Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas

Eureka Journal of Education & Learning Technologies (EJELT)

ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

LEGAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE AND ISSUES OF LEGAL LIABILITY

Turg‘unova Shodiya Shuhratjon qizi
Senior Consultant, Department of Justice of Namangan Region
shodiya0506@icloud.com

Abstract

Background: The rapid spread of artificial intelligence (AI) in public administration, finance, healthcare, education and the media creates new legal risks: opaque automated decisions, unlawful processing of personal data, deepfakes and harm caused by autonomous systems. Traditional rules of fault-based liability are difficult to apply when harm results from a self-learning system whose behaviour was not fully foreseeable to any human.

Aim: The article analyses the main models of legal regulation of AI and identifies approaches to allocating civil, administrative and criminal liability for harm caused by its use, with particular attention to the legislation of the Republic of Uzbekistan.

Methods: The study uses comparative legal analysis of the regulatory approaches of the European Union, the United States, China, Kazakhstan and Uzbekistan, doctrinal analysis of national legislation, and a review of the scholarly debate on the “responsibility gap” and the legal personality of AI.

Results: Four regulatory models are identified: risk-based comprehensive regulation (EU), sectoral and largely voluntary governance (US), targeted administrative control of specific services (China) and an emerging “information-law” model (Uzbekistan, Kazakhstan). Uzbekistan’s Law No. ZRU-1115 of 21 January 2026 introduced a legal definition of AI, prohibited legally significant decisions affecting human rights based solely on AI outputs and established

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

administrative liability for unlawful processing of personal data using AI. Across jurisdictions, liability is attributed to humans and legal persons, not to AI itself.
Conclusion: The article proposes a risk-based classification of AI systems in Uzbek law, strict liability for operators of high-risk systems, a rebuttable presumption of causation in favour of victims, adaptation of product liability rules to software, and targeted criminal-law provisions on malicious deepfakes.

Keywords: artificial intelligence; legal regulation; legal liability; responsibility gap; AI Act; strict liability; deepfakes; personal data; Uzbekistan.

Introduction

Artificial intelligence has become one of the defining technologies of the twenty-first century. The OECD defines an AI system as a machine-based system that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments, and notes that such systems vary in their levels of autonomy and adaptiveness after deployment.[1] These very features, autonomy and the capacity to learn, make AI economically valuable and, at the same time, legally problematic.

Classical models of legal liability are built on human conduct: intent or negligence, foreseeability of consequences and a causal link between an act and the harm. When a self-learning system produces an outcome that neither its developer nor its user specifically intended or could foresee, these elements become difficult to establish. In the philosophy of technology this problem has been called the “responsibility gap”: the growing number of situations in which it is unclear who, if anyone, can fairly be held responsible for the actions of

[1] OECD. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Adopted 22 May 2019, amended 3 May 2024.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

learning machines.[2] For victims, the practical result may be that harm remains uncompensated; for society, that trust in technology is undermined.

The international community has responded with soft-law instruments and, more recently, binding rules. UNESCO adopted the Recommendation on the Ethics of Artificial Intelligence in 2021,[3] the UN General Assembly adopted its first resolution on safe, secure and trustworthy AI systems in March 2024,[4] and the Council of Europe opened for signature in September 2024 the first international treaty in this field, the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.[5] The European Union adopted the comprehensive Artificial Intelligence Act in 2024.

Uzbekistan is actively integrating AI into its economy and public administration. Resolution of the President No. PQ-358 of 14 October 2024 approved the Strategy for the Development of Artificial Intelligence Technologies until 2030, with targets that include raising the volume of AI-based software products and services to 1.5 billion US dollars and the share of AI-based services on the Single Portal of Interactive Public Services to 10 per cent.[6] Decree of the President No. PF-189 of 22 October 2025 provided for at least 100 AI projects in public administration, the social sphere and the economy by the end of 2026.[7] Legal regulation followed with the Law No. ZRU-1115 of 21 January 2026.[8] The expanding use of AI therefore makes the question of liability practically urgent for Uzbek law.

[2] Matthias A. The responsibility gap: ascribing responsibility for the actions of learning automata // Ethics and Information Technology. 2004. Vol. 6, No. 3. P. 175–183.
[3] UNESCO. Recommendation on the Ethics of Artificial Intelligence. Adopted 23 November 2021.
[4] United Nations General Assembly. Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development. UN Doc. A/RES/78/265, 21 March 2024.
[5] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. CETS No. 225. Vilnius, 5 September 2024.
[6] Resolution of the President of the Republic of Uzbekistan "On the approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030" of 14 October 2024, No. PQ-358. URL: https://lex.uz/docs/-7158604; see also: https://gov.uz/en/digital/news/view/24510.
[7] Decree of the President of the Republic of Uzbekistan "On additional measures for the further development of artificial intelligence technologies" of 22 October 2025, No. PF-189. URL: https://gov.uz/oz/digital/news/view/96074.
[8] Law of the Republic of Uzbekistan of 21 January 2026, No. ZRU-1115; see: Qonunni algoritm yozsa, javobgar kim bo'ladi? // UzA. URL: https://uza.uz/ar/posts/qonunni-algoritm-yozsa-javobgar-kim-boladi_914229.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

The aim of this article is to analyse the main models of legal regulation of AI and to identify approaches to allocating legal liability for harm caused by its use, with proposals for the development of Uzbek legislation. The objectives are: (1) to compare the leading regulatory models; (2) to analyse the current Uzbek framework; (3) to evaluate the theoretical approaches to liability, including the idea of AI legal personality; and (4) to formulate recommendations. The research question is how liability for AI-related harm should be allocated so as to protect victims effectively without stifling innovation.

Methods

The study is a qualitative legal analysis that combines three methods.

Comparative legal analysis: Five jurisdictions were selected to represent different regulatory philosophies: the European Union (Regulation (EU) 2024/1689, the AI Act, and Directive (EU) 2024/2853 on liability for defective products);[9] the United States (federal executive policy and state legislation); China (the Interim Measures for the Management of Generative AI Services and related rules);[10] Kazakhstan, as a neighbouring post-Soviet system that adopted a dedicated AI law in 2025;[11] and Uzbekistan. For each jurisdiction, four parameters were compared: the scope of regulation, the method (risk-based, sectoral or service-specific), the main obligations of actors and the liability consequences of non-compliance.

Doctrinal (formal-legal) analysis: The Uzbek framework was examined on the basis of the Law No. ZRU-1115 of 21 January 2026, which amended the Law "On Informatization" and the Code of Administrative Responsibility, the Civil Code (general rules on liability for harm, including harm caused by a source of

[9] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. L series. 12 July 2024.

[10] Cyberspace Administration of China et al. Interim Measures for the Management of Generative Artificial Intelligence Services (in force 15 August 2023); Measures for Labelling Artificial Intelligence-Generated Synthetic Content (in force 1 September 2025).

[11] Qozog'istonda SIni tartibga soluvchi qonun yaratildi: Deepfeyk taqiqlandi // Anhor.uz. URL: https://anhor.uz/uzl/world/qozogistondasini-tartibga/.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

increased danger), the Law "On Personal Data" of 2 July 2019 No. ZRU-547, and the strategic acts PQ-358 and PF-189. Texts were obtained from the National Database of Legislation (lex.uz) and official portals.

Theoretical analysis: The scholarly debate on the responsibility gap, on the possible legal personality of AI and on the choice between fault-based, strict and product liability was reviewed, including the report of the EU Expert Group on Liability and New Technologies.[12][13]

Limitations:

AI regulation is changing rapidly; the analysis reflects sources available as of October 2026. Uzbek case law on AI-related harm is not yet publicly available, so the evaluation of the national framework is based on legislation rather than on judicial practice.

Results

The comparative analysis identified four models of AI regulation. Their key features are summarised in Table 1 and described below.

Table 1. Comparative models of legal regulation of AI

Jurisdiction	Model	Core instruments	Main obligations	Liability approach
European Union	Comprehensive, risk-based	AI Act (Regulation (EU) 2024/1689); Product Liability Directive (EU) 2024/2853	Prohibited practices; conformity, risk management and human oversight for high-risk systems; transparency for deepfakes and chatbots	Administrative fines up to EUR 35 million or 7% of worldwide turnover; strict product liability extended to software
United States	Sectoral, largely voluntary at federal level	Executive policy; state laws (e.g., Colorado SB 24-205)	Varies by sector and state; anti-discrimination duties for high-risk systems in Colorado	Existing tort, product liability and consumer protection law

[12] Expert Group on Liability and New Technologies – New Technologies Formation. Liability for Artificial Intelligence and Other Emerging Digital Technologies. Luxembourg: Publications Office of the European Union, 2019.

[13] Bryson J.J., Diamantis M.E., Grant T.D. Of, for, and by the people: the legal lacuna of synthetic persons // Artificial Intelligence and Law. 2017. Vol. 25, No. 3. P. 273–291.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

Jurisdiction	Model	Core instruments	Main obligations	Liability approach
China	Targeted administrative control of services	Interim Measures on Generative AI Services (2023); labelling rules (2025)	Content security, training data legality, labelling of synthetic content	Administrative sanctions; providers responsible as content producers
Kazakhstan	Information-law model	Dedicated AI law (2025)	Labelling of AI-generated products; risk management by owners and users	Owners and users responsible; AI treated as a tool
Uzbekistan	Information-law model (emerging)	Law No. ZRU-1115 (2026); Strategy PQ-358 (2024)	Human-made legally significant decisions; personal data protection	Administrative fines; general civil-law liability

Source: compiled by the author.

European Union: risk-based regulation and product liability: The AI Act, which entered into force on 1 August 2024, classifies AI systems by the level of risk they pose.[14] Practices considered an unacceptable risk, such as social scoring and certain manipulative techniques, have been prohibited since 2 February 2025. High-risk systems, including those used in employment, education, access to essential services, law enforcement and the administration of justice, are subject to requirements on risk management, data governance, technical documentation, transparency, human oversight, accuracy and cybersecurity. Providers of general-purpose AI models have had specific obligations since 2 August 2025, and most other provisions were scheduled to apply from 2 August 2026; in November 2025 the European Commission proposed a "digital omnibus" package that would adjust the timetable for some high-risk obligations. Users must be informed when they interact with an AI system, and deepfakes must be disclosed as artificially generated. Fines for prohibited practices can reach EUR 35 million or 7 per cent of total worldwide annual turnover, whichever is higher.

On liability, the new Product Liability Directive expressly treats software, including AI systems, as a product. It eases the burden of proof for victims

[14] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. L series. 12 July 2024.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

through court-ordered disclosure of evidence and rebuttable presumptions of defectiveness and causation where technical or scientific complexity makes proof excessively difficult; member states must transpose it by 9 December 2026.[15] By contrast, the proposed AI Liability Directive, which would have harmonised fault-based claims, was withdrawn: the Commission announced its withdrawal in its 2025 work programme.[16]

United States: sectoral governance: The United States has no comprehensive federal AI statute. Executive Order 14110 of October 2023 on safe, secure and trustworthy AI was revoked in January 2025, and federal policy has since emphasised innovation, as reflected in the AI Action Plan of July 2025.[17] Regulation develops at state level: Colorado's Senate Bill 24-205 of 2024 became the first comprehensive state law imposing duties on developers and deployers of high-risk AI systems to prevent algorithmic discrimination.[18] Liability for AI-related harm is resolved mainly through existing tort, product liability and consumer protection law.

China and Kazakhstan: service-specific and information-law models: China regulates specific AI services through administrative measures. The Interim Measures for the Management of Generative AI Services, in force since 15 August 2023, require providers to ensure lawful training data, prevent illegal content and label generated content, and treat providers as responsible for the content produced.[19] Measures on labelling AI-generated synthetic content took effect on 1 September 2025. Kazakhstan's AI law of 2025 treats AI systems as

[15] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.
[16] European Commission. Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). COM(2022) 496 final, 28 September 2022; European Commission. Commission Work Programme 2025, Annex IV (withdrawals). 11 February 2025.
[17] Executive Order 14110 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence", 30 October 2023; Executive Order 14179 "Removing Barriers to American Leadership in Artificial Intelligence", 23 January 2025; The White House. America's AI Action Plan. July 2025.
[18] Colorado Senate Bill 24-205 "Consumer Protections for Artificial Intelligence" (2024).
[19] Cyberspace Administration of China et al. Interim Measures for the Management of Generative Artificial Intelligence Services (in force 15 August 2023); Measures for Labelling Artificial Intelligence-Generated Synthetic Content (in force 1 September 2025).

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

objects of informatization and tools for achieving human-defined goals, not as independent legal subjects; owners and users bear responsibility for their use and safety, and AI-generated products must be labelled.[20]

Uzbekistan: the emerging national framework: The Law No. ZRU-1115 of 21 January 2026 introduced the core of AI regulation into the Law "On Informatization".[21] It defines artificial intelligence as a set of technological solutions that make it possible to imitate human knowledge and skills, to learn independently, to search for solutions and to perform specific tasks with results comparable to those of human intellectual activity. It establishes the general basis for using AI technologies and clarifies the powers of the authorised state body. A key provision is that legally significant decisions concerning human rights and freedoms may not rely solely on the conclusions of information systems operating on AI-based technologies.[22] The draft law also provided for mandatory labelling of information resources created with AI.[23]

On liability, the Law added to the Code of Administrative Responsibility a provision on the unlawful processing of personal data using AI, or its dissemination through the mass media, telecommunications networks or the internet. The sanction is a fine of 50 to 100 times the base calculation amount, with confiscation of the instruments of the offence.[24] During parliamentary discussion, the drafters explained that they deliberately chose administrative rather than criminal liability at this stage so as not to discourage young innovators, while noting that criminal-law amendments were being considered.[25]

[20] Qozog'istonda SIni tartibga soluvchi qonun yaratildi: Deepfeyk taqiqlandi // Anhor.uz. URL: https://anhor.uz/uzl/world/qozogistondasini-tartibga/.
[21] Law of the Republic of Uzbekistan of 21 January 2026, No. ZRU-1115; see: Qonunni algoritm yozsa, javobgar kim bo'ladi? // UzA. URL: https://uza.uz/ar/posts/qonunni-algoritm-yozsa-javobgar-kim-boladi_914229.
[22] Sun'iy intellekt yordamida shaxsga doir ma'lumotlarga noqonuniy ishlov berganlik uchun javobgarlik belgilandi // Spot.uz. 21 January 2026. URL: https://www.spot.uz/oz/2026/01/21/ai-liability/.
[23] Uzbekistan takes steps to regulate AI with new legislation // Kun.uz. 16 April 2025. URL: https://kun.uz/en/news/2025/04/16/uzbekistan-takes-steps-to-regulate-ai-with-new-legislation.
[24] Sun'iy intellekt yordamida shaxsga doir ma'lumotlarga noqonuniy ishlov berganlik uchun javobgarlik belgilandi // Spot.uz. 21 January 2026. URL: https://www.spot.uz/oz/2026/01/21/ai-liability/.
[25] MPs defend AI regulation bill, stress soft approach over harsh punishments // Kun.uz. 21 April 2025. URL: https://kun.uz/en/news/2025/04/21/mps-defend-ai-regulation-bill-stress-soft-approach-over-harsh-punishments.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

Civil liability for AI-related harm is not regulated specifically and therefore falls under the general rules of the Civil Code, including liability for harm caused by a source of increased danger, which applies regardless of fault.

Discussion

Should AI itself bear liability?: The most radical answer to the responsibility gap is to grant AI a form of legal personality. In 2017 the European Parliament invited the Commission to consider creating, in the long run, a specific legal status of "electronic persons" for the most sophisticated autonomous robots.[26] The proposal was widely criticised. Bryson, Diamantis and Grant argued that electronic personhood would allow humans to shield themselves from responsibility behind synthetic persons that lack assets, interests and the capacity to be deterred.[27] The EU Expert Group on Liability and New Technologies concluded in 2019 that it is not necessary to give autonomous systems legal personality, because harm they cause can and should be attributed to existing persons or bodies.[28]

The results confirm that legislators have followed this view. None of the jurisdictions studied recognises AI as a subject of law. Kazakhstan expressly treats AI as a tool for achieving human-defined goals, and Uzbekistan's Law No. ZRU-1115 frames AI as a set of technological solutions whose outputs cannot alone determine decisions on human rights.[29][30] This position is also sound from the standpoint of legal theory: legal liability presupposes a subject capable of understanding norms and bearing sanctions, which AI currently is not.

[26] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), para. 59(f).
[27] Bryson J.J., Diamantis M.E., Grant T.D. Of, for, and by the people: the legal lacuna of synthetic persons // Artificial Intelligence and Law. 2017. Vol. 25, No. 3. P. 273–291.
[28] Expert Group on Liability and New Technologies – New Technologies Formation. Liability for Artificial Intelligence and Other Emerging Digital Technologies. Luxembourg: Publications Office of the European Union, 2019.
[29] Qozog'istonda SIni tartibga soluvchi qonun yaratildi: Deepfeyk taqiqlandi // Anhor.uz. URL: https://anhor.uz/uzl/world/qozogistondasini-tartibga/.
[30] Sun'iy intellekt yordamida shaxsga doir ma'lumotlarga noqonuniy ishlov berganlik uchun javobgarlik belgilandi // Spot.uz. 21 January 2026. URL: https://www.spot.uz/oz/2026/01/21/ai-liability/.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

The same reasoning applies to criminal law. Hallevy has proposed models under which AI could be treated as an innocent agent, as a source of natural and probable consequences, or even as a direct offender.[31] However, criminal liability in Uzbek law, as in most legal systems, is based on the principle of guilt, which requires intent or negligence of a natural person. When AI is used as an instrument, for example to produce a deepfake for fraud, the existing offences already apply to the person who used it, such as fraud under Article 168 of the Criminal Code. The real gap concerns cases where harm is caused by a system that no one intended to misuse; such cases are better handled by civil law than by criminal punishment.

Allocating civil liability among human actors: An AI system involves many actors: the developer of the model, the provider who places a system on the market, the deployer who uses it professionally, the data supplier and the end user. Fault-based liability requires the victim to identify which of them acted negligently and to prove causation through an opaque, self-learning process. As Matthias observed, the more a system learns in operation, the weaker the control of its creators over its behaviour, and the harder it becomes to ascribe fault.[32] Pagallo similarly showed that AI disperses responsibility across a network of human and organisational actors.[33]

Three complementary instruments emerge from the comparative analysis. First, product liability, as in the EU Directive of 2024, makes producers liable for defective software without proof of fault and eases proof through presumptions.[34] Second, strict liability for operators of AI systems that create a significant risk of harm to the public, which the EU Expert Group recommended by analogy with

[31] Hallevy G. Liability for Crimes Involving Artificial Intelligence Systems. Cham: Springer, 2015.
[32] Matthias A. The responsibility gap: ascribing responsibility for the actions of learning automata // Ethics and Information Technology. 2004. Vol. 6, No. 3. P. 175–183.
[33] Pagallo U. The Laws of Robots: Crimes, Contracts, and Torts. Dordrecht: Springer, 2013.
[34] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

motor vehicles.[35] Third, procedural tools, such as disclosure of evidence and rebuttable presumptions of causation, which keep fault-based liability workable for lower-risk systems.

In Uzbekistan, the rule on liability for harm caused by a source of increased danger could, in principle, be applied to some AI uses, such as autonomous vehicles or industrial robots. Its application to purely software-based systems, such as credit scoring or recruitment algorithms, is uncertain, and leaving this question to courts case by case reduces legal certainty for both victims and businesses.

Assessment of the Uzbek framework: The Law No. ZRU-1115 is a significant first step. Its strongest element is the rule that legally significant decisions affecting human rights may not rely solely on AI outputs. This corresponds to the human oversight requirement of the AI Act and to the right not to be subject to solely automated decisions in European data protection law. To be effective, however, the rule needs procedural guarantees: a right to be informed that AI was used, a right to an explanation and a right to contest the decision before a human.

The framework also has gaps. First, administrative liability is limited to the unlawful processing and dissemination of personal data; failure to label AI-generated content, discriminatory automated decisions and breach of the human-decision rule are not sanctioned as such. Second, the Code of Administrative Responsibility is traditionally oriented to natural persons and officials, while most AI systems are developed and deployed by companies; corporate accountability therefore remains weak. Third, there is no classification of AI systems by risk, so the same general rules apply to a chatbot and to a system used in courts or healthcare. The drafters' caution about over-regulation is reasonable,[36] and

[35] Expert Group on Liability and New Technologies – New Technologies Formation. Liability for Artificial Intelligence and Other Emerging Digital Technologies. Luxembourg: Publications Office of the European Union, 2019.

[36] MPs defend AI regulation bill, stress soft approach over harsh punishments // Kun.uz. 21 April 2025. URL: https://kun.uz/en/news/2025/04/21/mps-defend-ai-regulation-bill-stress-soft-approach-over-harsh-punishments.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

Chesterman has warned against regulating too early or too broadly.[37] Yet the targets of Strategy PQ-358 and Decree PF-189, which envisage AI in public services, healthcare and courts, mean that high-risk uses are arriving quickly, and liability rules should keep pace.

Conclusion and recommendations

The study shows that four models of AI regulation have emerged: the comprehensive risk-based model of the European Union, the sectoral model of the United States, the service-specific administrative model of China and the information-law model adopted by Kazakhstan and, since 2026, by Uzbekistan. Despite their differences, all of them share one principle: AI is not a subject of law, and liability for its use is borne by natural and legal persons who develop, place on the market, deploy or use it.

Uzbekistan has laid the foundation of its AI law through the Strategy PQ-358, Decree PF-189 and Law No. ZRU-1115. The legal definition of AI, the rule that decisions on human rights must not rest solely on AI outputs and administrative liability for AI-based misuse of personal data are important achievements. The answer to the research question, however, is that effective protection of victims requires a more differentiated liability system, while innovation is best protected by legal certainty rather than by the absence of rules. The following measures are proposed:

1. Introduce a risk-based classification of AI systems in the Law “On Informatization” or in a separate law, distinguishing prohibited uses, high-risk systems (public administration, justice, healthcare, education, employment, finance) and other systems, with obligations proportionate to risk.

[37] Chesterman S. We, the Robots? Regulating Artificial Intelligence and the Limits of the Law. Cambridge: Cambridge University Press, 2021.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

2. Establish strict liability for operators of high-risk AI systems in the Civil Code, with compulsory liability insurance for the most dangerous uses, while retaining fault-based liability for other systems.
3. Introduce a rebuttable presumption of causation and a court-ordered disclosure of evidence in favour of persons harmed by AI, where technical complexity makes proof excessively difficult.
4. Adapt product liability and consumer protection rules so that software and AI systems are expressly recognised as products and services whose defects give rise to liability.
5. Expand administrative liability and extend it to legal persons, covering failure to label AI-generated content, breach of the human-decision rule and discriminatory automated decisions.
6. Provide procedural guarantees for persons affected by AI-assisted decisions: notification of AI use, a right to an explanation and a right to human review.
7. Adopt targeted criminal-law provisions on the creation and dissemination of malicious deepfakes that damage honour and dignity, interfere with elections or facilitate fraud.

Further research should address AI use in the justice system, liability in AI supply chains involving foreign developers, and the compatibility of Uzbek legislation with the Council of Europe Framework Convention on Artificial Intelligence.

References

Legal acts of the Republic of Uzbekistan
1. Law of the Republic of Uzbekistan of 21 January 2026, No. ZRU-1115 (amendments to the Law “On Informatization” and the Code of Administrative Responsibility in connection with the regulation of relations arising from the use of artificial intelligence).
2. Law of the Republic of Uzbekistan “On Personal Data” of 2 July 2019, No. ZRU-547.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

3. Civil Code of the Republic of Uzbekistan.
4. Criminal Code of the Republic of Uzbekistan.
5. Code of the Republic of Uzbekistan on Administrative Responsibility.
6. Resolution of the President of the Republic of Uzbekistan "On the approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030" of 14 October 2024, No. PQ-358. URL: https://lex.uz/docs/-7158604
7. Decree of the President of the Republic of Uzbekistan "On additional measures for the further development of artificial intelligence technologies" of 22 October 2025, No. PF-189.
Foreign and international legal acts
8. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
9. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products.
10. European Commission. Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence. COM(2022) 496 final, 28 September 2022.
11. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).
12. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. CETS No. 225. Vilnius, 5 September 2024.
13. Executive Order 14110 of 30 October 2023 (United States); Executive Order 14179 of 23 January 2025 (United States).
14. Colorado Senate Bill 24-205 "Consumer Protections for Artificial Intelligence" (2024).
15. Interim Measures for the Management of Generative Artificial Intelligence Services (People's Republic of China, 2023).

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

16. Measures for Labelling Artificial Intelligence-Generated Synthetic Content (People's Republic of China, 2025).
International soft-law instruments and reports
17. OECD. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. 2019, amended 2024.
18. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris, 2021.
19. United Nations General Assembly. Resolution A/RES/78/265, 21 March 2024.
20. Expert Group on Liability and New Technologies – New Technologies Formation. Liability for Artificial Intelligence and Other Emerging Digital Technologies. Luxembourg: Publications Office of the European Union, 2019.
21. The White House. America's AI Action Plan. Washington, July 2025.
Scholarly literature
22. Bryson J.J., Diamantis M.E., Grant T.D. Of, for, and by the people: the legal lacuna of synthetic persons // Artificial Intelligence and Law. 2017. Vol. 25, No. 3. P. 273–291.
23. Chesterman S. We, the Robots? Regulating Artificial Intelligence and the Limits of the Law. Cambridge: Cambridge University Press, 2021.
24. Hallevy G. Liability for Crimes Involving Artificial Intelligence Systems. Cham: Springer, 2015.
25. Matthias A. The responsibility gap: ascribing responsibility for the actions of learning automata // Ethics and Information Technology. 2004. Vol. 6, No. 3. P. 175–183.
26. Pagallo U. The Laws of Robots: Crimes, Contracts, and Torts. Dordrecht: Springer, 2013.
Official portals and media sources
27. Spot.uz. Sun'iy intellekt yordamida shaxsga doir ma'lumotlarga noqonuniy ishlov berganlik uchun javobgarlik belgilandi. 21 January 2026.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

28. UzA. Qonunni algoritm yozsa, javobgar kim bo‘ladi?
29. Kun.uz. Uzbekistan takes steps to regulate AI with new legislation. 16 April 2025.
30. Kun.uz. MPs defend AI regulation bill, stress soft approach over harsh punishments. 21 April 2025.
31. Anhor.uz. Qozog‘istonda SIni tartibga soluvchi qonun yaratildi: Deepfeyk taqiqlandi.
32. Ministry of Digital Technologies of the Republic of Uzbekistan. Official news on PQ-358 and PF-189. URL: https://gov.uz/en/digital