International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 5, Issue 5, May - 2026
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

Issues of Civil Liability for Damage Caused by Artificial Intelligence Systems in the Fintech Sector

Abdurakhmonova Noila Kuvondik qizi
Doctoral Student (PhD) at Tashkent State University of Law
nobeln1908@gmail.com



Abstract:
The article examines theoretical and practical issues of civil liability for damage caused by artificial intelligence systems in the financial technology (fintech) sector. It argues that the autonomy, self-learning and "black box" nature of AI complicate the application of traditional tort-law concepts of fault, causation and burden of proof. Based on a comparative analysis of the European Union, the United States, the United Kingdom and Singapore, as well as foreign scholarship, the article proposes measures to improve the civil legislation of the Republic of Uzbekistan.

Keywords: Artificial intelligence, fintech, civil liability, damage, source of increased danger, strict liability, credit scoring, burden of proof.

Introduction

Annotatsiya

Maqolada moliyaviy texnologiyalar (fintex) sohasida sun'iy intellekt tizimlari yetkazgan zarar uchun fuqarolik-huquqiy javobgarlikning nazariy va amaliy masalalari tahlil qilinadi. Sun'iy intellektning avtonomligi, o'z-o'zidan o'rganishi va "qora quti" xususiyati an'anaviy delikt huquqining ayb, sababiy bog'lanish va isbotlash yukiga oid konstruksiyalarini qo'llashni murakkablashtirishi asoslanadi. Yevropa Ittifoqi, AQSh, Buyuk Britaniya va Singapur tajribasi hamda xorijiy ilmiy adabiyotlar qiyosiy o'rganilib, O'zbekiston Respublikasi fuqarolik qonunchiligini takomillashtirish bo'yicha takliflar ishlab chiqilgan.

Kalit so'zlar: sun'iy intellekt, fintex, fuqarolik-huquqiy javobgarlik, zarar, yuqori xavf manbai, aybsiz javobgarlik, kredit skoring, isbotlash yuki.

Аннотация

В статье анализируются теоретические и практические вопросы гражданско-правовой ответственности за вред, причинённый системами искусственного интеллекта в сфере финансовых технологий (финтех). Обосновывается, что автономность, самообучение и эффект «чёрного ящика» затрудняют применение традиционных деликтных конструкций

вины, причинной связи и бремени доказывания. На основе сравнительного анализа опыта Европейского союза, США, Великобритании и Сингапура, а также зарубежной доктрины предложены меры по совершенствованию гражданского законодательства Республики Узбекистан.

Ключевые слова: искусственный интеллект, финтех, гражданско-правовая ответственность, вред, источник повышенной опасности, безвиновная ответственность, кредитный скоринг, бремя доказывания.

Introduction

The financial technology (fintech) sector is one of the areas where artificial intelligence (AI) systems are being introduced most rapidly. Today, credit scoring, anti-fraud monitoring, customer identification, algorithmic trading, automated investment advice (robo-advisors) and customer service chatbots all operate on the basis of AI. This process is also actively under way in Uzbekistan: the Strategy for the Development of AI Technologies until 2030 was approved by Presidential Resolution No. PQ-358 of 14 October 2024[1], the Central Bank has launched a credit platform based on AI scoring and is developing a fintech development strategy for 2026–2030 [2]. However, the use of AI systems gives rise to new types of damage: unjustified refusal of credit as a result of erroneous scoring, blocking of an account or failure of a payment due to an error of an anti-fraud system, market-destabilising behaviour of an algorithmic trading system, discriminatory decisions, and unlawful processing of personal data. The issue of compensation for such damage, however, is not sufficiently regulated by law. Although Law No. ZRU-1115 adopted in Uzbekistan on 21 January 2026 introduced the concept of AI into legislation and established administrative liability [3], a special mechanism of civil liability still does not exist. Therefore, research into this issue on the basis of scholarship and foreign experience is of topical importance. There are various scholarly approaches to the theoretical and practical issues of civil liability for damage caused by artificial intelligence systems.

Classical tort law requires four conditions for compensation of damage: an unlawful act, damage, a causal link between them, and the fault of the tortfeasor. Three features of AI systems complicate the application of this construction. First, owing to autonomy and the capacity for self-learning, a specific decision of the system may not have been pre-programmed by the developer. Second, the "black box" (opacity) effect: even the developer cannot fully explain on what basis a model built on deep neural networks has made a decision. Third, the multiplicity of actors: the developer who created the model, the data supplier who trained it, the financial institution that deployed the system (the operator) and the cloud infrastructure provider all participate in the occurrence of damage. As a result, the injured party faces almost insurmountable difficulties in identifying the person at fault and proving causation. A. Matthias called this situation a "responsibility gap"[4].

[1] Resolution of the President of the Republic of Uzbekistan "On Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030", No. PQ-358 of 14.10.2024.
[2] The Central Bank has created a credit platform using AI-based scoring // Spot.uz, 25.08.2026; The Central Bank is developing a fintech development strategy until 2030 // Anhor.uz, 2025.
[3] Law of the Republic of Uzbekistan No. ZRU-1115 of 21 January 2026 "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Regulation of Relations Arising from the Use of Artificial Intelligence" // lex.uz.
[4] Matthias A. The responsibility gap: Ascribing responsibility for the actions of learning automata // Ethics and Information Technology. – 2004. – Vol. 6. – P. 175–183.

Three main models for solving this problem have emerged in foreign doctrine.

The first model – retaining fault-based liability while shifting the burden of proof from the injured party to the AI operator or manufacturer.

The second model – strict (no-fault) liability: the AI system is treated as a product or a source of increased danger, and the person who benefits from it compensates the damage regardless of fault. Substantiating this approach, G. Wagner emphasises that it is economically efficient to place risks on the actor who benefits from them and can manage them at the lowest cost[5]; H. Zech likewise assesses strict liability, from a public policy perspective, as a tool that does not hinder innovation but, on the contrary, increases trust[6]. The 2019 report of the European Commission's expert group also recommended strict liability for operators of high-risk AI[7].

The third model – the idea of granting an AI system the status of an "electronic person", which was put forward in the European Parliament resolution of 2017, but was later reasonably criticised and rejected by scholars such as A. Bertolini[8] and S. Chesterman[9]: imposing liability on software that is not a legal subject deprives the injured party of real compensation. M. Lemley and B. Casey, in turn, propose combining "compensation and correction" remedies for AI instead of traditional sanctions[10].

Let us analyse the theoretical and practical issues of civil liability for damage caused by artificial intelligence systems on the basis of foreign experience. In international legislation, this issue has been addressed on the basis of various approaches.

European Union. The EU has created the most consistent regulatory framework. Regulation 2024/1689 (the AI Act) classifies systems for assessing the creditworthiness of natural persons and credit scoring, as well as risk assessment systems in life and health insurance, as "high-risk" and sets requirements for them concerning risk management, data quality, human oversight and transparency[11].

Civil liability, in turn, is governed by Directive 2024/2853 of 23 October 2024 (the new Product Liability Directive): under it, software and AI systems are recognised as a "product", the AI provider is deemed a manufacturer and is liable without fault for damage caused by a defective product; failure to install necessary security updates is also regarded as a defect. The Directive provides for mechanisms to ease the burden of proof – an obligation to disclose evidence at the request of the court, as well as presumptions of defectiveness and causation – and applies to

[5] Wagner G. Robot Liability // Liability for Artificial Intelligence and the Internet of Things / eds. S. Lohsse, R. Schulze, D. Staudenmayer. – Baden-Baden: Nomos, 2019. – P. 27–62.
[6] Zech H. Liability for AI: public policy considerations // ERA Forum. – 2021. – Vol. 22. – P. 147–158.
[7] Expert Group on Liability and New Technologies – New Technologies Formation. Liability for Artificial Intelligence and other emerging digital technologies. – Brussels: European Commission, 2019. – 65 p.
[8] Bertolini A. Artificial Intelligence and Civil Liability. Study requested by the JURI Committee of the European Parliament. – Brussels, 2020. – 132 p.
[9] Chesterman S. We, the Robots? Regulating Artificial Intelligence and the Limits of the Law. – Cambridge: Cambridge University Press, 2021. – 310 p.
[10] Lemley M.A., Casey B. Remedies for Robots // University of Chicago Law Review. – 2019. – Vol. 86, No. 5. – P. 1311–1396.
[11] 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) // OJ L, 12.07.2024.

products placed on the market from 9 December 2026[12]. The draft AI Liability Directive (2022), which was expected to introduce a presumption of causation for fault-based claims, was withdrawn by the Commission on 11 February 2025 because no agreement was reached among the Member States[13]. Therefore, product liability and national tort law currently remain the main instruments in the EU. What is important for fintech is that Directive 2024/2853 covers only damage to the life, health, property and data of a natural person; pure economic loss suffered as a result of a credit refusal or incorrect investment advice falls outside its scope. This gap should be filled by national legislation.

USA. In the USA, there is no special federal law on AI liability; the common-law institutions of negligence and product liability, as well as sector-specific rules, apply. The most important mechanism for fintech is the Equal Credit Opportunity Act (ECOA) and Regulation "B", which require a creditor, when taking an adverse decision, to state its specific and principal reasons. In its Circulars 2022-03 and 2023-03, the Consumer Financial Protection Bureau (CFPB) firmly established that the use of AI or complex algorithms does not relieve a creditor of this obligation, and that limiting oneself to generic template reasons constitutes a violation of the law [14]. Although this approach does not directly establish liability, through transparency it enables the injured party to obtain the evidence necessary for a civil claim. At the state level, the Colorado AI Act of 2024 (SB 24-205) classifies financial services as "consequential decisions" and establishes a duty of care to prevent algorithmic discrimination.

United Kingdom and Singapore. These countries are following the path of "technological neutrality" and adapting existing regulatory tools. In the United Kingdom, the 2022 Discussion Paper DP5/22 of the Bank of England, the PRA and the FCA, instead of a separate liability regime for AI, requires the clear designation of a person responsible for AI within a financial institution through the personal accountability regime for senior executives (Senior Managers Regime)[15]. The FEAT principles (fairness, ethics, accountability, transparency) adopted by the Monetary Authority of Singapore (MAS) in 2018 require internal accountability of the institution for AI decisions and the ability to explain the reasons for a decision to the customer[16]. These "soft law" instruments are used by courts in determining the standard of care and, in practice, are strengthening fault-based liability.

If we examine this issue on the basis of the legislation of our country, it is addressed in our legal system as follows.

The Civil Code of the Republic of Uzbekistan (CC) contains several general constructions that may be applied to damage caused by AI[17]. Article 985 of the CC, establishing the general grounds

[12] 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 // OJ L, 18.11.2024.
[13] European Commission. Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). COM(2022) 496 final; withdrawn by the Commission Work Programme 2025, 11.02.2025.
[14] Consumer Financial Protection Bureau. Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms (26.05.2022); Circular 2023-03: Adverse action notification requirements and the proper use of the CFPB's sample forms provided in Regulation B (19.09.2023).
[15] Bank of England, Prudential Regulation Authority, Financial Conduct Authority. Artificial Intelligence and Machine Learning. Discussion Paper DP5/22. – London, 2022.
[16] Monetary Authority of Singapore. Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector. – Singapore: MAS, 2018.
[17] Civil Code of the Republic of Uzbekistan (29 August 1996, No. 257-I) // National Database of Legislation: lex.uz/acts/-111189.

for causing damage, provides for a presumption of the tortfeasor's fault: the tortfeasor is released from liability if they prove the absence of fault. Article 999 of the CC establishes no-fault liability for damage caused by a source of increased danger, while Articles 1017–1020 provide that damage caused by defects in goods, works or services shall be compensated by the seller or manufacturer regardless of fault. In contractual relations, under Article 333 of the CC, a person carrying out entrepreneurial activity is liable for breach of an obligation regardless of fault unless they prove that the breach occurred as a result of force majeure.

An analysis of the application of these rules to AI-related damage reveals the following problems. **First,** the question of recognising an AI system as a source of increased danger is debatable. Although the list in Article 999 of the CC is open, judicial practice identifies a source of increased danger on the basis of the harmful properties of an object and the impossibility of full human control over it. Credit scoring or chatbot systems in fintech do not pose a physical danger; therefore, applying Article 999 to them is not justified; this rule may be discussed only in relation to high-risk solutions such as autonomous algorithmic trading systems.

Second, the concept of "defect" in Article 1017 of the CC is designed for a static product and is not adapted to a software product that learns by itself and changes after being placed on the market; the status of software as a good or a service is also not clearly defined by law. Third, the issue of the burden of proof: under civil procedural legislation, each party must prove its claims and objections, yet the customer has no access to the internal logic of the algorithm, and there is no special mechanism compelling the disclosure of evidence. Fourth, standard-form contracts of banks and payment institutions widely contain clauses limiting or excluding liability for technical errors, and their validity with respect to consumers is not clearly regulated.

At the same time, Law No. ZRU-1115 created an important basic rule for civil liability: it prohibits making legally significant decisions affecting human rights and freedoms solely on the basis of the output of an AI system [18]. A breach of this prohibition (for example, refusing credit solely on the basis of an algorithm without human involvement) may be used to prove the unlawfulness of the conduct. The Ethics Rules approved by Order No. 3787 of the Minister of Digital Technologies of 14 March 2026 establish the principles of reliability, safety and human oversight [19], creating normative criteria that may be used by courts in determining the standard of care. However, these documents do not establish a special mechanism for compensation of damage.

Based on the foregoing, by way of conclusion, the following proposals can be put forward.

First, to supplement Chapter 57 of the CC with a special article on "Liability for damage caused as a result of the use of an artificial intelligence system" and to enshrine a differentiated approach in it: a financial institution that is the operator of high-risk AI (credit scoring, anti-fraud, algorithmic trading) compensates damage regardless of fault and has a right of recourse against

[18] Law of the Republic of Uzbekistan No. ZRU-1115 of 21 January 2026 "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Regulation of Relations Arising from the Use of Artificial Intelligence" // lex.uz.
[19] Rules of Ethics for the Development, Implementation and Use of AI-based Solutions: approved by Order No. 3787 of the Minister of Digital Technologies of the Republic of Uzbekistan of 14 March 2026 // lex.uz.

the manufacturer; for other AI systems, the presumption of fault is retained. Such an approach is consistent with the model proposed in the European Parliament resolution of 2020[20].

Second, to redistribute the burden of proof: if the injured party shows a plausible link between the decision of the AI system and the damage caused, a presumption of causation should apply, and the court should be empowered to require the operator to disclose system logs, model documentation and test results.

Third, to enshrine in the Law "On the Protection of Consumer Rights" and in the regulations of the Central Bank, drawing on US experience, an obligation to state in writing the principal reasons when credit is refused, as well as the customer's right to request human review of the decision. Fourth, to introduce compulsory civil liability insurance for operators of high-risk AI and to clearly define the scope of compensation for pure economic loss. Fifth, to introduce into the CC the concept of a "software product defect" and to include within it the failure to provide necessary updates. Sixth, to declare invalid clauses in the contracts of financial institutions that limit liability towards consumers for AI errors.

The issue of civil liability for damage caused by AI systems in the fintech sector cannot be fully resolved within the framework of traditional tort law. An analysis of foreign experience shows that the most effective approach is not to grant AI separate legal personality, but to establish a liability regime differentiated according to the level of risk, to redistribute the burden of proof in favour of the injured party, and to ensure a real compensation mechanism through transparency obligations. Although the initial legislative framework for regulating AI was created in Uzbekistan in 2026, the institution of civil liability has not yet been formed. The proposals put forward in the article will serve to effectively protect the rights of consumers of financial services and to strengthen trust in AI technologies through the improvement of the Civil Code and sector-specific legislation.

[20] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)).