Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

Research Article

BRIDGING THE GAP: ACCOUNTABILITY AND RISK-BASED REGULATION IN KAZAKHSTAN'S ARTIFICIAL INTELLIGENCE LEGISLATION

Yenlik Nurgaliyeva, Aruzhan Baimakhanova*, Svetlana Zharkenova and Guzal Galiakbarova

DOI:
https://doi.org/10.33327/AJEE-18-9.2-a000187

Date of submission: 06 Jan 2026
Date of acceptance: 18 Feb 2026
Online First Publication: 20 March 2026
Last Publication: 20 May 2026

ABSTRACT

Background: *This article addresses the critical challenges of establishing a robust legal regime for artificial intelligence (AI) in the wake of the European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689, EU AI Act) and the Law of the Republic of Kazakhstan 'On Artificial Intelligence' (2025 or Kazakhstan AI Law). Despite these legislative efforts, scholarly debates persist regarding AI's legal status, personality, and protective functions. This study highlights a necessary shift from reactive regulation to a preventive, risk-based model in which legal norms adapt to algorithmic behavior before conflicts emerge. The research aims to identify regulatory gaps in the Kazakhstani framework relative to European standards, specifically in the areas of fundamental rights protection and judicial accountability.*

Method: *The study employs a descriptive-analytical, comparative research methodology. A legal doctrinal analysis of the EU AI Act and the Kazakhstan AI Law was conducted to*

identify existing regulatory gaps. The formal-legal method was used to evaluate definitions of AI and its legal characteristics. Content analysis of contemporary legal scholarship (2015–2025) provided the basis for legal modeling of the 'electronic personhood' status. The research also utilizes a systems approach to categorize AI risks—minimal, medium, and high—within the public administration and law enforcement sectors.

Results and Conclusions: *The analysis reveals that while the EU AI Act establishes a comprehensive ban on high-risk technologies such as mass biometric surveillance and predictive policing, the Kazakhstan AI Law lacks similar prohibitions, potentially leading to discriminatory law enforcement practices. The study concludes that recognizing AI as an 'electronic personhood' with a hybrid legal capacity is essential for ensuring accountability for autonomous decisions. Specific legislative amendments are proposed for the Kazakhstan AI Law, including: 1) mandating independent expert assessments for high-risk systems; 2) prohibiting the exchange of state secret databases via AI platforms; 3) establishing algorithmic accountability for providers and operators. The research emphasizes that balancing innovation with digital accountability is the key challenge for modernizing the national digital legal order.*

1 INTRODUCTION

The impact of AI on fundamental human rights is of great interest to legal scholars, who are concerned about the potential adverse effects of AI on humans and the need to develop legal mechanisms to protect human rights when using AI.

This discussion of the place and role of artificial intelligence in the legal system is among the central areas of legal research. Over the past decade, there has been an active development of new legal doctrines concerning the status of AI as a subject and an object of law, the ethical foundations of algorithmic management, and institutional mechanisms for the legal regulation of digital technologies. The researchers emphasize that AI is not just a technical phenomenon, but one that transforms the fundamental categories of law and order—subjectivity, responsibility, the expression of will, and legal personality.[1]

The EU AI Act adopted by the European Union in 2024 failed to solve all the problems related specifically to the legal regulation of AI, which is confirmed by ongoing

1 Joanna J Bryson, Mihailis E Diamantis, and Thomas D Grant, 'Of, For, and By the People: The Legal Lacuna of Synthetic Persons' (2017) 25 Artificial Intelligence and Law 273, doi:10.1007/s10506-017-9214-9.

discussions about its legal regime of use, regulatory methods, areas of its application, as well as its protective properties.[2]

In her capacity as the Rapporteur for the Committee on Legal Affairs, Mady Delvaux-Stehres argued that "robots can no longer be considered as simple tools in the hands of other actors. The more they are able to learn and take autonomous decisions, the less they are just a tool." This paradigm shift leads to the recommendation of "creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic personhoods responsible for making good any damage they may cause." This status would specifically apply to cases where robots make autonomous decisions or otherwise interact with third parties independently.[3]

At the same time, according to A. Hars, it has recently been impossible to implement legal regulation of AI, since, due to its complexity, opacity, and rapidly changing 'nature,' it will undoubtedly be challenging to establish regulatory rules with their transparency, certainty, and explicitness. In addition, possible failures in AI's work will not meet regulatory expectations, may harm, undermine confidence in the legal institutions they use, and, ultimately, affect its development and use.[4]

In this regard, the EU AI Act serves as a primary benchmark for our study, providing a comparative framework to evaluate the normative gaps in the recently adopted Kazakhstan AI Law.[5] This article critically analyzes the emerging legal regime in Kazakhstan, focusing on the transition toward a risk-based regulatory model and the contentious proposal to grant AI the status of an 'electronic personhood' to ensure accountability and the protection of fundamental rights.

2 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) [2024] OJ L <http://data.europa.eu/eli/reg/2024/1689/oj> accessed 5 January 2026; *EU Artificial Intelligence Act: Up-to-date developments and analyses of the EU AI Act* <https://artificialintelligenceact.eu/> accessed 5 January 2026.

3 European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) [2018] OJ C 252/239; Nathalie Nevejans, *European Civil Law Rules in Robotics: Study* (EU 2016) <https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2016)571379> accessed 21 February 2026.

4 András Hárs, 'AI and International Law: Legal Personality and Avenues for Regulation' (2021) 62(4) Hungarian Journal of Legal Studies 320, doi:10.1556/2052.2022.00352.

5 Law of the Republic of Kazakhstan No 230-VIII 'On Artificial Intelligence' (adopted 17 November 2025) [in Kazakh] <https://adilet.zan.kz/kaz/docs/Z2500000230> accessed 5 January 2026.

2 METHODOLOGY

This study employs a comprehensive descriptive-analytical and comparative research framework designed to evaluate the legal challenges posed by artificial intelligence (AI) within the digital legal order. To ensure a multidimensional examination, the research is organized into the following methodological stages:

The choice of EU Law as the main reference is due to its role as the world's first comprehensive regulatory standard, defining the global trajectory of AI regulation through risk assessment. The primary research tool is the comparative legal method, used to identify divergences and normative gaps between the European Union's Artificial Intelligence Act *(*Regulation (EU) 2024/1689, *EU AI Act*) (hereinafter – EU AI Law) and the Law of the Republic of Kazakhstan 'On Artificial Intelligence' (2025). This comparison extends beyond textual differences to a doctrinal inquiry into the underlying regulatory models—liberal, ethical-normative, and technocratic—to determine their suitability for the Kazakhstani legal tradition.

The method of legal modeling is applied to construct the conceptual framework for the 'electronic personhood' status. This involves a functional approach that prioritizes algorithmic accountability over purely technical definitions, shifting the focus from AI as a 'pile of metal' to AI as an autonomous legal category capable of bearing responsibility.

A systems approach was utilized to analyze AI as an integrated complex of software-hardware architecture and cognitive-functional elements. Content analysis of global scholarly literature (2015–2025) and international frameworks, such as UNESCO and OECD recommendations, provided the basis for evaluating emerging concepts, including predictive policing and risk-based regulation.

The study adopts a proactive legal design paradigm, to evaluate how transparency and the duty of explainability can be integrated into the legal framework to ensure effective judicial oversight. This methodological focus ensures that the proposed legislative amendments are designed to balance technological innovation with the protection of fundamental human rights.

3 EVALUATING THE KAZAKHSTAN AI LAW THROUGH THE PRISM OF THE EU AI ACT

3.1. Comparative Analysis of AI Definitions and Risk-Based Regulation

Economic growth and the modernization of national infrastructure are increasingly driven by the deep integration of digital technologies and AI across key industrial and financial sectors. Under these conditions, legal certainty in AI's interactions with humans is essential, ranging from access to 'data' to ensuring the security, confidentiality, and quality of that

'data'. The guarantee of security is directly related to the protection of human rights and freedoms, not only in the application of AI but also in its development, which, in turn, objectively requires ensuring the rule of law.

To develop effective legal regulation, special attention should be paid to the concept of 'artificial intelligence' and its features in the legal sense.

The definitions of AI in the scientific literature do not meet the requirements for legal definitions, as they are excessively vague and comprehensive, and therefore, their practical application is questionable.

The evolution of legal thought necessitates a shift from technical, hardware-oriented descriptions of artificial intelligence to a functional and risk-based framework.

Early definitions, such as those focusing on 'cybernetic computer-software-hardware systems', are increasingly viewed as outdated and overly localized, offering limited utility for determining modern civil liability.

In contrast, the European approach, epitomized by the EU AI Law, defines an AI system as a machine-based system designed to operate with varying levels of autonomy, focusing on its ability to generate outputs, such as predictions, recommendations, or decisions that influence physical or virtual environments.

This shift is mirrored in the OECD guidelines, which emphasize the system's capacity for 'inference' to achieve explicit or implicit objectives.[6]

Furthermore, the UNESCO Recommendation frames AI as an information ecosystem, prioritizing human rights and non-discrimination.[7] Aligning national legislation with these international standards is crucial for bridging the 'digital divide' and ensuring that AI is treated not merely as a 'pile of metal,' but as a sophisticated legal construct requiring a robust framework for liability and insurance.

When revealing the essence of the term 'artificial intelligence', in our opinion, there is no need to describe AI's abilities and capabilities in detail; instead, focus on the signs of AI. Without identifying which, it is impossible to give an understandable definition of AI.

Also, the definition of AI given in the 'AI Act' cannot be called successful, where AI is understood as a 'machine system' designed to work with various levels of autonomy and which can be adaptive after deployment, and which, to achieve explicit and implicit goals, draws conclusions based on the input data received on how to generate output

6 OECD, *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449, OECD 2025) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 21 February 2026.

7 UNESCO, *Recommendation on the Ethics of Artificial Intelligence 2021* (SHS/BIO/REC-AIETHICS/2021, UNESCO 2021) <https://unesdoc.unesco.org/ark:/48223/pf0000380455> accessed 21 February 2026.

data, such as forecasts, content, recommendations, or decisions that may affect physical or virtual environments.'[8]

In this definition, we also do not find significant signs of AI, such as the ability of AI to simulate human cognitive functions: to simulate the most complex functions of the brain, through which the process of rational cognition of the world is carried out, including self-learning and the search for solutions without a predefined algorithm; comparability of the result of AI with the results of human intellectual activity, etc.

The Kazakhstan AI Law, Art. 1, paragraph 3, defines the following:

> 'Artificial intelligence is a functional ability to simulate cognitive functions characteristic of humans, providing results comparable to or superior to the results of human intellectual activity.'[9]

This definition has not been finalized linguistically and does not reflect the essential features of AI.

The answer to the question of what the main policy directions are in the field of legal regulation and the use of AI was given in the Stanford University report 'Artificial Intelligence and Life in 2030':

> '1. Define a path toward accruing technical expertise in AI at all levels of government.
>
> 2. Remove the perceived and actual impediments to research on the fairness, security, privacy, and social impacts of AI systems.
>
> 3. Increase public and private funding for interdisciplinary studies of the societal impacts of AI.'[10]

Of course, these areas of AI development and use are not enough for the safe coexistence of AI and society, and therefore, they can be supplemented with the following:

- ensuring that people are informed about the benefits and risks associated with using AI;
- training of highly qualified specialists in the field of AI;
- ensuring the certification of AI systems and a ban on the production and use of non-certified systems;
- development of mechanisms of tort and joint liability for the use of non-certified systems.

8 Regulation (EU) 2024/1689 (n 2) para 12.
9 Law of the Republic of Kazakhstan No 230-VIII (n 5) art 1, para 3.
10 Peter Stone and others, 'Artificial Intelligence and Life in 2030: The One Hundred Year Study on Artificial Intelligence' (arXiv:2211.06318, 31 October 2022) 47, doi:10.48550/arXiv.2211.06318.

The purpose of the law adopted by the European Union is to protect fundamental rights, democracy, the rule of law, and environmental sustainability from the risks posed by high-risk artificial intelligence. That is, the primary focus is on protecting fundamental human rights from AI, which, in turn, is called high-risk. The Kazakh law does not have this goal. However, it proclaims, as one of the basic principles of state regulation of public relations in the field of artificial intelligence, the principle 'as the priority of human well-being, freedom of will in decision-making.'[11] As a well-known fact, the purpose of any law is a specific result that the legislator strives for, and the principle is the general idea underlying the law. Consequently, the basis of legal regulation is not only the ideas laid down in the law, but a specific result. Unfortunately, laws do not always clearly define the primary purpose of the law, but there is a 'substitution' of principles, objectives, etc., by categories.

Despite the difficulties associated with legal regulation, Kazakhstan has adopted the AI Law, the effectiveness of which will be demonstrated by its practical application. Thus, Chapter 4 'Artificial intelligence systems', in particular, Article 17 'Legal regime of artificial intelligence systems'

(voluminous in content) divides artificial intelligence systems, depending on the degree of impact on the security of society, users, and the state, into three categories: minimal, medium, and high risk. At the same time, the assignment of artificial intelligence systems to a specific category is determined by their owner in accordance with the principles of information object classification. Unlike Article 5 of the EU Law on AI, which establishes an exhaustive list of prohibited practices (in particular, real-time remote biometric identification), Article 17 of the Law of the Republic of Kazakhstan on AI focuses on risk classification, leaving issues such as crime prediction outside the scope of direct prohibition. For clarity, we will construct a table.

***Table* 1. Comparative table of prohibited practices**

No	Type of prohibition	EU AI Law[12]	Kazakhstan AI Law[13]
1	Social screening Clause "c" of paragraph 1 of Article 5 of the EU AI Law	Placing on the market, commissioning, or using an AI system that exploits a person's vulnerability due to their age, disability, or other specific social or economic situation is prohibited.	Article 17 of the Law of the Republic of Kazakhstan on AI Paragraph 3 prohibits the creation and operation of AI systems possessing one of the creative functional capabilities within the territory of the Republic of Kazakhstan;

11 Law of the Republic of Kazakhstan No 230-VIII (n 5) art 4, para 5.

12 Regulation (EU) 2024/1689 (n 2).

13 Law of the Republic of Kazakhstan No 230-VIII (n 5).

No	Type of prohibition	EU AI Law[12]	Kazakhstan AI Law[13]
		It is completely prohibited for the state and private individuals.	The assessment and classification of individuals or groups of individuals for a specific period based on their social behavior or known, assumed, or predicted personal characteristics is prohibited, except in cases stipulated by the Law of the Republic of Kazakhstan (clause 2, paragraph 3 of Article 17). The exploitation of an individual's moral and or physical vulnerability due to age, disability, social status, or any other circumstances for the purpose of causing or threatening to cause harm to an individual is also prohibited (clause 2, paragraph 3 of Article 17).
2	Biometric categorization Clause "b" of paragraph 1 of Article 5 of the EU AI Law	The placing on the market, putting into operation for a specific purpose, or use of biometric categorization systems that classify individuals based on their biometric data to conclude their race, political views, trade union membership, religious or philosophical beliefs, convictions, sex life, or sexual orientation is prohibited. The use of remote biometric identification systems in "real-time" mode in public places for law enforcement purposes is prohibited.	Classifying individuals based on their biometric data to conclude their race, political views, religious affiliation, or other circumstances (criteria) for the purpose of discriminating against them in any way is prohibited. (clause 5, paragraph 3 of Article 17 of the Law of the Republic of Kazakhstan)

No	Type of prohibition	EU AI Law[12]	Kazakhstan AI Law[13]
3	Manipulative methods Clause "a" of Article 5 of the EU AI Law	It is prohibited to place on the market, commission, or use AI systems that use subconscious techniques beyond human creation or purposefully manipulative or misleading methods to significantly distort personal behavior that impairs a person's ability to make an informed decision.	It is prohibited to use subconscious, manipulative, or other methods that use the behavior of an individual and limit the ability to make informed decisions or force them to make decisions that may cause harm or create a threat of harm (clause 1, paragraph 3 of Article 17 of the Law of the Republic of Kazakhstan)
4	Predictive methods based on profiling (predictive policing) Clause "da" of paragraph 1 of Article 5 of the EU AI Law)	It is prohibited to place on the market, put into operation, or use AI to assess the risk of individuals in order to assess or predict the risk of an individual committing a criminal offense based solely on profiling an individual or evaluating their personal qualities and characteristics. This prohibition does not apply to AI systems used to support human assessment, which is already based on objective and verifiable facts related to criminal activity.	Not mentioned.
5	Methods for determining emotions Clause "dc" of paragraph 1 of Article 5 of the EU AI Law	Placing on the market, commissioning, and using AI systems to determine an individual's emotions in workplaces and educational institutions are prohibited. Exception: It is allowed to use AI for medical or safety reasons.	Clause 6, paragraph 3 of Article 17 of the Law of the Republic of Kazakhstan: It is prohibited to determine the emotions of an individual without his consent, except in cases provided for by the laws of the Republic of Kazakhstan.

As shown in Table 1, the EU AI Law contains categorical prohibitions on unacceptable uses of AI. Some of these prohibitions are reflected in paragraph 3 of Article 17 of the Law of the Republic of Kazakhstan, although not in a categorical form. Thus, the prohibition of social screening (clause 2, paragraph 3 of Article 17) and methods of determining emotions (clause 6, paragraph 3 of Article 17) are prohibited by law, but may be supplemented by departmental regulatory legal acts or contain exceptions to legislative rules, which, in our opinion, should not be allowed. The law should be of direct effect, especially in terms of prohibitions; i.e., it should contain legal provisions that are directly applicable, without the need to adopt additional clarifying regulatory legal acts. For some reason, the ban on predictive policing was not reflected. This is not accidental, as lawmakers considered it possible to use AI in law enforcement, although this contradicts international standards. After all, it is known that AI modules can inherit the bias of historical crime data, which can lead to discriminatory police work methods.

3.2. The Doctrine of 'Electronic personhood' and Algorithmic Accountability

The difficulties of legal regulation of AI are highlighted in Ruschemeier's' article, which focuses on humanity overall attitude towards AI. In her opinion, on the one hand, AI is charged with solving humanity's most serious problems of without taking into account the human factor, i.e., its role is overestimated; on the other hand, the impact of 'big data' on man-made social, political, and other structures is underestimated. Given that AI systems pose different problems depending on the subject of use and the purpose of use, he considers it impossible to formulate a single comprehensive definition for 'algorithms' of 'AI'. She suggests developing various characteristics of various algorithms and applications of AI, and ways to use them in practice. Taking into account these problems, he justifies the need for legal regulation of AI, which would contain effective ways to manage them and, instead of a single comprehensive definition of the role of 'AI' algorithms, puts forward his position, which is to develop separate characteristics of various AI algorithms and applications and ways to use them in practice.[14] This proposal should be supported since in reality, practice needs not so much general legal regulation as specialized regulation that identifies the specifics of AI, taking into account its application industries.

Further, Ruschemaer suggests three approaches to the possible legal regulation of AI by legal norms: the first approach is objective regulation, in which AI will be in the situation in which it currently finds itself; the second approach is the introduction of minor changes to legislation; and, finally, the third approach is the possibility of providing AI with personality status.[15]

14 Hannah Ruschemeier, 'AI as a Challenge for Legal Regulation – The Scope of the Artificial Intelligence Act' (2023) 23(3) ERA Forum 361, doi:10.1007/s12027-022-00725-6.

15 ibid

We should pay attention to the second and third approaches, since it is impossible to constantly 'keep' AI static; it is rapidly developing. We should take a closer look at the third approach while making minor changes to the legislation. In this regard, it is impossible not to turn to the opinion of Hars, who proposes to provide AI not with a full, but with a semi-status, the essence of which is that AI will receive the status 'in portions', i.e., rights and obligations will be granted to it as necessary, with mandatory justification for their provision. That is to assign legal personality to AI in accordance with human needs.[16]

A group of scientists advocating the endowment of AI with legal capacity, i.e., to be a subject of legal relations (to have rights and responsibilities), does not take into account that AI is currently in the process of formation and development, and recognition of legal personality for AI is unlikely to be implemented in practice.

One can consider awarding AI a hybrid legal capacity, i.e., one that combines elements of both an individual and a legal entity. Recently, there has been a shift away from treating AI solely as an object of law, in which it has only property rights. In the legal literature, the prevailing position is to recognize AI in the distant future as a legal entity or formally award it legal status.

The uncertainty in matters of legal personality stems from the fact that AI and its properties have not been sufficiently studied, not only from a legal perspective but also as a phenomenon, despite the benefits of AI for humanity and society being recognized. One thing is known that 'AI differs from conventional computer algorithms in that it can train itself and, based on its experience, can act differently in similar situations depending on previously performed actions.'[17]

The heterogeneity of AI makes it possible to divide them into two types: conventional AI, which ensures the creation of new scientific and technical products for all spheres of public life, and universal AI, which has significantly greater opportunities to influence public relations involving individuals and legal entities, which objectively requires their differentiated legal regulation.

Despite the uncertainty in establishing AI's legal personality, it should be recognized that AI is a legal category, if only because of the need to develop a concept that provides for AI's liability for damage caused by its actions against individuals and legal entities.

Thus, there are three leading positions of scientists regarding the status of AI: 1) AI is a subject of law and is close to an individual in content; there is a proposal to introduce a separate legal status of an 'electronic personhood'; 2) AI is an object of law and should be equated with animals in status, i.e. it is property; 3) AI is only a technical means.

16 Hárs (n 4).

17 Paulius Čerka, Jurgita Grigienė and Gintarė Sirbikytė, 'Liability for Damages Caused by Artificial Intelligence' (2015) 31(3) Computer Law & Security Review 376, doi:10.1016/j.clsr.2015.03.008.

The most appropriate way to characterize AI is to recognize it as a status of 'electronic personhood' with hybrid legal capacity, which is necessary not as a technical formality, but as a mechanism for distributing algorithmic responsibility. The proposed status will enable AI to make independent decisions, interact with other actors, and most importantly, be responsible for its autonomous decisions. Establishing legal responsibility is objectively necessary, as AI activities pose significant risks, including breaches of data security and confidentiality, targeted attacks, and serious consequences for users due to unauthorized access to personal data. It is the risks of using AI that require a responsible approach to the use of AI and the creation, on the one hand, of 'adequate legal protection of fundamental human rights and, on the other hand, conditions for the development of innovation. The balance between security and innovation will be a key challenge to the implementation of the new EU law.'[18]

Undoubtedly, the EU AI Act has become the basis for regulating neural networks worldwide, including Kazakhstan. Kazakhstan's current 'Concept for the Development of Artificial Intelligence for 2024-2029'[19] has established benchmarks for reaping the benefits of AI technologies in the short- and medium-term, as well as for preparing for potential long-term challenges. It also stipulates that AI technologies should not discriminate against anyone or violate privacy, personal, or family secrets. Unfortunately, this Concept mentions the liability of AI system providers and operators for harm caused to third parties. The 'Act on AI' only provides for fines for failure to comply with established regulations governing the operation of AI systems, for non-compliance with established requirements, and for failure to provide information or for providing false or incomplete information about the system's operation to the authorized body. As can be seen, none of the aforementioned documents address who is responsible for decisions made by AI. Kazakhstan's law partially fills this gap by establishing civil and administrative liability for these actions, but it does not specify the mechanisms for their implementation.

In the Anglo-American legal tradition, by contrast, researchers' attention is focused on legal responsibility for AI's actions. Ryan Calo notes that algorithmic autonomy creates 'legal blind spots' where classical institutions of civil, administrative, and criminal responsibility lose their effectiveness.[20] The scientist introduces the Concept of 'moral crumple zones', a metaphor describing how responsibility for the actions of autonomous systems is actually shifted to the people involved in their operation, regardless of the actual degree of control. Continuing this thought, Joanna Bryson argues that recognizing AI as a legal entity is

18 Asel Imangalieva and Dauren Karashev, 'Issues of Legal Personality of Artificial Intelligence: Responsibility of Artificial Intelligence in Kazakhstan' (*PRG*, 28 March 2024) <https://prg.kz/document/?doc_id=34826280> accessed 5 January 2026.

19 Resolution of the Government of the Republic of Kazakhstan No 594 'Concept for the Development of Artificial Intelligence for 2024–2029' (adopted 24 July 2024) [in Kazakh] <https://adilet.zan.kz/kaz/docs/P2400000592> accessed 5 January 2026.

20 Ryan Calo, 'Robotics and the Lessons of Cyberlaw' (2015) 103(3) California Law Review 513.

unacceptable, as it would lead to 'blurring accountability' and undermine the principle of individual responsibility.[21]

Particular attention is paid to algorithmic accountability, which entails transparency in decision-making by machine systems. European authors emphasize that the duty of explainability must be integrated into the legal framework of AI, as without it, effective judicial and administrative oversight is impossible.[22]

It follows from this that, as a rule, the legal impact on public relations arises as the need to solve a problem, whereas preventive regulation is aimed at preventing offenses. Therefore, the strategic objective of legal regulation of AI is to ensure that existing norms are ready to prevent conflicts. At the same time, the transparency of decision-making by machine systems is of great importance.

As shown by the positions of the scientists described above, the optimal model of legal regulation has not yet been developed, indicating the complexity of the AI object we are studying.

In our opinion, especially in the context of the positions of scientists that have not been confirmed by practice, it is impossible to unequivocally answer the question of endowing AI with legal personality, since AI lacks several essential features of legal personality that a person possesses – this is assertive behavior (to feel, assert, defend, etc.). AI, imitating human behavior, at the same time cannot identify with a person.

3.3. Global Trends and Institutional Adaptation

Susskind draws attention to the institutional consequences of introducing AI into the legal sphere, noting that traditional professions are losing their monopoly on legal knowledge. He argues that the strategic goal of the legal system is to shift from reactive regulation to proactive legal design, where legal norms adapt to the behavior of algorithms even before a conflict arises.[23]

Analyzing the 'EU AI Law,' Lucaj et al. note that regulation alone will not be sufficient if additional tools are not in place throughout the entire lifecycle: testing, documentation and reliability practices, auditing, and interdisciplinary training. Further AI research should concern mandatory audits throughout the entire lifecycle; conducting technical expertise in government institutions and developing infrastructure and tools for accredited certification and harmonized standards.[24]

21 Bryson, Diamantis, and Grant (n 1).

22 Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12(4) Regulation & Governance 505, doi:10.1111/rego.12158.

23 Richard Susskind, *Tomorrow's Lawyers: An Introduction to Your Future* (3rd edn, OUP 2023) doi:10.1093/9780192864727.001.0001.

24 Laura Lucaj and others, 'TechOps: Technical Documentation Templates for the AI Act' (arXiv:2508.08804v1, 12 August 2025) doi:10.48550/arXiv.2508.08804.

We should note that several foreign studies address ethical principles and regulatory mechanisms of algorithmic management. Floridi and Cowls proposed the Concept of five universal principles of responsible AI—benevolence, harm avoidance, autonomy, justice, and explainability.[25] These principles have served as the basis for some international documents, including the UNESCO Recommendations on AI Ethics (2021) and the OECD Framework Policy.[26] Karen Yeung develops the idea of algorithmic governance, understanding it as a system of regulatory management of citizens' behavior through codes and algorithms, which transforms the classical model of public regulation.[27]

In EU Law, all AI-based systems are classified by risk level: unacceptable, high, limited, and minimal. Unacceptable risk is prohibited; high risk has eight categories; limited risk has a fixed, predetermined maximum amount of possible damage; and minimal risk is practically unregulated. The Kazakhstan AI Law defines three levels of risk without detailing: high, medium, and minimal risk, categories that the Government of the Republic of Kazakhstan determines.

Thus, EU AI Law contains:

- misuse of images of people from the Internet or from surveillance cameras to create facial recognition databases;
- recognizing emotions in the workplace and in educational institutions, conducting social ratings, manipulating human behavior, or exploiting its vulnerability;
- predictive policing (predicting the future behavior of someone or something); predictive activities when crimes are predicted by artificial intelligence.

At the same time, law enforcement agencies can use a biometric identification system to search for a missing person or prevent a terrorist attack. However, in this case, they need to obtain judicial or administrative permission and strictly observe security measures. Mass biometric surveillance in real time is prohibited. In addition, the law strictly regulates generative AI and high-risk AI-based systems.

EU law grants citizens the right to file complaints about AI systems and receive clarifications about decisions that affect their rights. AI systems must also respect copyright, and artificial or processed images, audio, or video content must be clearly marked as such.[28] These issues are reflected in the Kazakh law in one interpretation or another.

25 Luciano Floridi and Josh Cowls, 'A Unified Framework of Five Principles for AI in Society' (2019) 1(1) Harvard Data Science Review 2, doi:10.1162/99608f92.8cd550d1.

26 OECD, *State of Implementation of the OECD AI Principles: Insights from National AI Policies* (OECD Digital Economy Papers no 311, OECD Publishing 2021) doi:10.1787/1cd40c44-en.

27 Yeung (n 22).

28 Regulation (EU) 2024/1689 (n 2) arts 50, 86.

One of the main issues is the legal personality of AI, which is not, by accident, included in the European Union's agenda, which is seriously considering two issues that have arisen: 1) whether AI should be considered as individuals or legal entities, animals, or other existing subjects of law; 2) whether a new category should be created with its own characteristics and applicable consequences in the context of the distribution of rights and obligations, including liability for damage.

In comparative legal terms, three main models for regulating artificial intelligence are generally distinguished:

1. The liberal model (USA, Canada) is characterized by a focus on the principles of self-regulation and soft law, where the state sets only general frameworks. At the same time, specific standards are developed in industry codes of ethics and professional associations.[29]

2. The ethical-normative model (EU) is based on a combination of mandatory norms (GDPR, AI Act) and ethical regulators aimed at protecting human rights and preventing discrimination.[30]

3. The technocratic model (China) assumes the integration of AI into the system of state control, where legal regulation serves as a tool for achieving strategic development goals, rather than protecting private interests.[31]

In the Asian region, the Concept of 'human-centric artificial intelligence' is coming to the forefront, reflected in the strategies of Japan and South Korea. Here, the key objective is the harmonization of technological progress and social values, while regulatory policy is built around the principles of trust, transparency, and social inclusiveness.[32]

Thus, international studies demonstrate a shift from technological determinism to legal pragmatism: artificial intelligence is increasingly viewed not as a threat, but as a socially regulated entity with limited autonomy. International approaches emphasize the need for a balance between innovative development and the protection of human rights, shaping a new paradigm of digital legal order.

A comprehensive analysis of various sources suggests that the current trend is toward the development of hybrid regulatory models that combine mandatory legal norms with mechanisms of self-organization and ethical oversight. This evolution reflects a global shift

29 Ryan Calo, A Michael Froomkin, and Ian Kerr, *Robot Law* (Edward Elgar 2016).

30 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) [2016] OJ L 119/1; Regulation (EU) 2024/1689 (n 2).

31 Angela Huyue Zhang, 'The Promise and Perils of China's Regulation of Artificial Intelligence' (2025) 63 Columbia Journal of Transnational Law 1.

32 OECD (n 26).

in the understanding of law as a dynamic system capable of responding to the technological challenges of the 21st century and integrating elements of algorithmic governance and digital accountability.

Kazakhstan is strengthening its global position in digital governance. According to the UN E-Government Survey 2024, the country rose to 24th place in the global e-government development ranking, improving its position by four places compared to the previous report.[33] The advancement of digital services has been facilitated by the digitalization of the banking sector, and Kazakhstan's openness to integrating its services with banks. For example, the Halyk Bank app allows its clients to register their place of residence. The development of public services is facilitated not only by cooperation with the banking sector but also by nationwide high-speed Internet and cellular coverage.

Despite the widespread implementation of the above-mentioned areas outlined in the State Program, some of the main obstacles to the development of digitalization in Kazakhstan are:

- cumbersome, contradictory, and unstable legislation;
- excessive regulation of government functions and administrative procedures at the legislative level, which deprives authorized bodies of independence and the ability to make prompt decisions to optimize external and internal business processes, implement best practices, and digital solutions;
- legislative gaps in the regulation of digital human and civil rights;
- uncontrolled use of big data, data processing algorithms using artificial intelligence (AI), and the Internet of Things for the implementation of digital surveillance;
- the lack of a unified legislative framework governing the activities of digital service providers.

These problems have become even more acute with the adoption of the 'Concept for the Development of Artificial Intelligence for 2024–2029'[34] in Kazakhstan, as well as the Kazakhstan AI Law,[35] which defines only the guidelines for obtaining the benefits of AI technologies in the short and medium terms.

In addition to discussions of the legal personality of artificial intelligence and the problem of attributing responsibility, the international academic literature also shows a persistent interest in institutional formats for regulating digital technologies. A special place is occupied by the analysis of so-called regulatory sandboxes. These are experimental legal regimes created by the state for the controlled testing of innovative solutions. A study by

33 Department of Economic and Social Affairs, *United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development, With the addendum on Artificial Intelligence* (UN 2024).

34 Resolution of the Government of the Republic of Kazakhstan No 594 (n 19).

35 Law of the Republic of Kazakhstan No 230-VIII (n 5).

Truby et al. traces the dynamics of the development of the European approach to such mechanisms: the authors demonstrate that sandboxes serve as a form of managed legal flexibility, enabling the testing of artificial intelligence systems under reduced regulatory risk.[36] As a result, they become a tool for balancing the need to stimulate technological progress with the requirement to maintain a high level of legal certainty.[37] Similar initiatives are operating in Canada and Singapore, where government agencies act as mediators between AI developers and law enforcement agencies, forming a model of 'adaptive governance,' or adaptive regulation.[38]

US scholarly literature focuses on the problem of antitrust and tort regulation of algorithmically controlled systems. Researchers emphasize that the concentration of large amounts of data in the hands of large corporations (e.g., Amazon, Google, and Meta) poses a threat of 'algorithmic dominance' and requires the modernization of antitrust legislation.[39] At the same time, the existing legal doctrines of 'product liability' and 'negligence' are not able to fully take into account the autonomous nature of AI solutions, which requires the development of a new category of 'algorithmic liability' based on the principles of predictability and verifiability of algorithms. In this context, a significant contribution is made by the literature on the principle of accountability-by-design, which involves the introduction of legal accountability mechanisms at the design stage of artificial intelligence systems.[40]

The research area devoted to international legal aspects of AI regulation deserves special attention. The works of E. Sassoli and M. Ketts consider the problem of autonomous weapon systems (AWS) in the context of international humanitarian law. The authors emphasize that the legal categories of guilt and intent are difficult to apply to autonomous algorithms, which raises the question of the need for a new regulatory paradigm that enshrines the principle of 'meaningful human control' as a prerequisite for the legitimacy of the use of AI.[41] In turn, the doctrine of public international law is developing towards the recognition of artificial intelligence as an object of international regulation, as evidenced by the initiatives of the Council of Europe and the OECD to develop a global Code of Ethics for autonomous technologies.[42]

36 Jon Truby and others, 'A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications' (2022) 13(2) European Journal of Risk Regulation 270, doi:10.1017/err.2021.52.

37 ibid

38 Yeung (n 22).

39 Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard UP 2016).

40 Andrew D Selbst and Solon Barocas, 'The Intuitive Appeal of Explainable Machines' (2018) 87(3) Fordham Law Review 1085.

41 Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare.* (2nd edn, Edward Elgar2022).

42 Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law [2024] CETS 225.

The integration of AI into legal practice, particularly in the justice system, is attracting increasing attention from researchers. Two areas of its application in the justice system are distinguished: 1) office work and general judicial matters; 2) the evaluation of evidence and the establishment of legally significant circumstances in a specific case.

Currently, Kazakhstan has implemented the 'Electronic Justice' system, which allows claims, complaints, and petitions to be filed online through the "Court Office" service, and judicial decisions are issued. This service also determines the jurisdiction for civil cases, minimizing errors in court selection and speeding up claim registration by automatically distributing them. The unified information and analytical system of judicial bodies, "Torelik", is used in the drafting of civil procedural documents. By the beginning of 2025, 665,000 out of two million court cases had been reviewed using AI. The "Digital Analytics of Judicial Practice" program is operational, trained to analyze court decisions, compare them, identify shortcomings, and predict the outcome of a civil case. When a specific claim is submitted, a judge can see judicial practice in similar cases, including cassation, and make the right decision. It should be especially noted that the AI analysis is used as additional reference material.[43]

Effective access to justice requires not only the filing of a complaint, but also legislative recognition of the "duty of explainability." This would allow courts to conduct meaningful analysis of algorithmic decisions, transforming AI from a "black box" into a subject of judicial review.

To explore the second area of AI application in assessing evidence and establishing legally significant circumstances in a specific case, let's consider the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment, which enshrines the following principles:

- respect for fundamental human rights – the right to an adversarial trial;
- the right to a fair hearing;
- non-discrimination against individuals or groups;
- the principle of quality and security, designed to ensure the processing of court documents by officially functioning databases of regulatory legal acts, court decisions, etc.;
- transparency, impartiality, and reliability of data processing methods, as well as external auditing;
- control by the user as an informed subject over the court's decision made using AI.

43 Ainash Seitmuratova, 'Kazakhstani Courts Embrace AI in their Daily Practices' (*Kursiv News*, 22 January 2025) <https://kz.kursiv.media/en/2025-01-22/engk-nknk-kazakhstani-courts-embrace-ai-in-their-daily-practices/?utm_campaign=endless_feed> accessed 5 January 2026.

It is particularly emphasized that AI does not make, but are instead made by a human judge.[44]

In UK court practice, the concept of access to justice when using AI emerged in the case of R (Bridges) v Chief Constable of South Wales Police (2020), which concerned the use of automated facial recognition. The Court of Appeal held that the lack of clear, statutory criteria for the functioning of the algorithmic system and the scope of officials' discretion hindered individuals' ability to predict the legal consequences of its use and, therefore, hindered the exercise of the right to effective judicial review. The court emphasized that even with a formal complaints mechanism, the lack of transparent rules and explainability of the algorithmic decision deprives judicial review of any meaningful content. Thus, the algorithmic system was deemed incompatible with the requirements of legality and procedural fairness precisely because of the lack of legal guarantees of contestability.[45] The British experience confirms that access to justice presupposes not only the possibility of recourse to the courts, but also the legally supported verifiability of algorithmic interventions.

The judicial approaches of EU member states were consolidated with the adoption of the EU Artificial Intelligence Regulation 2024 (AI Act), which, for the first time, enshrined at the supranational level the right of a person affected by an individual decision made using a high-risk AI system to receive an explanation of that decision. The legislator explicitly links the obligation of explainability with the possibility of pursuing legal remedies, including judicial appeal. Thus, the explainability of algorithmic decisions is legally enshrined as a tool for transforming AI from a "black box" into an object of legal assessment and judicial review.[46]

This approach reflects the transition from fragmented judicial protection to a systemic model for ensuring access to justice in the context of digitalization. International judicial experience demonstrates the emergence of a robust approach, according to which the right to appeal decisions made using artificial intelligence cannot be considered effective without legislative and procedural codification of the duty of explainability. Judicial practice confirms that the opacity of algorithmic decisions deprives courts of meaningful oversight and deprives citizens of the right to defense. In this context, explainability is not a technical but a legal condition for access to justice, ensuring that AI becomes an object subject to judicial review.

Thus, a general pattern can be observed: the higher a state's level of technological development, the more attention is paid not to legal prohibition but to institutional adaptation—the creation of flexible, integrated forms of regulation. Canada operates the

44 European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment (adopted 3 December 2018) <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment> accessed 5 January 2026.

45 Case C1/2019/2670 *R (Bridges) v South Wales Police* [2020] EWCA Civ 1058.

46 Regulation (EU) 2024/1689 (n 2) arts 85, 86.

Algorithmic Impact Assessment (AIA), a mandatory risk assessment tool for all government agencies using machine learning systems.[47] These approaches demonstrate that modern legal thought is increasingly leaning toward 'soft governance,' in which mechanisms of monitoring, transparency, and public oversight replace norms.

In the Asia-Pacific region, jurisdictions such as Singapore and South Korea have pioneered operationalized AI governance. Singapore, through its AI Verify Foundation, provides a standardized technical framework for algorithmic testing and verification, facilitating both self-assessments and third-party audits[48]. Similarly, South Korea's Ministry of Science and ICT has integrated ethical compliance into the oversight of high-risk AI applications, moving beyond theoretical guidelines toward institutionalized monitoring and evaluation[49].

The development of legal regulation of artificial intelligence is carried out within the framework of multilevel normativity, in which traditional imperative norms are combined with principles of self-regulation and ethical responsibility. The idea of 'responsible AI' is becoming a kind of legal meta-category that combines legal, ethical, and social mechanisms under a single concept of digital law and order. This trend indicates a shift in emphasis from issues of legal personality and AI to the practical implementation of the principles of transparency, non-discrimination, and the predictability of algorithmic decisions. Therefore, when developing legal mechanisms to regulate AI, it is necessary to draw on scientific and conceptual ideas developed by scientists as guidelines for building national AI regulatory models.

In the context of the evolving legal regulation of artificial intelligence, particular significance should be attached to the problem of normative uncertainty arising from the rapid technological development and the lag of legal institutions. AI systems develop at a pace that outstrips traditional legislative cycles, which leads to the formation of so-called 'regulatory gaps', situations in which socially significant relations mediated by AI fall outside clear legal qualification. This circumstance objectively necessitates a revision of classical approaches to legal regulation based exclusively on static legal norms.

From the standpoint of legal theory, artificial intelligence should be viewed not only as a technological phenomenon but also as a factor transforming the architecture of legal regulation itself. The growing autonomy of algorithmic systems challenges the traditional model of legal causality, which assumes a direct link between the subject's will, action, and legal consequences. In the case of AI, decision-making is often probabilistic, opaque, and

47 'Algorithmic Impact Assessment Tool' (*Government of Canada*, 7 January 2026) <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html> accessed 10 January 2026.

48 Infocomm Media Development Authority (IMDA), 'AI Verify: An International Open-Source Foundation for AI Testing' (2023) <https://aiverifyfoundation.sg/> accessed 21 February 2026.

49 Ministry of Science and ICT (Republic of Korea), 'National Strategy for Artificial Intelligence: National AI Ethics Guidelines' (2020).

distributed across complex socio-technical systems, which complicates the attribution of intent, fault, and foreseeability, core categories of legal responsibility.

In this regard, modern doctrine increasingly turns to functional and risk-oriented approaches to regulation. Instead of focusing exclusively on the legal status of artificial intelligence as a potential subject or object of law, emphasis is placed on controlling the risks generated by AI systems throughout their entire lifecycle: from design and training to deployment and decommissioning. Such an approach corresponds to the law's preventive function and enables the development of flexible regulatory instruments that adapt to technological change without undermining legal certainty.

For Kazakhstan, the adoption of this paradigm is particularly relevant. As a state actively pursuing digital transformation, Kazakhstan faces the challenge of integrating artificial intelligence into public administration, healthcare, finance, and law enforcement while safeguarding constitutional rights and freedoms. Under these conditions, the legal regulation of AI should not be limited to declarative principles but must include enforceable mechanisms of accountability, transparency, and oversight. The introduction of mandatory impact assessments, algorithmic audits, and requirements for human oversight in high-risk AI systems could serve as effective tools for minimizing legal and social risks.

Thus, the development of the Kazakhstan AI Law should be based on a combination of doctrinal clarity, institutional flexibility, and a human-centered approach. Such a model would not only protect fundamental rights but also create a stable legal environment conducive to innovation and responsible technological development.

4 CONCLUSIONS

The legal aspects of AI technology are still under discussion among scientists, who have not reached consensus on issues of legal capacity and liability for harm caused by AI. To develop an effective mechanism for legal regulation of AI, it is necessary to draw on the European Union's experience, in particular by adopting certain provisions of the EU AI Law. Potential threats to human rights and freedoms in the use of AI require scientific and applied research by scientists, taking into account international legal norms. When developing national laws, they should reflect the following provisions:

- Article 17 of the Law of the Republic of Kazakhstan on AI should include in the List of Prohibited Practices Using AI predictive methods based on profiling, i.e., "predictive policing" methods, to prevent AI from predicting crimes;
- establish the status of AI as an electronic personhood with hybrid legal capacity for the purpose of distributing algorithmic liability;
- excessive regulation of AI activities should be avoided to develop promising technologies;

- a balance must be struck between AI safety and the development of innovation;
- provide for the right of citizens to file complaints against AI systems and to receive clarification of decisions regarding violated rights.

REFERENCES

1. Bryson JJ, Diamantis ME, and Grant TD, 'Of, For, and By the People: The Legal Lacuna of Synthetic Persons' (2017) 25 Artificial Intelligence and Law 273, doi:10.1007/s10506-017-9214-9
2. Calo R, 'Robotics and the Lessons of Cyberlaw' (2015) 103(3) California Law Review 513
3. Calo R, Froomkin AM, and Kerr I, *Robot Law* (Edward Elgar 2016)
4. Čerka P, Grigienė J and Sirbikytė G, 'Liability for Damages Caused by Artificial Intelligence' (2015) 31(3) Computer Law & Security Review 376, doi:10.1016/j.clsr.2015.03.008
5. Ezrachi A and Stucke ME, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard UP 2016)
6. Floridi L and Cowls J, 'A Unified Framework of Five Principles for AI in Society' (2019) 1(1) Harvard Data Science Review 2, doi:10.1162/99608f92.8cd550d1
7. Hárs A, 'AI and International Law: Legal Personality and Avenues for Regulation' (2021) 62(4) Hungarian Journal of Legal Studies 320, doi:10.1556/2052.2022.00352
8. Imangalieva A and Karashev D, 'Issues of Legal Personality of Artificial Intelligence: Responsibility of Artificial Intelligence in Kazakhstan' (*PRG*, 28 March 2024) <https://prg.kz/document/?doc_id=34826280> accessed 5 January 2026
9. Lucaj L and others, 'TechOps: Technical Documentation Templates for the AI Act' (arXiv:2508.08804v1, 12 August 2025) doi:10.48550/arXiv.2508.08804
10. Nevejans N, *European Civil Law Rules in Robotics: Study* (EU 2016)
11. Ruschemeier H, 'AI as a Challenge for Legal Regulation – The Scope of the Artificial Intelligence Act' (2023) 23(3) ERA Forum 361, doi:10.1007/s12027-022-00725-6
12. Sassòli M, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare.* (2nd edn, Edward Elgar2022)
13. Selbst AD and Barocas S, 'The Intuitive Appeal of Explainable Machines' (2018) 87(3) Fordham Law Review 1085
14. Stone P and others, 'Artificial Intelligence and Life in 2030: The One Hundred Year Study on Artificial Intelligence' (arXiv:2211.06318, 31 October 2022) doi:10.48550/arXiv.2211.06318

15. Susskind R, *Tomorrow's Lawyers: An Introduction to Your Future* (3rd edn, OUP 2023) doi:10.1093/9780192864727.001.0001

16. Truby J and others, 'A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications' (2022) 13(2) European Journal of Risk Regulation 270, doi:10.1017/err.2021.52

17. Yeung K, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12(4) Regulation & Governance 505, doi:10.1111/rego.12158

18. Zhang AH, 'The Promise and Perils of China's Regulation of Artificial Intelligence' (2025) 63 Columbia Journal of Transnational Law 1

AUTHORS INFORMATION

Yenlik Nurgaliyeva
Prof, Constitutional and Civil Law, Eurasian National University named after L.N.Gumilyov of Astana, Kazakhstan
e.nurgalieva47@gmail.com
https://orcid.org/0009-0000-9919-2951
Co-author, responsible for Conceptualization, Methodology, Supervision, Project administration, Writing – original draft.

Aruzhan Baimakhanova*
PhD, Constitutional and Civil Law, Eurasian National University named after L.N.Gumilyov of Astana, Kazakhstan
baimahanovaa10@gmail.com
https://orcid.org/0009-0002-1399-7711
Corresponding author, responsible for writing – original draft; Formal analysis, Data curation, Investigation, Writing – review & editing.

Svetlana Zharkenova
Prof, Constitutional and Civil Law, Eurasian National University named after L.N.Gumilyov of Astana, Kazakhstan
https://orcid.org/0000-0002-7305-8305
Co-author, responsible for Validation, Funding acquisition, Writing – review & editing.

Guzal Galiakbarova
PhD, Constitutional and Civil Law, Eurasian National University named after L.N.Gumilyov of Astana, Kazakhstan
galiakbarova_gg@enu.kz
https://orcid.org/0000-0001-9375-1134
Co-author, responsible for Resources, Writing – review & editing.

CO-AUTHORISHIP CONTRIBUTION

Yenlik Nurgaliyeva - Conceptualization, Methodology, Supervision, Project administration, Writing – original draft.

Aruzhan Baimakhanova - Writing – original draft, Formal analysis, Data curation, Investigation, Writing – review & editing.

Svetlana Zharkenova - Validation, Funding acquisition, Writing – review & editing

Guzal Galiakbarova - Resources, Writing – review & editing.

Competing interests: No competing interests were disclosed by authors.

Disclaimer: The authors declare that their opinions and views expressed in this manuscript are free from any impact by any organization.

RIGHTS AND PERMISSIONS

EDITORS

ABOUT THIS ARTICLE

Cite this article
Nurgaliyeva Y, Baimakhanova A, Zharkenova S and Galiakbarova G, 'Bridging the Gap: Accountability and Risk-Based Regulation in Kazakhstan's Artificial Intelligence Legislation' (2026) 9(2) Access to Justice in Eastern Europe 161-86 <https://doi.org/10.33327/AJEE-18-9.2-a000187>

DOI: https://doi.org/10.33327/AJEE-18-9.2-a000187

***Keywords*:** *Algorithmic accountability, electronic personhood, risk-based regulation, predictive policing, Kazakhstan AI Law, EU AI Act, access to justice.*

ADDITIONAL INFORMATION

The article was prepared within the framework of the project: IRN AP26198993 «Legal support for digital nomads and monitoring of current problems in the field of social and labor relations in the context of digitalization». Financing from the state budget.

DETAILS FOR PUBLICATION

Date of submission: 06 Jan 2026
Date of acceptance: 18 Feb 2026
Online First Publication: 20 March 2026
Last Publication: 20 May 2026
Was the manuscript fast tracked? - No
Number of reviewer report submitted in first round: 3 reports
Number of revision rounds: 3 rounds with major and minor revisions

Technical tools were used in the editorial process:

Plagiarism checks - Turnitin from iThenticate
https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review
https://scholasticahq.com/law-reviews

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ПОДОЛАННЯ РОЗРИВУ: ПІДЗВІТНІСТЬ ТА РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД У ЗАКОНОДАВСТВІ КАЗАХСТАНУ ПРО ШТУЧНИЙ ІНТЕЛЕКТ

Єнлік Нургалієва, Аружан Баймаханова*, Світлана Жаркенова та Гузаль Галіакбарова

АНОТАЦІЯ

Вступ. *У статті розглядаються критичні проблеми створення надійного правового режиму для штучного інтелекту (ШІ) після ухвалення Акту Європейського Союзу про штучний інтелект (2024 р.) (Акт ЄС про ШІ) та Закону Республіки Казахстан «Про штучний інтелект» (2025 р.) (Закон Казахстану про ШІ). Незважаючи на ці законодавчі зусилля, наукові дебати щодо правового статусу, правосуб'єктності та захисних функцій ШІ тривають. У дослідженні підкреслюється необхідність переходу від реактивного регулювання до превентивної, ризик-орієнтованого підходу, де правові норми адаптуються до алгоритмічної поведінки щодо виникнення конфліктів. Метою дослідження є виявлення регуляторних прогалин у казахстанській системі порівняно з європейськими стандартами, зокрема щодо захисту основних прав та судової відповідальності.*

Методи. *У статті використовується описово-аналітична та порівняльна методологія дослідження. Було проведено юридичний доктринальний аналіз Акту ЄС про ШІ та Закону Казахстану про ШІ для виявлення наявних регуляторних прогалин. Формально-правовий метод було використано для оцінки визначень ШІ та його правових характеристик. Контент-аналіз сучасної юридичної науки (2015–2025 рр.) забезпечив основу для правового моделювання статусу «електронної особи». У дослідженні також використовується системний підхід для категоризації ризиків ШІ – мінімальних, середніх та високих – у секторах державного управління та правоохоронних органів.*

Результати та висновки. *Результати демонструють, що хоча Акт ЄС про ШІ встановлює повну заборону на технології високого ризику, такі як масове біометричне спостереження та прогнозне поліцейське забезпечення, Закон Казахстану про ШІ не містить аналогічних заборон, що потенційно може призвести до дискримінаційної практики правоохоронних органів. У дослідженні було зроблено висновок, що визнання ШІ «електронною особою» з гібридною правоздатністю є важливим для того, щоб забезпечити відповідальність за автономні рішення. Запропоновано конкретні законодавчі зміни до Закону Казахстану про ШІ, зокрема: 1) обов'язкове проведення незалежних експертних оцінок для систем високого ризику; 2) заборона обміну базами даних державної таємниці через платформи ШІ; 3) встановлення алгоритмічної відповідальності для постачальників та операторів. У дослідженні наголошується, що баланс між інноваціями та цифровою відповідальністю є ключовим викликом для модернізації національного цифрового правопорядку.*

Ключові слова. *Алгоритмічна підзвітність, електронна особа, регулювання на основі ризиків, прогнозна поліція, Закон Казахстану про ШІ, Акт ЄС про ШІ, доступ до правосуддя.*