IRSTI 10.27.65
UDC 347.42
JEL K14

https://doi.org/10.46914/2959-4197-2026-1-2-157-169

SHARIVKHAN ZH.,[1]
PhD, associate professor.
e-mail: zhardenbek.m@mail.ru
ORCID ID: 0000-0002-5450-0954
SATYBALDY L.,[1]
c.l.s., associate professor.
e-mail: North_@mail.ru
ORCID ID: 0009-0007-5930-6126
KOLDASSOV B.S.,[2]
master of law, senior lecturer.
e-mail: berik.koldassov@bk.ru
ORCID ID: 0009-0008-6437-5086
OSMANOVA D.B.,*[1]
c.l.s., associate professor.
*e-mail: o_dinara82@mail.ru
ORCID ID: 0000-0003-2760-7243
[1]A. Myrzakhmetov Kokshetau University,
Kokshetau, Kazakhstan
[2]Caspian University of Technology and
Engineering named after Sh. Yessenov,
Aktau, Kazakhstan

CIVIL LIABILITY FOR DAMAGE CAUSED BY ARTIFICIAL INTELLIGENCE SYSTEMS: KEY ISSUES OF LEGAL REGULATION IN THE REPUBLIC OF KAZAKHSTAN

Abstract

The article analyzes the current model of civil liability for damage caused by artificial intelligence systems in the Republic of Kazakhstan and assesses the need for its improvement. The study examines why, despite the adoption of a special law on artificial intelligence, compensation for harm continues to rely on the traditional tort mechanisms of the Civil Code, and whether these mechanisms are capable of addressing algorithmic autonomy, complex technological chains, evidentiary asymmetry, and risk allocation. Using formal-legal, comparative-legal, systemic, and doctrinal methods, the research analyzes the Law of the Republic of Kazakhstan "On Artificial Intelligence", the Civil Code, domestic legal doctrine, the European Union AI Act, the Product Liability Directive, and foreign legal practice. The study concludes that granting artificial intelligence independent legal personality does not simplify compensation mechanisms but instead obscures the identification of liable persons. A more effective approach is proposed whereby external liability toward the victim is concentrated on the entity that introduced and used the system, while liability among developers, integrators, and service providers is distributed through recourse claims. The article also argues that, for high-risk systems, failure to preserve logs, audit materials, and risk documentation should create adverse evidentiary consequences for the defendant.

Keywords: artificial intelligence, civil liability, tort, compensation for harm, causation, high-risk system, algorithmic transparency.

Introduction

The legal system of Kazakhstan has begun to perceive artificial intelligence no longer merely as a technical novelty or part of digital policy, but as an institution generating concrete legal consequences. It is insufficient to measure this change simply by the adoption of a law. More important is the point at which the new legislative layer intersects with old civil-law instruments. The 2025 Law of the Republic of Kazakhstan "On Artificial Intelligence" established as fundamental benchmarks the priority of the human being, his or her rights, freedoms, and well-being, justice and equality, the transparency and intelligibility of the algorithm, accountability and controllability, the protection of

data and privacy, and the safety and reliability of systems; the user must receive complete information about the capabilities, characteristics, and limitations of the artificial intelligence system, while owners and users are obliged to manage risks and bear responsibility, in accordance with legislation, for the results of the system's operation [1]. These are not mere declarations. Yet for civil law the key issue lies elsewhere: Article 24 of the law directly establishes that compensation for damage caused by artificial intelligence systems shall be carried out in accordance with the procedure defined in the Civil Code of the Republic of Kazakhstan, while liability and the insurance of risks are regulated in accordance with legislation [1, 2]. Hence, although the special law initiates a new philosophy of liability, the concrete fate of compensation is nonetheless decided through the classical constructions of the Civil Code [1, 2].

Here the first collision becomes visible. Traditional tort law has in many cases relied either on direct human conduct or on an instrument wholly under human control [2]. But in systems dependent on machine learning, self-adaptation, and data streams, damage often does not arise from a single decision alone. A defect in software architecture, bias in the data set, an integration error, excessive trust on the part of the professional user, an unsuccessful update, the absence of an explanatory interface, or even the very introduction of the system into a field for which it is wholly unsuitable may layer upon one another. In such a chain, to attribute the answer to the question "who exactly caused the damage?" to one defendant invariably distorts the real picture. Therefore, in this sphere, not merely a formal legal definition, but the very technique of attributing liability, acquires decisive significance [1, 2].

Materials and methods

The research relies on the methods of formal-legal, comparative-legal, systemic, and doctrinal analysis. The formal-legal method was used to examine the normative content of the Law of the Republic of Kazakhstan "On Artificial Intelligence" and the Civil Code of the Republic of Kazakhstan, with particular attention to provisions concerning risk management, accountability, compensation for damage, defects in goods, works and services, and the general grounds of tort liability [1, 2]. This method made it possible to identify the legal point at which the special AI legislation does not replace the civil-law regime, but refers the issue of compensation back to the traditional mechanisms of the Civil Code.

The comparative-legal method was applied not as a general description of foreign experience, but as a tool for testing the adequacy of Kazakhstan's model against selected regulatory and judicial materials. For this purpose, the study compares the risk-based logic of the European Union AI Act, the updated approach to defective digital products under Directive (EU) 2024/2853, the withdrawn proposal for the AI Liability Directive, and selected foreign cases involving automated decision-making and algorithmic interfaces [12–17]. The purpose of comparison is not mechanical borrowing, but the identification of those legal techniques that may be relevant for Kazakhstan: disclosure of evidence, documentation duties, risk-based differentiation, the treatment of software and AI systems as products or services, and the allocation of liability between the professional operator and other participants in the technological chain.

The systemic method was used to examine civil liability for AI-related harm not as an isolated private-law issue, but as a point of intersection between civil law, digital regulation, consumer protection, personal data protection, equality guarantees, and sectoral professional duties. This is important because damage caused by an AI system may arise simultaneously from a defective technological architecture, improper deployment, insufficient human oversight, biased data, failure to inform the user, or the absence of audit and logging procedures. The systemic approach therefore allows the research to distinguish between external liability toward the victim and internal allocation of responsibility among developers, integrators, service providers, owners and professional users.

The doctrinal method was used to analyze the positions of Kazakhstani and foreign scholars on the legal status of artificial intelligence, the limits of recognizing AI as a subject of law, and the more practically significant question of who must bear liability for damage caused by algorithmic systems [3–11]. This doctrinal analysis is necessary because the current academic debate often shifts attention to the abstract issue of "electronic personality," while for civil liability the decisive question is different: whether the victim can identify a solvent and legally responsible defendant, obtain evidence, and receive effective compensation.

Results and discussion

The Legal Status of Artificial Intelligence and the Problem of Identifying the Liable Subject. Kazakhstani academic literature has been showing this difficulty from different angles. Zh.O. Tilembaeva earlier noted that the legal regulation of artificial intelligence should be built on the basis of sectoral risks and the balance of the interests of the individual, society, and the state [3]. A.T. Beken, analysing the issue of legal liability for negative consequences arising from the actions of robots equipped with artificial intelligence, expands the circle of potentially liable persons beyond the manufacturer alone, to include the owner, programmer, developing company, and even a third person who unlawfully reprogrammed the system [4]. Zh.R. Temirbekov, in a literature review on the relationship between law and artificial intelligence, shows that current legal systems are not prepared for the phenomenon of autonomy and that, despite the attractiveness of the idea of an "electronic person," it does not automatically resolve the problem of liability [5]. A.N. Kulazhanova proposes, from the standpoint of civil law, the more rational path of considering artificial intelligence within the framework of objects of civil law [6]. A.A. Ondash arrives at similar logic, writing that although disputes concerning the recognition of legal personality have theoretical significance, they do not make easier the question of who is liable for concrete harm [7]. In later works, the conceptual apparatus, legislative definitions, sectoral regulatory principles, and the structure of the new law were examined in detail [8–10]. Among these works one debate has not ceased: should artificial intelligence be introduced into law as an independent subject, or should liability always be returned to a human or organizational link [5–10].

The present study supports the second direction. The reason lies not in a conservative attitude toward technology. The issue is not weakening the victim's legal protection. If artificial intelligence is symbolically recognized as an "electronic person" and liability is shifted onto it, it may remain unclear who exactly pays compensation, who takes out insurance, who conducts the audit, who stops the model, and who corrects the defect [4, 5, 7]. Conferring legal personality here does not deepen liability; on the contrary, it blurs it. The analysis of attribution proposed by Jerrold Soh also touches precisely upon this point: the characterization of artificial intelligence by law as "autonomous" is often the product not of factual reality but of legal convenience, and such convenience sometimes removes liability from the proper subject [11]. Therefore, in Kazakhstan's conditions, it is a far more robust path to regard artificial intelligence as a special object of law, a dangerous digital instrument, or a complex software-hardware product, while distributing liability among the real persons and organizations surrounding it [6, 7, 11].

The Existing Civil Liability Model and Its Limits. The current Civil Code is by no means a blank field for such disputes. Article 917 establishes the general grounds of liability for causing harm; Article 921 establishes the liability of a legal entity or citizen for harm caused by its employee; Article 947 and the related norms disclose the grounds for compensating harm caused as a result of defects in goods, works, and services [2]. Each may be activated in a particular scenario. For example, if a medical organization, relying on the result of a diagnostic system introduced into a doctor's work, prescribes erroneous treatment to a patient, both the regime of liability for employee conduct under Article 921 and the compensation mechanism related to defects in services under Article 947 may potentially be considered in parallel [2]. But if damage is caused by a software defect residing in an autonomous device placed on the market, a model approximated to product defect appears more logical [2, 13]. Yet it is precisely here that artificial intelligence "bends" the classical structures: the defect does not always reside solely in the finished product; it may lie in the data set, in continuous updating, in the cloud service, in the interface, in the safety filter, or in an insufficiently designed mode of human supervision [2, 6, 13].

Already now, two propositions are becoming clear for civil law. The first is that damage caused by artificial intelligence is not always a "software error." Sometimes the system functions correctly from a technical standpoint, but the organization that introduced it uses it in a legally unsuitable context. For example, a model intended to assess creditworthiness may produce biased results with respect to socially vulnerable groups and, in combination with the bank's own internal regulations, generate a discriminatory effect. In such a case, the issue lies not in broken code, but in the use of an algorithmic decision in a sphere affecting human destiny without appropriate safeguards [1, 8, 12]. The second

is the opposite scenario: the organization seems, formally, to have used the system correctly, but the damage arises from a technical defect in the system's core. Thus, for civil-law analysis it is necessary to distinguish at what level the violation is located-at the level of design, at the level of data, at the level of implementation, in the user interface, or in the stage of later updates [2, 13].

If this distinction is not made, judicial practice may move in one of two erroneous directions. The first erroneous direction is to place all liability upon the final user. The logic that "the final decision was made by a human" or that "the organization merely used the tool" looks simple from the outside. But it ignores the role in risk management of the subject that selected, adapted, integrated, and profited from the system, and that prepared its documentation [1, 3]. The second erroneous direction is automatically to blame the developer for all damage. This too is insufficient. For much damage arises not from the model designed by the developer, but from the professional user who did not verify it for its own field, misconfigured it, or removed human control [4, 7]. Therefore, to tie liability to only one center creates, in this sphere, an artificial simplicity [3–7].

Proof, Causation, and the Allocation of External/Internal Liability. In many cases, damage is the product not of one subject, but of a technological chain. For example, a banking scoring system may wrongly place a client into a risky category and groundlessly refuse to grant credit, or unjustifiably increase the cost of insurance. Here, even if the ultimate effect of the decision is connected with a particular algorithmic conclusion, at least four links participate in the dispute: the model creator, the data supplier, the integrator that introduced the system into the business process, and the organization that actually used the conclusion [4, 9, 10]. In the case of an erroneous medical decision, the clinic's own protocols, the doctor's professional judgment, and the quality of informing the patient also enter this circle. Thus, for civil law, the principal task is not to ignore technological complexity and make the person who "pressed the final button" the sole defendant; on the contrary, it is to distinguish between external and internal liability [2, 4, 9, 10].

Table 1 – Functional distribution of liability in cases of damage caused by artificial intelligence systems

Participant in the AI ecosystem	Function in the technological chain	Possible civil-law relevance	Form of liability
Professional operator / organization using the AI system	Introduces the system into professional circulation and applies its results in relations with the victim	Closest institutional link to the victim; controls deployment, instructions, audit, insurance and risk management	External liability toward the victim
Developer of the AI model	Designs the model architecture, training logic and technical functionality	May be responsible where the damage results from a defect in the model, unsafe design, inadequate documentation or failure to provide necessary updates	Internal liability through recourse
Integrator	Adapts and embeds the system into the business, medical, financial or administrative process	May be responsible where harm results from incorrect integration, improper configuration, removal of safeguards or failure to test the system in the relevant environment	Internal liability through recourse
Data supplier / data processor	Provides, prepares or structures data used for training or operation of the system	May be relevant where biased, incomplete, unlawful or poor-quality data materially contributed to the harmful result	Internal liability through recourse or shared liability
Service provider / cloud platform	Provides technical infrastructure, access, maintenance or updates	May be responsible where harm is linked to malfunction, failure of updates, cybersecurity vulnerability, lack of continuity or technical control at the infrastructure level	Internal liability, and in some cases direct liability
Victim / affected person	Suffers harm from the use or result of the AI system	Should not be required to reconstruct the entire technological chain before bringing a claim	Claimant entitled to effective compensation
Note: Compiled by the authors.			

This functional distinction is important because the person who suffered harm is usually not able to determine at the initial stage whether the damage was caused by model architecture, data quality, integration, an update, or improper professional use. Therefore, the external defendant should be the professional subject that introduced and applied the system in civil circulation, while internal disputes among the participants of the technological chain should be resolved through recourse mechanisms.

External liability must be maximally clear for the victim. The person claiming compensation for harm should not be obliged to analyse a complex technological supply chain and identify separately the author of the code, the contractor that selected the data set, the owner of the cloud server, and the subcontractor that configured the model. Such a requirement leaves legal protection on paper. It is fair that the professional subject standing closest to the victim and that actually introduced the artificial intelligence system into circulation should be regarded as the external defendant [2]. In a medical organization, this may be the clinic; in finance, the bank or insurer; in a digital platform, the platform itself; in public service, the relevant organization. Their advantage is not one alone: they selected the system, saw the economic benefit of its use, and possessed the institutional capacity to assess risk, obtain insurance, conduct an audit, draft instructions, and explain matters to the victim [1, 2]. Therefore, imposing external liability on this link is not a step against innovation; it is the alignment of legal burden with the subject capable of effectively managing risk [1, 2, 10].

Internal relations, by contrast, should be resolved through recourse. If the ultimate cause of the damage lay in a defect in the model architecture, the external defendant may later bring a recourse claim against the developer. If the defect arose during integration, recourse turns against the integrator. If the system was of proper quality, yet the professional user ignored instructions or left human control merely formal, there may even be no recourse at all. Such a model does not make the victim dependent on an internal technical dispute within a complex digital ecosystem. Beken's division of potentially liable persons into several categories, and Ondash's presentation of liability as an issue requiring concrete legal regulation, both support this idea [4, 7]. The principle in the new law of specifying liability according to the roles of owners and users also provides the normative precondition for precisely this distribution [1].

One qualification is necessary here. It is insufficient always to assign external liability simply to the "owner." In some cases, the "owner" possesses neither technical control nor professional influence. For example, a small enterprise using a cloud AI system offered as a service does not possess the same capacities as the platform owner managing it at the infrastructural level. Therefore, in possible future amendments to the Civil Code, it would be more appropriate not to confine oneself to the notion of "owner," but to use a functional criterion: "the person who introduced the system into professional use and applied its results in civil circulation" [2, 10]. It is precisely this shift in legislative technique that brings liability closer, not to the formalism of title, but to the real structure of control and profit [2].

The next difficult knot is the concept of fault. In traditional tort law, fault is understood within the framework of negligence or intent [2]. But in disputes concerning artificial intelligence, damage often arises not from a direct "wrong decision" by the operator, but from the organization's failure to create proper mechanisms of verification, control, and warning. Here fault appears not as an isolated psychological condition, but as organizational negligence. Introducing a system without testing it, failing to adapt it to a high-risk environment, not turning on the explanatory module, failing to validate the results, not candidly disclosing limitations to the user, and failing to preserve audit trails-these are the concrete manifestations of fault today [1, 2]. If civil law continues to describe this phenomenon only in the old language of "the employee made a mistake," it will not capture the real mechanism of technological harm.

Kazakhstan's new law obliges users to provide complete information regarding the system's capabilities, characteristics, and limitations, to monitor the operation of the system, to manage risks, and to answer, in accordance with legislation, for its results [1]. These norms are of substantial civil-law significance. They are not merely separate administrative or sectoral obligations; in future tort disputes they should become the benchmark by which the organization's standard of care is measured. Put differently, if an organization that launched a high-risk system failed to warn the user, failed to conduct an audit, failed to document the model's limitations, this ought to be assessed not merely as an ethical defect, but as an independent form of negligence from the standpoint of civil law [1, 3, 8].

Causation is even more difficult. It is precisely this element that, in many cases, becomes the heaviest barrier for the victim. For the connection between damage and an algorithmic decision is

often interrupted by intervening human decisions, organizational procedures, data quality, and system updates [2, 5]. In medicine it is often argued that the final word belongs to the doctor. But this argument does not justify every case. If the interface pushes the doctor into excessive trust in the algorithm, provides no alternative explanation, lacks an error-warning mechanism, then it is insufficient simply to say that "the final decision was made by a human." The same is true in the financial sphere: the fact that a human signed off does not mean that the whole chain of causation becomes detached from the algorithm. Therefore, in evaluating causation, it is necessary to move away from the narrow criterion of the "sole cause of the decision" and develop more precise civil-law tests such as "a substantial factor in the damage" or "the factor that materialized the risk" [2, 5].

The issue of the burden of proof also requires radical rethinking. The victim does not possess the logs, the specific version of the model, the metadata of the training data set, the previous configuration of the user interface, the risk map, or the internal audit materials. All of this is under the control of the defendant organization. In such a situation, to leave with the victim the obligation to provide full technical evidence creates, although it appears to be formal equality, a real procedural inequality. Therefore, for high-risk systems, at least two presumptions seem necessary. The first: if the defendant cannot produce logs, an audit, documented instructions, risk assessment, or proof that the user was informed, this should be evaluated not in its favour but, on the contrary, against itself [1]. The second: if the system was used in a high-risk sphere designated by the new law, and the damage arose in connection with precisely the decision covered by that system, the defendant should be obliged actively to prove that the system complied with the proper standards of safety and control [1, 12]. This approach does not completely reverse the burden of proof, but it softens the information asymmetry in legal terms [1, 2].

Another delicate issue is the defence that "a human remained in control." Many organizations, when introducing AI systems, declare that the final decision always remains with a human. Outwardly, this looks like a responsible model. But for law the issue lies not in a formal signature, but in the reality of the control. If the human is left only with a confirmation button, if there is no explanation, if there is time pressure, if the organization's internal instructions require no departure from the algorithm, or if the human does not have access to alternative sources of information, the expression "human in the loop" may signify not real control, but a technique for shifting liability [5, 11]. Therefore, in future domestic practice, criteria are needed for evaluating the sufficiency of human control: was the human able to explain the decision, was the human able to depart from the algorithmic recommendation on reasonable grounds, was there a possibility of independent verification, did the organization train the human to do so, were time and information provided? Without these, human participation cannot become a magical formula releasing one from liability [1, 5, 11].

Comparative Legal Analysis and Directions for Updating the Kazakhstani Model. The most recent step of the European Union well reveals how deep this problem is. At EU level, the AI Act entrenched a risk-based model: the greater the potential to cause damage, the stricter the requirements; the law separates prohibited practices, imposes special requirements on high-risk systems, introduces clear transparency obligations for certain systems, and requires the marking of generative outputs [12]. Kazakhstan's new law, in substantive terms, also resonates with this direction: it establishes classification according to the level of risk, prohibited practices, mandatory labelling of synthetic content, and duties of control and risk management for owners and users [1]. But EU practice did not stop there. The 2024 Product Liability Directive updated product liability for the digital age and included software, including AI systems, within the concept of "product" to which strict liability for a defective product applies; the Directive clarifies that software is treated as a product regardless of the form in which it is supplied, and that the developer or manufacturer acquires the status of producer [13]. Even more importantly, it was indicated that, in assessing defectiveness, account must be taken of the effect on safety of the product's capacity, after being placed on the market, to learn or acquire new properties [13]. This was law's recognition of the technical reality that the behaviour of an autonomous system may change over time.

The fact that the draft AI Liability Directive later acquired withdrawn status also indicates one thing: even within the European Union itself, the formation of a separate, fully completed civil-liability regime for AI remained difficult [16]. This fact is visible both in the European Parliament's Legislative Train materials and in the EUR-Lex procedural file [16]. Consequently, Kazakhstan does

not now need a "separate civil code for artificial intelligence." But a number of precise, targeted, technologically sensitive amendments to the Civil Code and sectoral legislation are needed.

The updated model of European product liability offers a useful guide in this regard. The 2024 Directive requires, in assessing product defectiveness, account to be taken of labelling, instructions, the absence of software updates, interoperability with other products, safety requirements related to cybersecurity, and the consequences of the product's ability to learn new properties [13]. That is, causation and defectiveness are understood not through purely physical "breakage," but through complex digital behaviour [13]. Even though the Kazakhstani Code lacks precisely this kind of detail, it is unfounded to confine the notion of "defects of goods, works, or services" in Article 947 to a narrow physical deficiency. If an AI system offered as a service misleads the user and pushes the user toward a wrong decision, if the explanatory module generates false confidence, if a mandatory update is not made, or if the quality of the training data set is systematically impaired, all this should be regarded as a contemporary form of defect in a service or product [2, 13].

The practical logic of such a direction is also indicated by a foreign case. In Moffatt v. Air Canada, the airline's chatbot provided a client with erroneous information concerning a bereavement fare, and the company later attempted to rely upon the argument that "the chatbot is a separate subject." Yet the tribunal held that the chatbot was only a part of the company's website, and that the company was therefore responsible for the information on its website; it was recognized that the client was not obliged to verify separately, by reference to another section of the site, information provided by one part of the site [14]. This case is not a model to be copied directly into Kazakhstan. But its principle is highly valuable: an enterprise cannot push outward, by reference to the independence of a "technical agent," the consequences of the algorithmic interface it used in civil circulation [14]. This very principle also comes naturally to domestic law. If a bank, clinic, marketplace, or insurer builds communication with the client precisely through an AI interface, the misleading nature of that interface should remain within the organization's zone of risk [2, 14].

Another useful illustration is Mobley v. Workday, Inc., a United States case concerning algorithmic applicant-screening tools. The plaintiff alleged that Workday's AI-based screening system discriminated against applicants on the basis of race, age and disability. The case is not a classical tort claim for defective products; nevertheless, it is highly relevant for civil liability analysis because it concerns the distribution of responsibility between the organization using an algorithmic system and the technology provider whose tools participate in decision-making. In 2024, the court allowed the claim to proceed under an "agent" theory, reasoning that the plaintiff had plausibly alleged that employers delegated traditional hiring functions to Workday's algorithmic tools. In 2025, the court granted preliminary collective certification for the age-discrimination claim, emphasizing the alleged use of Workday's AI recommendation system to score, sort, rank or screen applicants [17]. For Kazakhstan, the significance of this case is not in the direct borrowing of American employment-discrimination doctrine, but in the more general civil-law idea: where a technological provider does not merely supply a neutral instrument, but participates functionally in decisions affecting legally protected interests, the allocation of liability cannot be reduced to the formal argument that "the final decision belonged to the client."

At this point, the work of Amantai, Nurmagambetov, and Akhpanov, analysing AI tools as a means of expanding access to justice for consumers, is important, even if indirectly [15]. While recognizing the potential of algorithmic assistance, the authors show the need for human oversight, legal infrastructure, and precise regulation [15]. That is, the issue is not a total negation of AI, but its combination with institutional responsibility. In civil liability as well, the same logic should operate: an AI system may be useful, but precisely this usefulness must not obscure who bears the risk [15].

Another controversial topic is the civil-law dimension of harm caused by personal-data violations, breaches of privacy, and algorithmic discrimination. The new law prohibited the creation and use of systems that violate requirements for the protection of personal data, exploit human vulnerabilities, permit social or biometric discrimination, and use manipulative methods [1]. But prohibition does not automatically mean full compensation. The consequences of discrimination often manifest not through direct material loss, but through lost opportunity, damage to reputation, moral suffering, and exclusion from civil circulation [1, 8]. In such cases, the structure of compensation, the standard of proof, and the mechanism for evaluating moral harm remain for now unclear. Hence, AI liability is

not only a matter of technical defect; it also intersects with the principles of equality, dignity, and fair procedure [1, 3, 8].

From a practical standpoint, sectoral differences need to be laid open distinctly. In healthcare, if an artificial intelligence system influences diagnosis, risk assessment, or therapeutic tactics, it is appropriate to maintain the civil-liability standard at the highest level [2]. Here the patient's informational weakness, trust in the authority of the specialist, and the irreversibility of the consequences of an erroneous decision play a special role. In the financial sector, the situation is somewhat different: damage manifests itself more often not through an instantaneous physical consequence, but through erroneous scoring, unjustified refusals, incorrect calculation of insurance risk, or automated alteration of contractual terms. But here too the organization's professional status does not weaken. A financial institution is not merely a purchaser of an algorithm; it is an infrastructure of trust in civil circulation. For that reason, its argument that "the vendor offered it to us this way" cannot become a fully exculpatory proof [2, 9, 10]. In transport and logistics, disputes connected with autonomous or semi-autonomous systems are characterized by complex causation between software, sensor data, operator reaction, and technical maintenance. Here too it is preferable that external liability be located at the operator link standing closest to the victim, while internal distribution is resolved within the technical chain [2, 9, 10].

The sphere of public services requires particular attention. If artificial intelligence is used in the formation of state information resources, in the provision of services to citizens, in selection for social benefits, in risk assessment, or in other decisions of public significance, then the question of civil liability overlays a public-law dimension. Here the damage may not always manifest itself in the form of monetary loss; sometimes the citizen loses a right, a service, a status, or a procedural guarantee. Kazakhstan's new law introduces heightened requirements precisely for high-risk systems in such important spheres [1]. If the civil consequences of these requirements are not made clear, legal regulation will not be fully activated. If a citizen is groundlessly excluded from a public service or deprived of access to social support as a result of an automated decision, it may be insufficient to confine matters solely to an administrative appeal procedure. In certain situations, property damage, lost opportunity, moral harm, and even damage to reputation may arise in parallel [1, 8]. Therefore, in future law-enforcement practice it is necessary to see public and private law mechanisms not as opposed to one another, but as a complementary structure [1, 8].

The issue of auditing artificial intelligence systems should also be reassessed from the standpoint of civil liability. Ordinarily, audit is spoken of within the framework of administrative oversight, technical conformity, or corporate compliance. Yet in a civil dispute the existence or absence of an audit provides direct information about the defendant's diligence. If an organization introduces a system into a high-risk environment, but conducts no independent validation, models no probable error scenarios, does not test data bias, and does not train the user, it cannot later describe the resulting damage merely as an "accidental technical defect" [1, 3]. Here, in evaluating the standard of care, the work carried out in advance acquires decisive significance. The presence in the new law of norms concerning risk management and audit builds a direct bridge to civil law [1]. And if this bridge remains unused, the most important preventive potential of the legislation is lost. For that reason, in the future, a more complex analysis may be expected from courts-one that evaluates not only the fact of the damage, but also the managerial order preceding the introduction of the system [1, 2].

Another difficult question is how moral harm and damage to reputation are to be evaluated in an algorithmic environment. A system using artificial intelligence may place a person into an incorrect category, present that person as a false dangerous subject, produce an automated conclusion damaging professional reputation, or indirectly create conditions for the dissemination of false synthetic content. In such cases, the amount of damage is not measured by bookkeeping alone. Lost opportunity, social stigma, deterioration of business reputation, and psychological pressure-all these are real objects of civil-law protection [1, 2]. Kazakhstan law is not unfamiliar with this mechanism, but in the context of artificial intelligence proof and evaluation become more complicated. Here the court must take into account not only the truth or falsity of the result, but also the speed of the automated system's impact on reputation, the scale of dissemination, the possibility of correction, and whether the organization acted promptly. And where the requirement of mandatory labelling of synthetic content is violated, the weight of civil liability becomes even stronger [1].

There is yet another aspect connected with works and data sets used to train artificial intelligence. The new law has entrenched an approach under which works may be used for training AI models only where the author or right holder has not prohibited such use [1]. This rule is usually discussed within the framework of copyright. But it also bears upon civil liability. If a model is trained on unlawful or unauthorized data and later precisely that model produces an erroneous, false, or harmful output that causes civil loss, the original infringement related to the data source should not be excluded from consideration in internal recourse and in the distribution of risk [1, 10]. Put differently, it should not be possible to "feed" a model on unlawful data and then shift its consequences solely onto the final user. Here the closeness of the developer or provider to the original infringement increases its subsequent civil risk [1, 10].

Conclusion

The totality of the foregoing leads to one conclusion. Kazakhstan does not now need a "separate civil code for artificial intelligence." But a number of precise, targeted, and technologically sensitive amendments to the Civil Code and sectoral legislation are necessary. These amendments should not remain at the level of abstract references to "improvement of regulation." At least five concrete directions appear necessary. First, the Civil Code should clarify that a defect in a digital product or service may include not only physical malfunction, but also unsafe algorithmic behaviour, misleading interface design, inadequate documentation, failure to provide necessary updates, insufficient cybersecurity protection, and the use of data that creates legally significant discriminatory or harmful effects. Secondly, for high-risk AI systems, legislation should introduce a duty to preserve logs, audit reports, risk assessment materials, documentation on model limitations, and evidence that the user or affected person was properly informed. Thirdly, failure to preserve such materials should entail adverse evidentiary consequences for the defendant, since the victim normally has no access to the technical information needed to prove causation. Fourthly, external liability should be linked not to the formal title of "owner," but to the functional criterion of professional deployment: the person who introduced the system into civil circulation, applied its results and was able to manage the risk should be the primary defendant toward the victim. Fifthly, sectoral legislation should develop insurance and recourse mechanisms for high-risk AI systems, so that compensation for the victim is not delayed by internal disputes between developers, integrators, cloud providers and professional users [1, 2, 10, 13].

In addition, future judicial practice in Kazakhstan should receive methodological guidance on the assessment of causation in algorithmic harm cases. Courts should not ask only whether the AI system was the sole cause of damage. In technologically complex disputes, a more realistic test is whether the AI system was a substantial factor in the materialization of the risk, whether the defendant failed to maintain an adequate standard of organizational care, and whether the absence of documentation prevents the victim from proving the internal mechanism of harm. This approach would allow civil liability to respond to the actual structure of AI-related damage without transforming artificial intelligence into an independent legal person and without leaving the victim in an evidentiary vacuum.

As a final point, attention should be directed to the very culture of law enforcement. If the regulation of artificial intelligence is confined only to new terms, new prohibitions, and new ethical declarations, there will be little concrete result for civil circulation. The real test begins when a claim reaches the court: how does the judge understand the structure of the algorithmic system, what documents does the judge demand from the parties, how does the judge evaluate organizational diligence, does the judge recognize the asymmetry of proof or not, does the judge leave the victim under the burden of the costs of technical expertise, or does the judge take into account the informational dominance of the professional operator [1, 2]. Therefore, for Kazakhstan, not only the refinement of the legislative text is important, but also methodological explanations for judicial practice, principled positions at the level of the highest court, a specialized expert infrastructure for digital disputes, and, if necessary, model evidentiary standards. The real effectiveness of civil liability is tested precisely in this institutional layer. If law-enforcement bodies perceive artificial intelligence either as a "magic black box" or as "merely another computer program," in both cases they err. In the first case, they retreat excessively before technical complexity and blur liability. In the second, they ignore the specific features of autonomy, data dependence, and scale effects, and mechanically apply the old tort scheme. Kazakhstan needs

a balanced law-enforcement model operating between these two extremes, nourished by academic literature, comparative experience, and the data of the concrete digital environment. Only then will the new law's provisions concerning human rights, transparency, safety, and accountability cease to remain formal slogans and become concrete compensation, concrete standards of care, and concrete legal predictability [1, 2, 12, 13].

At the present stage, the most rational formula comes down to this: civil liability with respect to artificial intelligence should be evaluated not by the single question "who owns the technology?" but by four criteria – "who created the risk, who was capable of managing it, who profited from it, and who stands in the closest legal relationship to the victim?" Only when these four criteria are applied together can Kazakhstan's legal system distribute algorithmic harm fairly. Such an approach opens the way to recognizing new technology neither as a source of fear nor as a symbol of limitless progress, but as a complex institution bringing, for law, both concrete risk and concrete opportunity [2, 7, 11].

Therefore, discussion of liability for damage caused by artificial intelligence is not a hypothesis of the future, but already a practical task of civil law. For the legislator, for the courts, and for legal doctrine alike, the main test is the same: not to leave the victim in a legal vacuum by referring to technical complexity. The value of civil law is measured precisely at such a moment. The task of law lies not in placing the algorithm above the human being, but in fixing with precision the human and institutional responsibility for the risk generated by the algorithm. For that reason, any reform in this sphere should be evaluated through the accessibility of compensation, the fairness of proof, and the clarity of identifying the liable subject. An effective model of civil liability for damage caused by artificial intelligence systems will likewise take shape precisely through the concrete securing of these requirements.

REFERENCES

1 Закон Республики Казахстан «Об искусственном интеллекте» от 17 ноября 2025 года № 230-VIII ЗРК. URL: https://adilet.zan.kz/kaz/docs/Z2500000230 (дата обращения: 20.03.2026)

2 Civil Code of the Republic of Kazakhstan (Special Part). 1 July 1999. URL: https://adilet.zan.kz/eng/docs/K990000409_ (accessed: 20.03.2026)

3 Тлембаева Ж.У. О некоторых подходах к правовому регулированию искусственного интеллекта // Вестник Института законодательства Республики Казахстан. – 2021. – № 2(65). DOI: 10.52026/2788-5291_2021_65_2_61

4 Бекен А.Т. Некоторые вопросы правосубъектности роботов, оснащенных искусственным интеллектом // Вестник Института законодательства Республики Казахстан. – 2019. – № 4(58). – С. 170–175.

5 Темірбеков Ж.Р. Құқық пен жасанды интеллект // Право и государство. – 2022. – № 2(95). – С. 83–99. DOI: 10.51634/2307-5201_2022_2_83

6 Құлажанова А.Н. Жасанды интеллект азаматтық құқық объектісі ретінде // Dulaty University Хабаршысы. – 2024. – № 3. – Б. 143–151. DOI: 10.55956/HUFB6983

7 Ондаш А.А. Жасанды интеллекттің құқықтық мәртебесі және оның құқық субъектілігі туралы даулар // Право и государство. – 2024. – № 1(102). – Б. 55–64. DOI: 10.51634/2307-5201_2024_1_55

8 Жалтырбаева Р.С., Джангабулова А.Қ., Тілембаева Ж.О. Жасанды интеллект ұғымының құқықтық дефинициясы: теориялық негіздер мен заңнамалық тұжырымда // Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының Жаршысы. – 2025. – № 4(80). – Б. 35–53. DOI: 10.52026/2788-5291_2025_80_4_35

9 Бердиярова Ж.С., Саймова Ш.А., Абдуллаева Д.С. Жасанды интеллектіні пайдаланудың құқықтық мәселелері // Вестник им. Л.Н. Гумилева. Серия «Право». – 2026. – №. 1(154). – Б. 41–50. DOI: 10.32523/2616-6844-2026-154-1-41-50

10 Турецкий Н.Н. О Законе Республики Казахстан «Об искусственном интеллекте» // Вестник Института законодательства Республики Казахстан. – 2025. – № 4(80). – С. 398–408. DOI: 10.52026/2788-5291_2025_80_4_398

11 Soh J. Legal dispositionism and artificially-intelligent attributions // Legal Studies. 2023. Vol. 43. No. 4. P. 583–602. DOI: 10.1017/lst.2022.52.

12 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). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (accessed: 20.03.2026)

13 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. URL: https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng (accessed: 20.03.2026)

14 Moffatt v. Air Canada, 2024 BCCRT 149. URL: https://canlii.ca/t/k2spq (accessed: 20.03.2026)

15 Amantai A., Nurmagambetov A.M., Akhpanov A.N. The Use of Artificial Intelligence Tools as a Means of Ensuring Consumers' Access to Justice // Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan. 2025. Vol. 80. No. 3.

16 Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final; proposal withdrawn. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0496 (accessed: 20.03.2026)

17 Mobley v. Workday, Inc., Case No. 23-cv-00770-RFL, Order Granting Preliminary Collective Certification, United States District Court, Northern District of California, 16 May 2025. URL: https://www.govinfo.gov/content/pkg/USCOURTS-cand-3_23-cv-00770/pdf/USCOURTS-cand-3_23-cv-00770-1.pdf (accessed: 03.06.2026)

REFERENCES

1 Zakon Respubliki Kazahstan «Ob iskusstvennom intellekte» ot 17 nojabrja 2025 goda No. 230-VIII ZRK. URL: https://adilet.zan.kz/kaz/docs/Z2500000230 (data obrashhenija: 20.03.2026). (In Russian)

2 Civil Code of the Republic of Kazakhstan (Special Part). 1 July 1999. URL: https://adilet.zan.kz/eng/docs/K990000409_ (accessed: 20.03.2026). (In English)

3 Tlembaeva Zh.U. (2021) O nekotoryh podhodah k pravovomu regulirovaniju iskusstvennogo intellekta // Vestnik Instituta zakonodatel'stva Respubliki Kazahstan. No. 2(65). DOI: 10.52026/2788-5291_2021_65_2_61 (In Russian)

4 Beken A.T. (2019) Nekotorye voprosy pravosub#ektnosti robotov, osnashhennyh iskusstvennym intellektom // Vestnik Instituta zakonodatel'stva Respubliki Kazahstan. No. 4(58). P. 170–175. (In Russian)

5 Temırbekov J.R. (2022) Qūqyq pen jasandy intelekt // Pravo i gosudarstvo. No. 2(95). P. 83–99. DOI: 10.51634/2307-5201_2022_2_83 (In Kazakh)

6 Qūlajanova A.N. (2024) Jasandy intelekt azamattyq qūqyq obektısı retında // Dulaty University Habarşysy. No. 3. P. 143–151. DOI: 10.55956/HUFB6983 (In Kazakh)

7 Ondaş A.A. (2024) Jasandy intelekttıñ qūqyqtyq märtebesı jäne onyñ qūqyq subektılıgı turaly daular // Pravo i gosudarstvo. No. 1(102). P. 55–64. DOI: 10.51634/2307-5201_2024_1_55 (In Kazakh)

8 Jaltyrbaeva R.S., Jangabulova A.Q., Tılembaeva J.O. (2025) Jasandy intelekt ūğymynyñ qūqyqtyq definisiasy: teorialyq negızder men zañnamalyq tūjyrymda // Qazaqstan Respublikasynyñ Zañnama jäne qūqyqtyq aqparat institutynyñ Jarşysy. No. 4(80). P. 35–53. DOI: 10.52026/2788-5291_2025_80_4_35 (In Kazakh)

9 Berdiarova J.S., Saimova Ş.A., Abdullaeva D.S. (2026) Jasandy intelektını paidalanudyñ qūqyqtyq mäseleleri // Vestnik im. L.N. Gumileva. Seria «Pravo». No. 1(154). P. 41–50. DOI: 10.32523/2616-6844-2026-154-1-41-50. (In Kazakh)

10 Tureckij N.N. (2025) O Zakone Respubliki Kazahstan «Ob iskusstvennom intellekte» // Vestnik Instituta zakonodatel'stva Respubliki Kazahstan. No. 4(80). P. 398–408. DOI: 10.52026/2788-5291_2025_80_4_398 (In Russian)

11 Soh J. (2023) Legal dispositionism and artificially-intelligent attributions // Legal Studies. Vol. 43. No. 4. P. 583–602. DOI: 10.1017/lst.2022.52 (In English)

12 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). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (accessed: 20.03.2026). (In English)

13 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. URL: https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng (accessed: 20.03.2026). (In English)

14 Moffatt v. Air Canada, 2024 BCCRT 149. URL: https://canlii.ca/t/k2spq (accessed: 20.03.2026). (In English)

15 Amantai A., Nurmagambetov A.M., Akhpanov A.N. (2025) The Use of Artificial Intelligence Tools as a Means of Ensuring Consumers' Access to Justice // Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan. Vol. 80. No. 3. (In English)

16 Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final; proposal withdrawn.

URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0496 (accessed: 20.03.2026). (In English)

17 Mobley v. Workday, Inc., Case No. 23-cv-00770-RFL, Order Granting Preliminary Collective Certification, United States District Court, Northern District of California, 16 May 2025. URL: https://www.govinfo.gov/content/pkg/USCOURTS-cand-3_23-cv-00770/pdf/USCOURTS-cand-3_23-cv-00770-1.pdf (accessed: 03.06.2026). (In English)

ШАРИВХАН Ж.,[1]
PhD, қауымдастырылған профессор.
e-mail: zhardenbek.m@mail.ru
ORCID ID: 0000-0002-5450-0954
САТЫБАЛДЫ Л.,[1]
з.ғ.к., қауымдастырылған профессор.
e-mail: North_@mail.ru
ORCID ID: 0009-0007-5930-6126
КОЛДАСОВ Б.С.,[2]
з.ғ.м., аға оқытушы.
e-mail: berik.koldassov@bk.ru
ORCID ID: 0009-0008-6437-5086
ОСМАНОВА Д.Б.,*[1]
з.ғ.к., қауымдастырылған профессор.
*e-mail: o_dinara82@mail.ru
ORCID ID: 0000-0003-2760-7243
[1]А. Мырзахметов ат. Көкшетау университеті,
Көкшетау қ., Қазақстан
[2]Ш. Есенов атындағы Каспий технологиялар
және инжиниринг университеті,
Ақтау қ., Қазақстан

ЖАСАНДЫ ИНТЕЛЛЕКТ ЖҮЙЕЛЕРІ КЕЛТІРГЕН ЗИЯН ҮШІН АЗАМАТТЫҚ-ҚҰҚЫҚТЫҚ ЖАУАПКЕРШІЛІК: ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ ҚҰҚЫҚТЫҚ РЕТТЕУДІҢ ТҮЙІНДІ МӘСЕЛЕЛЕРІ

Аңдатпа

Мақала Қазақстан Республикасында жасанды интеллект жүйелері келтірген зиян үшін азаматтық-құқықтық жауапкершіліктің қолданыстағы моделін және оны жетілдіру қажеттігін талдауға арналған. Зерттеу өзегінде бір сұрақ тұр: арнайы заң қабылданған жағдайда неге зиянды өтеу мәселесі әлі де Азаматтық кодекстің дәстүрлі деликттік тетіктерімен шешіледі және бұл тетіктер алгоритмдік автономия, көпсубъектілі технологиялық тізбек, дәлелдеу асимметриясы мен тәуекелді үлестіру проблемаларына қаншалықты бейімделген. Талдау барысында Қазақстан Республикасының «Жасанды интеллект туралы» заңы, Азаматтық кодекс нормалары, отандық құқықтанудағы негізгі тұжырымдар, сондай-ақ Еуропалық одақтың AI Act, Product Liability Directive және шетелдік құқық қолдану материалдары формальды-құқықтық, салыстырмалы-құқықтық, жүйелік және доктриналдық әдістерді қолдану арқылы қарастырылды. Зерттеу нәтижесінде жасанды интеллектке дербес құқық субъектілігін беру қазіргі жағдайда өтем тетігін жеңілдетпейтіні, керісінше жауапты тұлғалар шеңберін бұлдыратыны айқындалды. Неғұрлым орнықты шешім ретінде жәбірленушіге қатысты сыртқы жауапкершілікті жүйені кәсіби айналымға енгізген және оның нәтижелерін пайдаланған субъектінің мойнына шоғырландыру, ал әзірлеуші, интегратор, сервис жеткізуші және өзге қатысушылар арасындағы жауапкершілікті регресс тәртібімен бөлу ұсынылады. Сонымен бірге жоғары тәуекелді жүйелер бойынша логтарды, аудит материалдарын, тәуекел карталарын және пайдаланушыны хабардар ету құжаттарын сақтамау дәлелдеу салдарын жауапкердің өзіне қарсы бұруға негіз болуы тиіс деген қорытынды жасалады.

Тірек сөздер: жасанды интеллект, азаматтық жауапкершілік, деликт, зиянды өтеу, себепті байланыс, жоғары тәуекелді жүйе, алгоритмдік ашықтық.

ШАРИВХАН Ж.,[1]
PhD, ассоциированный профессор.
e-mail: zhardenbek.m@mail.ru
ORCID ID: 0000-0002-5450-0954
САТЫБАЛДЫ Л.,[1]
к.ю.н., ассоциированный профессор.
e-mail: North_@mail.ru
ORCID ID: 0009-0007-5930-6126
КОЛДАСОВ Б.С.,[2]
м.ю.н., ст. преподаватель.
e-mail: berik.koldassov@bk.ru
ORCID ID: 0009-0008-6437-5086
ОСМАНОВА Д.Б.,*[1]
к.ю.н., ассоциированный профессор.
*e-mail: o_dinara82@mail.ru
ORCID ID: 0000-0003-2760-7243
[1]Кокшетауский университет
им. А. Мырзахметова,
г. Кокшетау, Казахстан
[2]Каспийский университет технологии и
инжиниринга им. Ш. Есенова,
г. Актау, Казахстан

ГРАЖДАНСКО-ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ ЗА ВРЕД, ПРИЧИНЕННЫЙ СИСТЕМАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: КЛЮЧЕВЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация

Статья посвящена анализу действующей модели гражданско-правовой ответственности за вред, причиненный системами искусственного интеллекта, в Республике Казахстан и необходимости ее совершенствования. В центре исследования стоит один вопрос: почему даже при принятии специального закона проблема возмещения вреда по-прежнему решается посредством традиционных деликтных механизмов Гражданского кодекса и насколько эти механизмы адаптированы к проблемам алгоритмической автономии, многосубъектной технологической цепочки, асимметрии доказывания и распределения риска. В ходе анализа были рассмотрены Закон Республики Казахстан «Об искусственном интеллекте», нормы Гражданского кодекса, основные концепции отечественной правовой науки, а также AI Act Европейского союза, Product Liability Directive и материалы зарубежной правоприменительной практики с использованием формально-юридического, сравнительно-правового, системного и доктринального методов. В результате исследования установлено, что наделение искусственного интеллекта самостоятельной правосубъектностью в современных условиях не упрощает механизм возмещения, а, напротив, размывает круг ответственных лиц. В качестве более устойчивого решения предлагается сосредоточить внешнюю ответственность перед потерпевшим на субъекте, который ввел систему в профессиональный оборот и использовал ее результаты, а ответственность между разработчиком, интегратором, поставщиком сервиса и иными участниками распределять в порядке регресса. Вместе с тем делается вывод о том, что по высокорисковым системам несохранение логов, материалов аудита, карт рисков и документов об информировании пользователя должно служить основанием для обращения последствий доказывания против самого ответчика.

Ключевые слова: искусственный интеллект, гражданская ответственность, деликт, возмещение вреда, причинная связь, высокорисковая система, алгоритмическая прозрачность.

Article submission date: 14.04.2026