org/10.21684/2412-2343-2025-12-4-147-166

Received: September 9, 2024
Reviewed: December 12, 2024
Accepted: September 7, 2025

Abstract. The article examines the approaches and specifics of legal responsibility in the context of artificial intelligence (AI) systems, focusing particularly on private and public law. The study aims to analyze current legal mechanisms for responsible use of AI systems, with a particular emphasis on BRICS and the European Union jurisdictions, in order to identify effective regulatory approaches for AI activities. The paper also discusses ethical and 'soft' regulatory mechanisms for AI applications. Special attention is given to international recommendations on AI governance and harmonization of transparency and accountability standards on a global scale. The authors highlight the significant initiatives of private law, driven by the active integration of AI into private economic sectors, as well as the flexibility of companies in developing internal standards and ethical codes. In conclusion, the article emphasizes the need for integrating private and public responsibility mechanisms, and harmonizing international standards to ensure the effective protection of citizens' rights while fostering innovation.

Keywords: responsibility; artificial intelligence; liability; private law; public law; ethics; BRICS; European Union.

To cite: Khmelevskoi, I. R., & Kalashnikov, N. A. (2025). Responsibility in the field of artificial intelligence systems usage: Features of private and public law regulation. *BRICS Law Journal*, *12*(4), 147–166.

Table of Contents

Introduction

In rapid digital transformation, artificial intelligence systems are being integrated into all areas of human life, from production processes to healthcare and jurisprudence. While technological advancements bring significant benefits, they also give rise to a complex array of fundamental challenges, ethical considerations, demands for transparency, and issues related to the accountability of AI systems, among others.

Issues concerning the legal personality of artificial intelligence, the regulation of its development processes, the systematization of potential risks, and the determination of responsibility for negative consequences arising from AI activities have become particularly pressing.[1] In the context of increasing autonomy and algorithmic complexity of artificial intelligence systems, legal mechanisms for accountability are facing new challenges that necessitate the adaptation and rethinking of current

[1] Mocanu, D. M. (2022). Gradient legal personhood for AI systems–Painting continental legal shapes made to fit analytical molds. *Frontiers in Robotics and AI*, *8*, 1–11.

legislative frameworks. This situation raises important questions regarding the methods of regulation of AI.[2]

The use of AI technologies not only holds great promise for progressive development but also creates conditions for unlawful acts and offences, underscoring the urgent need for a regulatory framework and accountability mechanisms. The timeliness and appropriateness of the regulatory provisions will determine not only the effectiveness of AI integration into various spheres of social life but also ensure the fundamental rights and freedoms.

Analysis of the BRICS countries' legal systems reveals a variety of approaches to regulating accountability in artificial intelligence. The Brazilian regulatory framework emphasizes the protection of personal data; however, this approach does not provide comprehensive regulation for the operation of AI systems.[3] The implementation of preventive measures and technical audits could substantially improve the existing regulatory mechanisms.[4]

The Russian Federation has initiated a regulatory legal framework for artificial intelligence through the adoption of the National Strategy for the Development of Artificial Intelligence and the Implementation of Experimental Legal Regimes. The Federal Law "On Experimental Legal Regimes in the Field of Digital Innovations"[5] lays the groundwork for testing various regulatory approaches. The proposed multilevel responsibility system is seamlessly integrated into the existing concept and can be implemented within experimental legal regimes. For a long time, China's legal framework in the field of AI was characterized by a lack of overarching control and oversight mechanisms. Legislators primarily focused on refining and updating key Chinese data protection laws, including the Personal Information Protection Law of 2021 and the Data Security Law of 2021, which complements the Cybersecurity Law of 2016.[6]

The South African Republic, despite the absence of specialized AI legislation, demonstrates active lawmaking efforts in this area. The current Protection of Personal

---

[2] *See* Kuteinikov, D. L., Izhaev, O. A., Zenin, S. S., & Lebedev, V. A. (2022). *Artificial intelligence and law: From fundamental problems to applied tasks: Monograph*. Tyumen State University. (In Russian).

[3] Weston, F. C. L., Paglioli, A. C. B., & Weston, M. W. (2023). Lei Geral de Proteção de Dados Pessoais e aplicabilidade para a Enfermagem. *Revista Brasileira de Enfermagem*, *76*(Suppl. 3), e20230126. https://doi.org/10.1590/0034-7167-2023-0126pt. (In Portuguese).

[4] Woolcott Oyague, O., Monje Mayorca, D. F., Comandé, G., Peláez Hernández, R. A., & Morales Hervias, R. (2019). *The modernization of civil law institutions: Civil liability, property and contract*. Universidad Católica de Colombia.

[5] Federal Law No. 258-FZ of July 31, 2020 "On Experimental Legal Regimes in the Field of Digital Innovation in the Russian Federation." SPS "ConsultantPlus." https://www.consultant.ru/document/cons_doc_LAW_358738/. (In Russian).

[6] Sakharov, A. G., & Shelepov, A. V. (2024). China's digital platforms regulation policy. *International Organisations Research Journal*, *19*(2), 145–160. (In Russian).

Information Act regulates only certain aspects of AI technology applications. The proposed accountability mechanism could serve as a foundation for developing a comprehensive approach to regulation within the South African legal system.[7]

A comparative analysis of AI regulatory mechanisms in certain BRICS jurisdictions reveals that the proposed liability system correlates with the main legislative trends. However, more advanced research is required on issues concerning causality and responsibility, which are particularly relevant for the evolving legal systems of BRICS nations.

1. Ethical Mechanisms in Regulation of Artificial Intelligence System Applications

Within the system of regulatory mechanisms, a special place is given to ethical and observational instruments classified as "soft law." These mechanisms, while not providing for sanctions in case of non-compliance with established recommendations, are becoming increasingly prevalent at various levels ranging from state structures to private entities.

Ethical codes and principles governing AI systems being an essential component of anthropocentric technological development, nevertheless exhibit certain inefficiencies. Established ethical constraints can be circumvented through technical modifications, additional training of systems, or manipulative methods of interaction with AI, as vividly demonstrated by the operation of modern AI assistants such as ChatGPT.

In the context of regulating artificial intelligence, ethical codes and rules are developed with the aim of forming a comprehensive system of standards designed to prevent discrimination, ensure transparency, and hold AI systems accountable. These regulatory tools, created by professional associations, technology corporations, and international organizations,[8] establish principles and guidelines for subjects involved in the development of artificial intelligence systems. However, the discretionary nature of most ethical codes, coupled with the lack of enforcement mechanisms and sanctions for their non-compliance, significantly undermines their effectiveness.

To optimize the system of responsibility regulation of AI, it seems expedient to integrate ethical and legal mechanisms. Ethical codes can serve as a conceptual basis for the formation of legal norms that provide more effective control and legal

---

[7] Staunton, C., Adams, R., Anderson, D., Croxton, T., Kamuya, D., Munene, M., & Swanepoel, C. (2020). Protection of Personal Information Act 2013 and data protection for health research in South Africa. *International Data Privacy Law*, *10*(2), 160–179.

[8] European Commission. (2019). *Ethics guidelines for trustworthy AI*. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai; Institute of Electrical and Electronics Engineers. (2017). IEEE standard review–Ethically aligned design: A vision for prioritizing human wellbeing with artificial intelligence and autonomous systems. https://ieeexplore.ieee.org/document/8058187

accountability. Such a synthesis will enable overcoming existing limitations and creating a balanced regulatory system that takes into account both public interests and the technological capabilities of developers and operators of AI.

The establishment of legal mechanisms for imposing responsibility on parties violating ethical norms in the realm of AI facilitates a more prompt and effective response to emerging challenges. Given the cross-border nature of AI technologies, the development of international cooperation and harmonization of ethical and legal norms on a global scale becomes particularly relevant. The unification of regulatory approaches will help minimize legal conflicts and create optimal conditions for the development of AI systems, avoiding both excessive restrictions and ineffective regulatory mechanisms.

In the context of regulating artificial intelligence, preventive and 'soft' respon-sibility mechanisms demonstrate some significance, yet their effectiveness is substantially limited by several factors: the voluntary nature of implementation, the potential possibility of circumventing established rules, insufficient specificity of formulations, and the absence of an interdisciplinary approach. To overcome these limitations, it is necessary to develop mandatory standards and monitoring mechanisms.

Legal regulation of AI in China is currently undergoing active legislative exploration and the search for optimal legal solutions amidst the multi-faceted structure and accelerated pace of economic development.

An example of this effort is the development and adoption of the "Code of Ethics for Next Generation Artificial Intelligence," aimed at implementing and specifying the institution of AI responsibility. This code was approved and adopted by the National Professional Committee for Artificial Intelligence Management in the fall of 2021.[9]

The Code of Ethics for Next Generation Artificial Intelligence sets forth both fundamental ethical requirements and specific requirements for particular activities involving AI technologies. The provisions of the Code address various aspects of interactions between individuals and legal entities with AI technologies and their management during operational activities.

The Code includes the following ethical requirements for the use of AI:

1) The use of AI should improve human well-being;

2) Individuals and organizations using AI must adhere to the principles of universality and inclusivity;

3) The functioning of AI must not violate the legitimate rights and interests of all participants in legal relations, ensuring and protecting all aspects of citizens' privacy;

4) AI technologies must be manageable;

5) Responsibility for those using AI technologies should be significantly tightened;

6) Enhancing the ethical literacy of subjects who employ AI technologies in their activities.

---

[9] Filippova, I. A. (2024). Legal regulation of artificial intelligence: Experience of China. *Journal of Digital Technologies and Law*, *2*(1), 46–73. (In Russian).

Despite the increasing prevalence of ethical and soft-law mechanisms for regulating artificial intelligence, their effectiveness remains constrained due to the absence of enforceable sanctions and the potential to circumvent established norms. To ensure more robust and comprehensive oversight of AI technology development, it is imperative to integrate ethical codes with legal mechanisms of accountability. Such integration would strengthen adherence to ethical standards, enhance the accountability of AI developers and operators, and establish a resilient legal framework for preventing discrimination and ensuring transparency.

2. Public Regulation of Responsibility for the Use of Artificial Intelligence

The complexity of contemporary algorithms, along with their ability to self-learn and autonomously make decisions, poses significant risks to the rights and interests of citizens, organizations, and society as a whole.

The lack of clear standards set at the international level and uniform approaches to regulating responsibility for actions taken by AI systems leads to legal uncertainty. The fragmentation of national regulations and differences in the legal systems of various countries complicate the cross-border use of AI technologies. In such circumstances, studying best practices in legal regulation of responsibility within the AI domain becomes especially pertinent.

The global nature of AI development and associated risks necessitates the formulation of harmonized approaches to the issue of regulating responsibility for AI actions. It is crucial to strike a balance between fostering innovation and safeguarding citizens' rights, as well as between the interests of AI system developers and public safety. Analyzing current regulatory practices helps identify existing trends and mechanisms to achieve this balance and determine promising directions for further legal regulation in this area.

2.1. U.N. Approaches to Regulation of Responsible Use of AI

In December 2023, the U.N. High-Level Advisory Body on AI published its interim report titled "Governing AI for Humanity."[10] It presents comprehensive recommendations for establishing a global AI governance system, emphasizing the need for international cooperation, transparency, and accountability in managing artificial intelligence.

According to the report, one of the primary challenges lies in ensuring mechanisms of accountability and responsibility in areas where AI is already actively employed. Several substantial obstacles to determining responsibility for AI actions are highlighted:

---

[10] *See* United Nations. (2023). *Interim report: Governing AI for humanity*. https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_governing_ai_for_humanity_interim_report.pdf

- lack of transparency in AI operations due to technological complexity;
- constraints related to trade secrets;
- insufficient access to computational resources;
- uncertainty regarding the legal status of AI;
- absence of a unified legal approach.

To address these issues, it is recommended to establish transparency standards and ensure access to data and AI models. Currently, many countries (including Russia, China, and the United States) are developing national documents on AI regulation. However, existing AI regulation remains fragmented and primarily focused on the private sector. The growing influence of AI requires the establishment of clear frameworks of responsibility for organizations that create, implement, and monitor AI systems. Furthermore, it is necessary to:

- prioritize public interests over private ones;
- establish mechanisms for compensating damages;
- develop procedures for dispute resolution.

Legal regulation should clearly differentiate between public and private liability. At the international level, primary responsibility for the functioning of AI should be assigned to international organizations and government bodies.

According to the final report "Governing Artificial Intelligence for Humanity"[11] published by the UN High-Level Advisory Body on AI in September 2024, the inherent complexity of modern AI systems renders it impossible to exercise complete control over their outcomes or predict developmental trajectories, both for developers and users.

Given the conclusion presented in the final report of the U.N. High-Level Advisory Body on Artificial Intelligence, ensuring transparency and interpretability of AI functioning becomes paramount. It is essential to establish a transparent system that allows tracing causality back to a specific legal entity that will bear responsibility in cases where AI causes harm through its actions.

It is important to note that contemporary AI models do not possess sufficient characteristics to qualify them as independent legal subjects in the traditional sense.[12]

In this regard, it appears prudent to intensify the development of the following aspects:

1. Transparency of AI systems, defined as the availability of information to interested parties about decision-making processes, datasets used, and algorithmic models applied.[13]

---

[11] *See* United Nations. (2024). *Governing artificial intelligence for humanity: Final report*. https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_ru.pdf. (In Russian).

[12] Drozdov, V. Y. (2024). Limits of criminal liability for the use of artificial intelligence. *Legal Science*, *9*, 207–210. (In Russian).

[13] Kaminski, M. E. (2019). The right to explanation, explained. *Berkeley Technology Law Journal*, *34*(1), 189–218.

2. Interpretability, which means the presence of verifiable mechanisms to explain the causal reasoning behind specific decisions made by AI systems.[14]

The regulatory framework should include requirements for mandatory transparency of key parameters of AI algorithms, including the models used, operating principles, and decision-making criteria.

2.2. Legal Liability in the Field of AI: Regulatory Practice of the European Union

An interesting case is he experience of the European Union, where the most advanced system of public-law regulation of responsibility in the use of AI has been established. The EU Regulation on Artificial Intelligence (AI Act 2024/1689)[15] (hereinafter referred to as the EU Regulation), which came into force in August 2024, establishes a comprehensive set of norms governing the development, market introduction, and operation of AI systems. A critical aspect of this act is the definition of responsibility for the actions of artificial intelligence systems. The EU Regulation imposes specific obligations on various stakeholders, including AI providers, users, importers, and distributors, ensuring accountability throughout the entire life cycle of the artificial intelligence system. Interpretation of the provisions of this act should be carried out in conjunction with the General Data Protection Regulation (GDPR) 2016/679;[16] Product Liability Directive 85/374/EEC;[17] and the General Product Safety Regulation 2023/988/EU.[18]

One of the key features of this regulation is the introduction of a risk-based classification system for AI systems. This not only enables the systematic categorization of different types of AI applications but also allows for the establishment of differentiated requirements based on the potential hazards they may pose.

---

[14] Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. *Fordham Law Review*, *87*, 1085–1139.

[15] *See* Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[16] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[17] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

[18] *See* Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC. https://eur-lex.europa.eu/eli/reg/2023/988/oj

Under the current EU Regulation, a four-tier classification of AI systems has been established, encompassing prohibited systems, high-risk systems, low-risk systems, and general-purpose systems with potential systemic risk.[19]

In the legal framework governing responsibility, emphasis is placed on AI systems classified as either prohibited or high-risk. Despite their potential societal benefits, these systems pose significant risks of infringement upon the rights and freedoms of citizens.

If AI systems manipulate people's decisions or exploit their vulnerabilities, evaluate or classify people based on their social behavior or personal qualities, predict the risk of criminal activity for an individual, extract facial images from the internet or surveillance camera recordings, draw conclusions about emotions in workplaces or educational institutions, or classify people based on biometric data, then entities placing, deploying, or using such AI systems are subject to liability (Art. 5). In the event that any harm is caused to third parties by high-risk AI systems as a result of experiments conducted in controlled digital and physical environments, suppliers, including potential ones, are held administratively liable if they fail to comply with experimentation guidelines and supervision rules stipulated in EU laws and national acts (para. 12, Art. 57).

Thus, the contemporary system of legal regulation concerning responsibility for the functioning of AI systems in the European Union represents a comprehensive mechanism aimed at ensuring safety, transparency, and ethical application of artificial intelligence technologies. The implementation of a risk-based approach and a multi-level AI classification system based on potential hazard provides a toolkit for protecting citizens' rights and ensuring their safety amid the advancement of artificial intelligence technologies.

3. Liability for AI Use in Private Law

3.1. Private Law specifics for Liability Implementation in the Field of AI

When discussing civil law methods of regulating responsibility, it is crucial to emphasize that they play a foundational role in maintaining order and protecting the rights and legitimate interests of all participants in civil legal relationships.[20]

The adaptation of civil liability mechanisms to address the challenges presented by the advancement of artificial intelligence systems is of paramount significance.[21]

---

[19] Söderlund, K., & Larsson, S. (2024). Enforcement design patterns in EU law: An analysis of the AI act. *Digital Society*, *3*, 1–21.

[20] Hussein S., & Towards M. F. (2023). Granting of legal personality to autonomous robots in the UAE. *International Journal of Innovation, Creativity and Change*, 17(2), 248–272.

[21] Eidenmueller, H. (2017). *The rise of robots and the law of humans* (Oxford Legal Studies Research Paper No. 27/2017). http://dx.doi.org/10.2139/ssrn.2941001

Legal relationships involving interaction with AI show a steady trend towards quantitative growth, while the existing mechanisms for regulating AI activities are characterized by inadequate effectiveness.

In the doctrine of civil law, liability is interpreted as a legal obligation of a subject to bear negative consequences resulting from the violation of civil norms or contractual obligations in favor of the injured party. This legal institution operates as a mechanism for restitution of violated rights, compensation for property losses, and ensuring stability in civil transactions.[22]

In the legal nature of civil liability, the pecuniary character of applied sanctions prevails, which are implemented through compensation for damages, recovery of penalties, or indemnification for harm caused. This feature is determined by the specifics of civil law as a regulator of property and personal non-property relations, where the principle of equivalent compensation plays a primary role.

Despite the predominantly discretionary nature of civil relationships, the implementation of civil liability is ensured by a mechanism of state coercion, which is manifested in the possibility of judicial enforcement when pre-trial dispute resolution procedures prove ineffective.

From a teleological perspective, this type of liability aims at providing financial compensation and creating incentives for good-faith conduct among participants in civil transactions. In several jurisdictions, including Russian and American ones, there is a convergence between private-law liability and public-law sanctions.[23]

In legal scholarship, there exist various approaches to defining the nature and grounds of such liability.[24] The fundamental basis for civil liability lies in an unlawful act, expressed either through action (breach of contract terms) or omission (delay in fulfilling an obligation). A crucial element is the presence of actual damage or harm. To qualify a civil wrong, it is necessary to establish causation and fault on the part of the offender, except in cases of strict liability, such as those involving the operation of inherently dangerous activities.[25]

The specificity of civil liability is evident across different types of legal relationships. In contractual relations, it arises from breaches of obligations stipulated in agreements between parties, whereas in tortious relations, it stems from causing non-contractual

---

22 Mozolin, V. P. (2012). Civil liability in the system of Russian law. *Journal of Russian Law*, *1*(181), 33–40.

23 Rostovtseva A. M. (2013). The relationship between civil liability of participants in corporate relations and administrative and criminal liability. *Society and Law*, *1*(43), 83–87. (In Russian).

24 Aleksikova, O. E., & Melnik, E. A. (2017). Problems of determining the legal nature of civil liability of a legal entity. *Bulletin of the Volga Region Institute of Management*, *17*(6), 60–66. (In Russian).

25 Kazakova, I. A., Kamalieva, L. A., & Sled, Y. G. (2020). On the specifics of bringing to justice the owners of sources of increased danger. *Law and State: Theory and Practice*, *3*(183), 36–39. (In Russian); Kovalenko, S. P. (2014). Legal nature of civil liability of participants in corporate relations. *Legal Concept*, *1*, 76–80. (In Russian).

harm. Special instances include liability for moral damage, for hazardous activities, and for actions taken by third parties within the context of agency relationships.[26]

The issue of civil liability for artificial intelligence systems is a subject of intense scholarly discourse within the global legal community. Doctrinal studies reveal a variety of approaches to regulating this area:

1. Strict Liability of Manufacturers: manufacturers bear primary responsibility for any losses caused by AI.[27]

2. Operator Liability: operators are responsible for controlling and supervising the actions of AI.[28]

3. Partial Legal Personhood: AI is recognized as a legal entity with limited liability, but primary responsibility remains with the owners.[29]

4. Mandatory Insurance: insurance funds compensate for damages if AI causes losses.

5. Registration of AI: registering AI owners and functions helps identify responsible parties.

A key challenge is to identify the correct subject of liability for the actions of AI systems. The existing regulatory tools demonstrate insufficient adaptability to the unique characteristics of AI as a legal object, marked by its autonomous functioning and capacity for self-learning.

In practice, a conceptual contradiction emerges between the traditional understanding of fault as a subjective ground for liability and the nature of AI, which lacks mental awareness of its actions.[30] Proposed solutions involve either excluding fault from the essential elements of liability (similar to inherently dangerous activities) or implementing objective criteria for evaluating actions.

Scholarly literature highlights the difficulty of establishing a causal link between the actions of an agent and ensuing adverse outcomes[31]. In the context of the autonomous functioning of AI systems, this issue becomes even more complex. The ability of artificial intelligence to make independent decisions and learn autonomously complicates the identification of a specific liable party among potential stakeholders: developers, operators, or owners. Traditional mechanisms for assigning liability, based on direct involvement in a wrongdoing, prove ineffective,

---

[26] Musalov, M. A., & Rashidov, Sh. M. (2023). Interrelated provisions of Articles 15 and 1064 of the Civil Code of the Russian Federation. *Law and State: Theory and Practice*, *3*(219), 172–174. (In Russian).

[27] Eidenmueller, 2017.

[28] Mocanu, 2022.

[29] *Id*.

[30] Liu, H., Maas, M., Danaher, J., Scarcella, L., Lexer, M., & Rompaey, L. (2020). Artificial intelligence and legal disruption: A new model for analysis. *Law, Innovation and Technology*, *12*(2), 205–258.

[31] Aleksikova & Melnik, 2017.

necessitating the development of innovative approaches to regulate the liability of AI systems.

In examining the issue of private-law liability for AI systems, the question of establishing a causal link between the functioning of AI and ensuing adverse outcomes takes on significant importance. The intricate decision-making processes of AI, relying on multifactorial analysis of large data sets, pose methodological challenges in identifying specific actions that led to the occurrence of harm. With the integration of AI into complex multi-component systems involving multiple actors (manufacturers, operators, owners), there is a risk of distributing responsibility.

The immanent characteristics of artificial intelligence, manifested in its ability to self-learn and autonomously make decisions that can be unpredictable even for the system's developers, give rise to significant legal uncertainties. In this context, it seems reasonable to establish a multi-level responsibility system that takes into account the specifics of AI and differentiates the roles of each subject in potential harm causation. The primary element of such a system is the basic responsibility of the developer, which encompasses fundamental aspects of system creation: algorithm architecture, principles of self-learning, implementation of necessary constraints, and security systems. It should be noted, however, that the developer's responsibility cannot extend to all possible consequences of the system's operation, especially those resulting from subsequent self-learning.

The next level of responsibility should be borne by operators and owners of AI systems. The grounds for liability here include improper use of AI, disregard for system warnings, misuse or failure to update safety measures as required. This approach fosters responsible usage of AI and ensures a balance of interests among all parties involved in legal relations.

Of particular methodological significance is the development of criteria for establishing a causal link between the functioning of AI and ensuing consequences. Key factors proposed for consideration include the predictability of outcomes and the degree of autonomy in decision-making. Predictability assessment involves analyzing the likelihood of a specific scenario unfolding, the presence of similar precedents in test data, and the potential predictability of the system's behavior. The degree of autonomy in decision-making is determined by the level of independence exhibited by the AI and the possibility of human intervention in the decision-making process.

This proposed mechanism of legal regulation aims at creating legal certainty regarding responsibility for actions taken by artificial intelligence, ensuring effective protection of the rights of affected subjects, and fostering favorable conditions for the industry's growth within the legal framework. At the same time, it is essential to consider the need for dynamic adaptation of this mechanism to keep pace with the advancing development of AI technologies.

The property-based nature of civil liability in the context of applying AI systems gives rise to a complex set of methodological issues related to determining the scope

of liability and quantifying compensation amounts, particularly in cases involving non-material damages such as breaches of data confidentiality. Additionally, the question of whether and how material responsibility could be directly attributed to an AI becomes highly relevant.

3.2. Private Law Development Trends in the context of AI

The first trend that can be mentioned involves implementing a mechanism of strict (no-fault) liability, akin to existing regulations governing liability for sources of increased danger. This approach entails holding the owner or operator of the AI liable regardless of any fault on their part.

The second trend, described in D. Mocanu's scholarly works,[32] involves introducing the concept of partial legal personality (*Teilrechtsfähigkeit*) for artificial intelligence, which would enable it to possess a limited set of rights and obligations, including the capacity to bear financial responsibility. Implementing this approach creates prerequisites for redistributing some of the responsibility onto the AI itself, specifically through the establishment of a specialized insurance fund.

The third trend pertains to the necessity of rethinking the categories of subjective elements (fault) and causality in relation to AI systems. Establishing cause-and-effect relationships must take into account the unique functional characteristics of AI, including its capability for self-learning. Consequently, there arises a pressing need to develop special standards and methods of proof based on in-depth analysis of algorithmic decisions and data sets.

Improving private law regulation of responsibility in the field of AI application requires a thorough examination and adaptation of the current legal tools to suit the specific features of AI technologies. Contemporary mechanisms of responsibility face numerous challenges stemming from the autonomy of these systems, the opacity of algorithmic decisions, and the multi-layered nature of responsibility. Effective legal regulation necessitates the formation of a specialized regulatory framework, the introduction of mandatory standards, the advancement of insurance and compensation mechanisms, and international harmonization of legislation.

The institution of civil liability must evolve, and this evolution should aim to strike an optimal balance between protecting the interests of injured parties and fostering innovative development.

The modern artificial intelligence is characterized by limited cognitive capabilities and relative autonomy, the concept of distributed responsibility among participants involved in the creation and operation of AI systems becomes paramount.[33] This approach entails differentiating responsibilities between manufacturers of

[32] Mocanu, 2022.

[33] Drozdov, 2024.

specialized equipment, software developers, and system operators based on their functional roles and degree of control over the system.[34]

Identifying the responsible party hinges on establishing a causal link between the culpable actions of a specific individual and the ensuing adverse consequences. Within this paradigm, the following categories of responsible entities are distinguished:[35]

1. The manufacturer bears responsibility when harm results from technical defects of a design or manufacturing nature. This category includes flaws in the physical architecture of the system, component failures, and other technical imperfections that led to the materialization of risk causing harm.

2. The software developer is held accountable if a causal connection is verified between the incurred damage and dysfunctions of an algorithmic nature. Grounds for liability in this case include programming errors, incorrect implementation of machine learning algorithms, deficiencies in security and control systems.

3. The system operator becomes the responsible entity in situations determined by human factors during the operation of the AI system. Such instances involve incorrect control inputs, violations of established protocols for using the system, ignoring requirements specified in technical documentation and operational guidelines.

4. Artificial Intelligence Systems Responsibility: Public Law Perspective

Regulating legal responsibility for AI-system actions has become increasingly urgent, requiring adaptation of both private law and public law regulatory mechanisms. However, there is a noticeable lag in public law regulation compared to private law initiatives.

Public sector regulation of AI lags behind private sector initiatives for several key reasons. Firstly, AI adoption is most active in private economic sectors. Private companies engaged in developing and deploying AI encounter urgent legal and ethical questions that demand prompt responses and tailored approaches.

Secondly, the private-law sphere demonstrates greater flexibility and speed in adapting to rapidly changing technological realities. Companies actively develop internal standards, ethical codes, and self-regulatory mechanisms, enabling them to quickly implement innovations while managing risks associated with AI use. This

---

[34] Gorokhova, S. S. (2021). On some aspects of public legal liability in the field of using artificial intelligence and autonomous robots. *Legal Research*, *5*, 24–41. (In Russian); Pomeranets, A. D., & Kolentsova, V. V. (2022). Criminal liability and artificial intelligence. *Law and State: Theory and Practice*, *2*(206), 273–278. (In Russian).

[35] Zhaglina, M. E., & Zhaglin, A. V. (2022). Liability for harm caused by artificial intelligence: reality and prospects. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, *2*, 75–78. (In Russian).

process fosters best practices that government structures can later adopt to establish broader public norms.

Moreover, governmental bodies traditionally have a slower legislative response due to the need to consider a wide range of interests and conduct lengthy coordination procedures. Nonetheless, there is a growing trend toward heightened state attention to AI regulation, driven by active discussions at the international level and examples of successful private sector initiatives. States are beginning to adopt and adapt best practices from the private sector, integrating them into their regulatory frameworks to create a more coherent and effective system of public law regulation for AI.[36]

The effectiveness of the public law regulatory system concerning responsibility for AI actions largely depends on clearly defining procedures for establishing cause-and-effect links between AI system actions and ensuing consequences, as well as having mechanisms to determine the extent of damage caused and the order of its compensation.

In today's technological landscape, identifying the subject of criminal and administrative liability for unlawful acts committed with the involvement or through AI systems becomes particularly crucial. Fundamental to resolving this issue is understanding the technological essence of modern AI systems, which currently lack autonomous consciousness and legally significant capacity for independent decision-making,[37] significantly influencing the construction of appropriate models of legal responsibility.

In the contemporary doctrine of criminal and administrative law, the prevailing conceptual approach suggests assigning responsibility to individuals who exercise control over AI systems' operations.[38] These subjects may include developers of AI system software, operators performing direct management, as well as owners and users who hold rights to utilize such systems. This concept aligns systematically with foundational principles of criminal law, emphasizing the necessity of personalizing responsibility for the outcomes of technological activities.

The theoretical-methodological basis for the approach under consideration rests upon the feasibility of verifying the cause-and-effect relationship between the actions of controlling subjects and the ensuing adverse consequences, as well as the potential to establish forms of guilt in the actions of these individuals. This paradigm allows for the effective implementation of existing legal mechanisms for holding individuals accountable within the context of utilizing modern AI technologies,

---

[36] *See* Kuteinikov et al., 2022.

[37] Ponkin, I. V., & Redkina, A. I. (2018). Artificial intelligence from the point of view of law. *Bulletin of the Peoples' Friendship University of Russia. Series: Legal Sciences*, *1*, 91–109. (In Russian).

[38] Mosechkin, I. N. (2019) Artificial intelligence and criminal liability: Problems of becoming a new type of crime subject. *Bulletin of St. Petersburg State University. Series 14. Law*, *3*, 461–476. (In Russian).

thereby ensuring adherence to fundamental legal principles while accounting for the technological specificity of the systems in question. Public law regulation in this area is characterized by the absence of specific provisions addressing responsibility for AI actions. An analysis of Chinese legislation indicates that offenders will be prosecuted under general laws of the People's Republic of China without considering the specificities of AI as a tool for committing offenses.

Within the practical realization of this concept, considerable importance lies in developing a methodological toolkit for establishing and proving cause-and-effect relationships between the actions of controlling subjects and ensuing consequences, as well as determining forms of guilt while taking into account the specifics of AI system functionality. This necessitates the advancement of corresponding mechanisms for technical monitoring, documentation, and expert analysis of AI systems' operations.

This approach was codified in the Measures for Managing Generative Artificial Intelligence Services of the People's Republic of China,[39] which came into effect on August 5, 2023. The Interim Provisions place legal responsibility for AI actions primarily on the service provider (provider) of AI (a natural person or legal entity). According to Article 9, the provider is responsible for the content generated by AI, promptly removing any portion that violates Chinese law. Furthermore, the provider is obligated to report each such instance to competent law enforcement authorities.

It is important to note that China places responsibility in the field of AI technology predominantly on developers and platform holders, as well as on users as auxiliary participants, allowing for the identification and exposure of illegal actions involving AI. Now, AI does not function as an independent quasi-subject in private and public legal relations. Issues concerning user and developer responsibility for AI and robots closely intertwine with ethical norms and maintain a human-centric character. Thus, China's legal foundation regarding AI responsibility often serves as a guideline, laying the foundation for further specification in targeted regulatory acts. There is no unified system of sanctions for AI-related offenses; punishment is regulated by principles of general criminal and administrative law.

One distinctive feature of public law regulation of artificial intelligence in China is the absence of private-law liability. This means that within such regulatory approaches, mechanisms of civil liability are not applied to subjects for violations of established norms and standards for using AI technologies. Instead, the focus is on state supervision and control, as well as the development of general rules and standards regulating the operation and application of AI systems, along with the application of administrative and criminal sanctions. For example, Article 7 of the Interim Provisions limits the data used by AI in generating content to only data

[39] *See* Measures for managing generative artificial intelligence services (2023). China Cyberspace Administration. https://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm. (In Chinese).

obtained legally and on legitimate grounds. The final generative product must not infringe on the intellectual property rights of third parties, although the question remains open as to how and by whom the legality of information sources used by AI will be determined and what criteria this information must meet. The Interim Provisions prohibit companies from collecting user personal data beyond what is necessary and storing data entered by the user that could identify them or provide such information to third parties.

The final version of the Measures for managing generative artificial intelligence services of the People's Republic of China does not specify clear-cut sanctions imposed on violators of this act when using AI technologies but retains the option to apply general rules for imposing administrative and criminal penalties for offenses related to the operation of generative AI. Civil liability measures, however, are not provided for in the Interim Provisions.

A second distinct feature of public law regulation of artificial intelligence lies in the use of labeling AI-generated content as an important control mechanism. Labeling provides a means to ensure transparency and accountability in the use of AI technologies, distinguishing content created by artificial intelligence from that produced by humans. Regarding the labeling of AI-generated content, the aforementioned Interim Provisions refer to the "Provisions on the Administration of Deep Synthesis Internet Information Services,"[40] which envisages such labeling for providers of information services. In 2024, the Cyberspace Administration of China introduced a document titled "Measures for Identifying AI-Generated Synthetic Content,"[41] which outlines types of labels, requirements for AI-powered chatbots, and requirements for digital platform holders. The document identifies two categories of labeling: explicit (logo, graphic, sound, text) and implicit (metadata and other technical marking means hidden from the user's view). Implicit labeling will be mandatory for all deep synthesis service providers.[42] Thus, the People's Republic of China demonstrates a policy aimed at unifying regulatory acts governing the use of generative artificial intelligence by both individuals and legal entities. Overall, the interim measures adopted in China to regulate generative AI represent a significant step towards creating a comprehensive system for controlling the use of AI technologies. Integrating state oversight mechanisms, mandatory content labeling, and administrative and criminal sanctions helps establish a robust legal framework that balances innovation with the protection of public interests.

---

[40] Regulation on the in-depth management of the synthesis of Internet information services (2022). China Cyberspace Administration. https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm. (In Chinese).

[41] China Daily. (2024, September 14). *China proposes new regulation on labeling AI-generated content*. https://global.chinadaily.com.cn/a/202409/14/WS66e53f8da3103711928a80d1.html

[42] Interim measures for the management of generative artificial intelligence services (2023). China Cyberspace Administration. https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm. (In Chinese).

Conclusion

Amidst the rapid advancements in artificial intelligence technologies, the formation of a comprehensive legal regulatory system integrating private law and public law responsibility mechanisms has become increasingly critical. A comparative analysis of existing regulatory approaches reveals the dualistic nature of AI legal regulation, where the interaction between private law and public law methods shapes a cohesive system of normative governance.

In the realm of private law, there is a trend towards institutionalizing responsibility mechanisms, whose primary function is to compensate for damages and restore violated rights. The implementation of strict liability for subjects involved in the development and operation of AI systems ensures efficient distribution of responsibility among participants throughout the life cycle of AI systems. Applying a differentiated approach to determining operator responsibility, grounded in concepts of strict and fault-based liability, enhances safety levels and accountability in the functioning of AI systems. However, the specific characteristics of AI, including decision-making autonomy and self-learning capabilities, pose certain challenges to traditional models of civil liability, necessitating the improvement of legal norms and the development of innovative concepts, notably the notion of partial legal personality for AI.

From a public law perspective, regulation occurs via imperative normative acts, exemplified by the European Union Regulation on Artificial Intelligence (AI Act 2024/1689). This act implements a risk-based approach to classifying AI systems, setting forth differential requirements depending on the level of potential risks. Public-law responsibility mechanisms encompass not only direct participants in the development and operation of AI systems but also state institutions, endowing them with appropriate supervisory powers to ensure compliance with established regulatory requirements.

Integrating these regulatory trends is crucial for creating a balanced legal system capable of adapting to the challenges posed by the evolving technology of AI. The synthesis of effective public-law regulation and modernized civil responsibility mechanisms establishes a fundamental legal foundation for the functioning of AI technologies, facilitating sustainable innovation while simultaneously minimizing the risks of their detrimental impact on socio-economic relations.

Acknowledgements

The research was supported by the Russian Science Foundation, Project No. 24-28-01112, https://rscf.ru/project/24-28-01112/.

References

Aleksikova, O. E., & Melnik, E. A. (2017). Problems of determining the legal nature of civil liability of a legal entity. *Bulletin of the Volga Region Institute of Management*, *17*(6), 60–66. https://doi.org/10.22394/1682-2358-2017-6-60-66. (In Russian).

Drozdov, V. Y. (2024). Limits of criminal liability for the use of artificial intelligence. *Legal Science*, *9*, 207–210. (In Russian).

Eidenmueller, H. (2017). *The rise of robots and the law of humans* (Oxford Legal Studies Research Paper No. 27/2017). http://dx.doi.org/10.2139/ssrn.2941001

Filippova, I. A. (2024). Legal regulation of artificial intelligence: Experience of China. *Journal of Digital Technologies and Law*, *2*(1), 46–73. https://doi.org/10.21202/jdtl.2024.4. (In Russian).

Gorokhova, S. S. (2021). On some aspects of public legal liability in the field of using artificial intelligence and autonomous robots. *Legal Research*, *5*, 24–41. https://doi.org/10.25136/2409-7136.2021.5.35557. (In Russian).

Kaminski, M. E. (2019). The right to explanation, explained. *Berkeley Technology Law Journal*, *34*(1), 189–218. https://doi.org/10.31228/osf.io/rgeus

Kazakova, I. A., Kamalieva, L. A., & Sled, Y. G. (2020). On the specifics of bringing to justice the owners of sources of increased danger. *Law and State: Theory and Practice*, *3*(183), 36–39. (In Russian).

Kovalenko, S. P. (2014). Legal nature of civil liability of participants in corporate relations. *Legal Concept*, *1*, 76–80. (In Russian).

Kuteinikov, D. L., Izhaev, O. A., Zenin, S. S., & Lebedev, V. A. (2022). *Artificial intelligence and law: From fundamental problems to applied tasks: Monograph*. Tyumen State University. (In Russian).

Liu, H., Maas, M., Danaher, J., Scarcella, L., Lexer, M., & Rompaey, L. (2020). Artificial intelligence and legal disruption: A new model for analysis. *Law, Innovation and Technology*, *12*(2), 205–258. https://doi.org/10.1080/17579961.2020.1815402

Mocanu, D. M. (2022). Gradient legal personhood for AI systems–Painting continental legal shapes made to fit analytical molds. *Frontiers in Robotics and AI*, *8*, 1–11. https://doi.org/10.3389/frobt.2021.788179

Mosechkin, I. N. (2019) Artificial intelligence and criminal liability: Problems of becoming a new type of crime subject. *Bulletin of St. Petersburg State University. Series 14. Law*, *3*, 461–476. https://doi.org/10.21638/spbu14.2019.304. (In Russian).

Mozolin, V. P. (2012). Civil liability in the system of Russian law. *Journal of Russian Law*, *1*(181), 33–40.

Musalov, M. A., & Rashidov, Sh. M. (2023). Interrelated provisions of Articles 15 and 1064 of the Civil Code of the Russian Federation. *Law and State: Theory and Practice*, *3*(219), 172–174. (In Russian).

Pomeranets, A. D., & Kolentsova, V. V. (2022). Criminal liability and artificial intelligence. *Law and State: Theory and Practice*, *2*(206), 273–278. https://doi.org/10.47643/1815-1337_2022_2_273. (In Russian).

Ponkin, I. V., & Redkina, A. I. (2018). Artificial intelligence from the point of view of law. *Bulletin of the Peoples' Friendship University of Russia. Series: Legal Sciences*, *1*, 91–109. https://doi.org/10.22363/2313-2337-2018-22-1-91-109. (In Russian).

Rostovtseva A. M. (2013). The relationship between civil liability of participants in corporate relations and administrative and criminal liability. *Society and Law*, *1*(43), 83–87. (In Russian).

Sakharov, A. G., & Shelepov, A. V. (2024). China's digital platforms regulation policy. *International Organisations Research Journal*, *19*(2), 145–160. https://doi.org/10.17323/1996-7845-2024-02-08. (In Russian).

Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. *Fordham Law Review*, *87*, 1085–1139. https://doi.org/10.2139/ssrn.3126971

Söderlund, K., & Larsson, S. (2024). Enforcement design patterns in EU law: An analysis of the AI act. *Digital Society*, *3*, 1–21. https://doi.org/10.1007/s44206-024-00129-8

Staunton, C., Adams, R., Anderson, D., Croxton, T., Kamuya, D., Munene, M., & Swanepoel, C. (2020). Protection of Personal Information Act 2013 and data protection for health research in South Africa. *International Data Privacy Law*, *10*(2), 160–179. https://doi.org/10.1093/idpl/ipz024

Weston, F. C. L., Paglioli, A. C. B., & Weston, M. W. (2023). Lei Geral de Proteção de Dados Pessoais e aplicabilidade para a Enfermagem. *Revista Brasileira de Enfermagem*, *76*(Suppl. 3), e20230126. https://doi.org/10.1590/0034-7167-2023-0126pt. (In Portuguese).

Woolcott Oyague, O., Monje Mayorca, D. F., Comandé, G., Peláez Hernández, R. A., & Morales Hervias, R. (2019). *The modernization of civil law institutions: Civil liability, property and contract*. Universidad Católica de Colombia.

Zhaglina, M. E., & Zhaglin, A. V. (2022). Liability for harm caused by artificial intelligence: reality and prospects. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, *2*, 75–78. (In Russian).

Information about the authors

Ilya R. Khmelevskoi (Tyumen, Russian Federation) – Teaching Assistant, Academic Department, School of Law and Governance, University of Tyumen; Postgraduate Student, Academic Department, School of Law and Management, University of Tyumen (6 Volodarskogo St., Tyumen, 625003, Russian Federation; e-mail: i.r.khmelevskoi@utmn.ru) – **corresponding author**.

Nikita A. Kalashnikov (Tyumen, Russian Federation) – Teaching Assistant, Academic Department, School of Law and Governance, University of Tyumen; Laboratory Assistant, "4Bio" Laboratory, Center for Innovative Design and Applied Research, School of Law and Management, University of Tyumen; Postgraduate Student, Academic Department, School of Law and Management, University of Tyumen (6 Volodarskogo St., Tyumen, 625003, Russian Federation; e-mail: n.a.kalashnikov@utmn.ru).