



How to cite this article:

Lotfi, A., Qasim Ashour Alabbas, M., & Tareq Kadhim Kadhim, W. (2025). Civil Liability Arising from the Use of Artificial Intelligence Systems: An Analytical–Comparative Study in Light of the Provisions of the Iraqi Civil Code and Iranian Civil Law. *Journal of Historical Research, Law and Policy*, 3(4), 1-17. <https://doi.org/10.61838/jhrp.339>



Article history:
Original Research

Dates:

Submission Date: 19 May 2025

Revision Date: 12 November 2025

Acceptance Date: 19 November 2025

Publication Date: 01 December 2025

Civil Liability Arising from the Use of Artificial Intelligence Systems: An Analytical–Comparative Study in Light of the Provisions of the Iraqi Civil Code and Iranian Civil Law

1. Abdolreza. Lotfi ^{1*}: Assistant Professor, Department of Jurisprudence and Law, University of Tabriz, Tabriz, Iran
2. Mohammed. Qasim Ashour Alabbas ²: MA Student, Department of Jurisprudence and Law, University of Tabriz, Tabriz, Iran
3. Wefaq. Tareq Kadhim Kadhim ³: MA Student, Department of Jurisprudence and Law, University of Tabriz, Tabriz, Iran

*corresponding author's email: tasnim4757@gmail.com

ABSTRACT

This study examines civil liability arising from the use of artificial intelligence systems through an analytical–comparative approach focused on Iraqi civil law and Iranian civil law. The rapid expansion of artificial intelligence in medical, commercial, judicial, administrative, educational, and financial fields has created new forms of harm that challenge traditional doctrines of civil liability. Unlike conventional tools, AI systems may operate with autonomy, opacity, adaptive learning, and distributed technical control, making it difficult to determine fault, prove causation, and identify the legally responsible party. The study analyzes the extent to which existing Iraqi and Iranian civil liability rules can address damages caused by AI systems, particularly where harm results from algorithmic decision-making, defective data, insufficient human supervision, or unpredictable system behavior. The findings indicate that both legal systems possess flexible foundations, including fault-based liability, compensation for harmful acts, causation principles, and responsibility for damage, but these rules are not fully adequate for high-risk AI applications. The study argues that AI should not be granted independent legal personality, because such recognition may obscure the responsibility of developers, operators, owners, users, manufacturers, data providers, and institutions benefiting from AI deployment. Instead, liability should be allocated among human and legal persons connected to the design, production, deployment, supervision, and use of AI systems. The article proposes a hybrid liability model that preserves fault-based liability for ordinary AI applications, applies presumed fault where technical opacity prevents effective proof, and adopts strict liability for high-risk AI systems affecting life, health, property, privacy, or fundamental rights. It further recommends mandatory insurance, technical documentation, algorithmic auditability, human oversight, and specialized evidentiary rules. The study concludes that Iraqi and Iranian civil law require legislative modernization to ensure effective victim compensation, legal certainty, and responsible technological innovation.

Keywords: Artificial intelligence; civil liability; Iraqi Civil Code; Iranian civil law; algorithmic harm; strict liability; fault-based liability; comparative law.

Introduction

Artificial intelligence has moved from a specialized computational field into a pervasive infrastructure of social, commercial, administrative, medical, financial, educational, and judicial decision-making. In its contemporary form, AI does not merely accelerate human activity; it increasingly participates in producing decisions, classifications,



© 2025 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

recommendations, predictions, diagnoses, and operational acts that may directly affect legally protected interests. The technical foundations of modern AI, especially machine learning and data-driven optimization, mean that many systems no longer function as passive instruments whose outputs are fully predetermined by a programmer at the moment of design. Rather, such systems may adapt to data environments, modify their output patterns, and generate results that are difficult to anticipate even for their developers. This technical reality is central to the civil liability problem, because traditional liability doctrines are largely built around human agency, intentionality, negligence, foreseeability, and identifiable causal chains. As Russell and Norvig explain in their foundational account of artificial intelligence, intelligent systems are designed to perceive environments and act toward goals, and this functional orientation gives AI systems a distinctive position between ordinary tools and autonomous decision-making agents (1). When such systems produce harmful outcomes, civil law must determine whether responsibility should be attributed to the producer, programmer, owner, operator, user, data provider, service platform, or another actor involved in the system's lifecycle.

The emergence of AI-related civil liability has therefore created a doctrinal tension between technological autonomy and legal accountability. Civil liability in its classical structure depends on the establishment of damage, a legally relevant act or omission, and a causal connection between the conduct of a responsible person and the harm suffered by the injured party. However, AI systems challenge each of these elements. The harmful conduct may not be a direct human act but the result of algorithmic inference; the causal chain may be distributed across software design, training data, system deployment, user interaction, and post-deployment learning; and fault may be difficult to prove because the harmful output may arise from opaque internal processing. Scherer emphasizes that AI systems create regulatory difficulty because their risks are not limited to isolated defects but arise from complexity, autonomy, and unpredictability in dynamic environments (2). Similarly, Marchant argues that tort law must confront forms of harm in which the traditional negligence model is strained by the technical opacity and adaptive behavior of intelligent systems (3). In this sense, AI does not simply add a new category of harmful object to existing civil law; it transforms the conditions under which attribution, proof, and compensation are understood.

The importance of this problem is intensified in legal systems such as Iraq and Iran, where the civil liability framework is rooted in a combination of codified civil law, general principles of fault and causation, and, especially in Iranian law, jurisprudential concepts such as guarantee, direct causation, indirect causation, and the prohibition of harm. The Iraqi Civil Code is structured around general civil liability provisions that can be extended to harmful acts, unlawful conduct, and compensation for damage. Iranian civil law, in addition to the Civil Code and the Civil Liability Act, draws heavily on Islamic jurisprudential doctrines concerning liability for loss, causation, and harmful conduct. These frameworks contain flexible concepts capable of responding to new harms, but they were not originally designed for autonomous digital systems. Keshavarz's analysis of AI-related liability in European documents and Iranian law indicates that Iranian doctrine must confront the question of whether existing bases of civil responsibility can properly accommodate AI systems whose performance depends on multiple technical and organizational actors (4). The comparative value of examining Iraqi and Iranian law lies precisely in this shared doctrinal challenge: both systems possess general liability tools, yet both must determine whether such tools are sufficient for technologically mediated harm.

The first central issue concerns fault. In classical civil liability, fault normally refers to an unlawful act, negligence, imprudence, lack of care, or violation of a legal duty. Yet in the AI context, the injured person may be unable to identify the precise human error that produced the harm. If an AI medical system misdiagnoses a patient, the

relevant fault might lie in defective programming, biased data, inadequate clinical supervision, improper deployment, failure to update the model, or unreasonable reliance by the physician. Montazeri and Shakrian show that pharmaceutical and medical uses of AI raise special liability problems because harm may result from the interaction of scientific uncertainty, automated recommendation, and professional decision-making (5). This difficulty also appears in autonomous vehicles, algorithmic credit scoring, predictive policing systems, automated trading tools, robotic devices, and AI-generated informational harms. In such cases, insisting on proof of individualized fault may leave victims uncompensated, while imposing liability too broadly may discourage innovation. Wagner therefore argues that liability rules for autonomous AI must balance victim protection, risk allocation, and technological development rather than mechanically applying older fault-based categories (6).

The second issue concerns causation. AI systems often operate through layered and distributed processes in which a harmful output cannot easily be traced to one actor or one moment of conduct. A developer may design the model architecture, another entity may supply training data, a third may integrate the system into a commercial product, and the final user may deploy it in a concrete context. Lemley's discussion of liability for autonomous AI highlights that autonomy disrupts conventional assumptions about control because the system's behavior may not be fully predictable by any single participant in the chain (7). This is especially problematic in Iraqi and Iranian civil law, where causation remains central to compensatory responsibility. If a court cannot determine whether the harm resulted from a defect in the algorithm, improper use, environmental conditions, or data bias, liability may become uncertain. Gless also notes that AI creates evidentiary and normative problems because legal systems must decide how to attribute consequences when algorithmic processes intervene between human action and legal harm (8). The causation problem is therefore not merely technical; it is a legal problem of attribution in a world where harmful consequences may emerge from human-machine interaction.

The third issue concerns the legal status of AI itself. Some scholars have asked whether highly autonomous AI systems should be treated as legal persons, electronic agents, products, objects, or dangerous instruments. Chesterman's work on the limits of legal personality warns against prematurely granting AI independent legal personality, because legal personality is not merely a functional device but a normative institution connected to rights, duties, accountability, and social recognition (9). Solaiman similarly analyzes the legal personality debate by comparing robots and corporations, showing that recognition of artificial personality requires careful justification and cannot be reduced to technological sophistication (10). For Iraqi and Iranian law, the question is especially sensitive because civil responsibility is traditionally attached to natural persons, legal persons, owners, possessors, guardians, and those who directly or indirectly cause harm. AI systems may therefore be better understood not as independent legal persons but as sources of risk managed by human or corporate actors. Yet even this approach requires identifying which actor should bear responsibility when harm occurs.

The objective of this study is to analyze the civil liability arising from the use of artificial intelligence systems through a comparative examination of Iraqi civil law and Iranian civil law, with particular attention to the adequacy of traditional liability doctrines and the need for risk-based legal reform. This study proceeds from the premise that AI-related harm cannot be understood solely through the lens of ordinary tools, because the autonomy, opacity, and adaptive capacity of AI alter the relationship between human control and legal responsibility. At the same time, the study does not assume that AI must be granted legal personality or treated as an independent legal subject. Instead, it investigates how existing liability doctrines may be interpreted, extended, or restructured to protect injured parties while preserving doctrinal coherence and technological development. Calo's policy roadmap suggests that

effective AI regulation requires legal systems to understand the specific properties of AI rather than responding through vague technological anxiety (11). This article therefore adopts an analytical-comparative method, examining the conceptual foundations of AI and civil liability, the application of Iraqi and Iranian doctrines to AI-related harm, comparative international approaches, and the normative direction of reform.

Conceptual and Legal Foundations of Artificial Intelligence and Civil Liability

The conceptual foundation of AI-related civil liability must begin with the distinctive nature of artificial intelligence as a technological system. AI is not a single technology but a broad family of computational techniques capable of classification, prediction, pattern recognition, natural language processing, automated reasoning, image interpretation, decision support, and autonomous action. Modern AI systems are especially significant because they often depend on machine learning, where the system's performance is shaped not only by explicit instructions but also by training data and iterative optimization. Russell and Norvig's account of intelligent agents is important for legal analysis because it frames AI as a system that receives inputs from an environment and produces outputs or actions in pursuit of objectives (1). This functional structure differs from ordinary mechanical tools, which generally operate according to fixed and transparent causal mechanisms. In AI systems, the legal relevance of a harmful outcome may depend on the design of the model, the quality of the data, the context of deployment, and the scope of human oversight.

The legal difficulty becomes clearer when one distinguishes between different degrees of autonomy. Some AI systems merely assist human decision-making by providing information or recommendations, while others perform actions with limited real-time human control. Decision-support systems used in medicine, finance, education, insurance, or litigation may influence human judgment without formally replacing it. Autonomous vehicles, robotic medical devices, automated trading platforms, and industrial robots may act more directly in the physical or economic world. Turner notes that legal rules for robots and AI must address the fact that such systems blur the distinction between tool and actor, particularly when machines are capable of responding to environmental conditions in ways not specifically anticipated by the designer (12). Barfield similarly argues that autonomous and artificially intelligent robots require liability analysis that accounts for both technical design and operational independence (13). For civil liability, the degree of autonomy matters because the more independent the system appears in operation, the harder it becomes to characterize the harm as the simple and immediate result of a human act.

Opacity is another defining feature of many AI systems. The so-called black-box problem refers to the difficulty of explaining how complex models reach particular outputs. In some systems, especially those using deep learning, even developers may not be able to provide a simple causal explanation for a specific decision. This opacity affects civil liability because proof of fault and causation often requires access to the reasons behind a harmful outcome. Finck's analysis of AI liability and consumer law highlights that consumers and injured parties are often structurally disadvantaged because they lack access to the information necessary to understand how an AI system caused harm (14). Bertolini likewise emphasizes that civil liability frameworks must respond to the informational asymmetry between victims and technologically sophisticated actors (15). In Iraqi and Iranian legal contexts, where civil claims generally require the claimant to establish essential elements of liability, opacity may produce a practical denial of compensation unless evidentiary rules, presumptions, or risk-based liability mechanisms are developed.

Civil liability traditionally performs several legal functions. It compensates injured persons, allocates loss, deters harmful conduct, expresses legal condemnation of wrongful behavior, and encourages actors to adopt reasonable precautions. In both Iraqi and Iranian civil law, liability is fundamentally connected to the idea that unjustified harm should not remain without remedy. However, the doctrinal routes to liability may differ depending on whether the claim is contractual or non-contractual. Contractual liability may arise where AI systems are provided through service agreements, software licenses, medical contracts, financial services, consumer transactions, or professional engagements. Tort liability may arise where there is no contractual relation between the injured party and the responsible actor, such as a pedestrian harmed by an autonomous vehicle or a citizen harmed by an automated administrative system. Hubbard's discussion of sophisticated robots shows that liability analysis must consider the interaction between contract, tort, regulation, and insurance when advanced systems create foreseeable but difficult-to-attribute risks (16). This insight is highly relevant to AI systems because many harms emerge at the boundary between private contractual use and broader social risk.

The classical elements of liability, namely fault, damage, and causation, require reinterpretation in the AI context. Damage remains the least conceptually difficult element because AI may cause bodily injury, property damage, economic loss, reputational harm, privacy infringement, discrimination, and emotional distress. Mortazavi and Khodaeifam's discussion of AI, privacy, and civil liability indicates that AI-related harm is not limited to physical injury but may include violations of personal privacy and informational autonomy (17). The more complex elements are fault and causation. Fault may consist of negligent design, insufficient testing, defective data governance, failure to warn, inadequate monitoring, lack of human oversight, failure to update, or unreasonable reliance on automated outputs. Causation may require identifying the contribution of several actors across the system's lifecycle. Abbott's "reasonable computer" thesis challenges the traditional paradigm by asking whether liability should be assessed by comparing machine performance to human standards or by developing standards appropriate to computational decision-making (18). This debate is crucial for Iraqi and Iranian law because both systems must decide whether the standard of care should remain human-centered or become technology-sensitive.

A key theoretical debate concerns whether AI systems should be conceptualized as products. Product liability appears attractive because many AI harms arise from defective design, defective manufacturing, inadequate instructions, or failure to warn. However, AI systems differ from ordinary products because they may change after deployment, interact with new data, or produce outputs not fixed at the time of sale. Marchant's analysis suggests that tort law will face pressure to move beyond conventional product-defect categories because AI-related harms often arise from adaptive functionality rather than a simple manufacturing flaw (3). Wagner's approach similarly indicates that autonomous AI may require special liability rules because the risk does not always correspond to a traditional defect but to the very operation of a complex autonomous system (6). In Iraqi and Iranian law, where product liability doctrines are not always as specialized as in some Western systems, courts may instead rely on general principles of harmful act, causation, guarantee, and responsibility for dangerous activity. This flexibility may help, but it also creates uncertainty.

Another possible conceptual model is to treat AI as a dangerous object or hazardous activity. This approach shifts attention from moral blame to risk creation. If an actor introduces a system capable of causing serious harm and benefits from its operation, that actor may be required to bear the resulting loss even without proof of subjective fault. Eidenmüller's analysis of robots and the law of humans argues that legal systems must consider how risk allocation should evolve when autonomous technologies produce benefits for some actors while distributing risks

to others (19). The European Parliament's work on civil liability for AI also reflects the tendency to distinguish high-risk AI systems from lower-risk systems and to consider stricter liability for the former (20). For Iraqi and Iranian law, a risk-based approach may be doctrinally justified through general principles of harm prevention, guarantee, and responsibility for activities that create abnormal danger. Yet such a model must be carefully limited, because excessive liability could burden innovation and create unfair responsibility for actors who had no meaningful capacity to prevent the harm.

The debate over AI legal personality remains conceptually important but practically limited for civil liability. Granting AI systems independent legal personality might appear to solve the attribution problem, but it risks producing an empty form of responsibility if the AI lacks assets, moral agency, and meaningful accountability. Chesterman warns that AI legal personality may obscure rather than solve responsibility because it can shift attention away from the human and corporate actors who design, deploy, profit from, and control AI systems (9). Solaiman's analysis reinforces this concern by showing that legal personality is a constructed legal status that must serve practical and normative purposes, not merely reflect technological novelty (10). Balkin's account of robotics law also suggests that law should focus on the social relations surrounding robots and AI rather than treating machines as isolated legal subjects (21). From the perspective of Iraqi and Iranian civil law, it is therefore more coherent to locate liability among human and institutional actors connected to the AI system rather than attributing responsibility to the system itself.

The ethical foundation of AI liability is also significant. Civil liability is not only a technical mechanism for compensation; it reflects a society's judgment about who should bear the cost of harmful innovation. Floridi's ethical framework for a good AI society emphasizes principles such as beneficence, non-maleficence, autonomy, justice, and explicability (22). These principles correspond to civil liability concerns because a legal system that allows AI-related harms to remain uncompensated undermines justice, while a system that imposes responsibility without clear standards undermines legal certainty. Sezavar and colleagues' discussion of AI literacy also indirectly points to a broader social issue: as AI systems enter education and professional life, users must understand both capabilities and limits in order to avoid unreasonable dependence on automated outputs (23). In civil liability terms, AI literacy may affect the standard of care expected from users, professionals, and institutions. A physician, teacher, judge, lawyer, or administrator who relies on AI without understanding its limitations may be negligent even if the system itself contributed to the harmful result.

Civil Liability Arising from AI Systems under Iraqi Civil Law and Iranian Law

The application of civil liability rules to AI-related harm in Iraqi and Iranian law requires identifying the responsible parties within the AI ecosystem. Unlike ordinary harms caused by a single individual, AI harms often emerge from a chain of actors. The developer may design the algorithm, the data provider may supply training material, the manufacturer may integrate the system into a device, the platform operator may distribute the service, the owner may control deployment, the user may activate the system, and a professional may rely on its recommendation. Lemley's work on autonomous AI is particularly relevant because it shows that liability becomes difficult when no single human actor fully controls the system's output at the moment harm occurs (7). In Iraqi and Iranian law, this difficulty must be resolved through doctrines of direct causation, indirect causation, fault, guarantee, and joint responsibility. Where several actors contribute to harm, courts must decide whether liability should be individual, proportional, joint, or based on the actor best positioned to prevent the harm.

In Iraqi civil law, general tort principles provide a starting point for AI liability. Harmful acts, unlawful conduct, and compensable damage may allow courts to impose responsibility where a person causes injury to another. These general provisions are flexible enough to cover new technological harms, but their effectiveness depends on how courts interpret fault and causation. If an AI system causes harm because a developer failed to test it adequately, a fault-based claim may be possible. If a company deploys AI in a high-risk context without reasonable human oversight, negligence may be inferred. Scherer's analysis supports this approach by emphasizing that AI regulation must address risks through competence, monitoring, and institutional responsibility (2). However, if the harm results from an unpredictable interaction between a self-learning system and its environment, Iraqi courts may face difficulty in locating fault. Wagner's discussion of autonomous AI liability suggests that legal systems may need presumptions or stricter forms of liability where ordinary proof requirements make compensation unrealistic (6).

Iranian civil law offers several doctrinal resources for addressing AI harms. The Civil Liability Act and general civil law principles support compensation where a person causes material or moral harm through fault or unlawful conduct. In addition, Islamic jurisprudential concepts such as *daman*, direct causation, indirect causation, and the no-harm principle provide flexible tools for allocating responsibility. Keshavarz's analysis of Iranian law and EU documents indicates that Iranian law can engage AI liability through existing principles, but it requires clarification of the basis on which developers, operators, or users are responsible for AI performance (4). Where AI harm is directly linked to a human act, such as negligent deployment or misuse, traditional liability may be adequate. The more difficult case is where the AI system behaves in a harmful but technically autonomous manner. In such cases, Iranian law may need to rely on risk allocation, presumed fault, or guarantee-based reasoning to ensure that the injured person is not left without remedy.

The developer's liability is among the most important categories. Developers may be responsible where they design unsafe systems, ignore foreseeable risks, use biased or unreliable training data, fail to test the model in realistic conditions, or provide inadequate documentation. Abbott's discussion of the reasonable computer is relevant because it suggests that machine performance may need to be evaluated against standards of reasonableness adapted to AI rather than merely human negligence (18). In both Iraqi and Iranian law, developer liability may be grounded in fault where the claimant proves that the system was negligently designed or insufficiently tested. Yet the claimant may lack access to technical evidence, source code, model documentation, or training data. Finck's discussion of consumer vulnerability in AI contexts supports the need for evidentiary mechanisms that reduce the burden on injured parties when technical information is controlled by producers or service providers (14). Without such mechanisms, developer liability may exist in theory but fail in practice.

Manufacturer and product-integrator liability also deserves attention. AI systems are often embedded in physical products such as vehicles, medical devices, industrial machines, drones, smart home devices, and robotic assistants. When such products cause harm, liability may arise from defective design, defective production, inadequate warnings, or failure to update the system. Barfield argues that liability for autonomous robots must take into account the relationship between hardware, software, autonomy, and user interaction (13). Hubbard similarly shows that sophisticated robots require a legal framework that balances product liability, negligence, and regulation (16). In Iraqi and Iranian law, the challenge is that AI defects may not resemble ordinary product defects. A system may be technically functional but unsafe because it produces discriminatory, unpredictable, or contextually inappropriate outputs. This means that courts may need to recognize defects in data, model design, algorithmic governance, and post-market monitoring as legally relevant forms of defect.

The operator or user of an AI system may also bear liability. In many cases, harm occurs not because the AI was defectively designed but because the user deployed it in an inappropriate context or relied on it unreasonably. For example, a physician who follows an AI diagnosis without exercising professional judgment may be liable if the reliance falls below the expected medical standard of care. Montazeri and Shakrian's analysis of AI in pharmaceuticals demonstrates that professional and institutional users must remain attentive to the limits of automated systems in health-related contexts (5). Similarly, a bank that relies on an AI credit-scoring system without checking for discriminatory effects may be responsible for economic or dignitary harm. Calo's policy roadmap stresses that AI policy must focus on actual contexts of use because the same technology may create different risks depending on deployment (11). In Iraqi and Iranian civil law, user liability can be grounded in negligence, misuse, failure of supervision, or breach of professional duty.

A major issue is the liability of owners and beneficiaries. Where an AI system is used in a business operation, the enterprise that benefits from the system may be best positioned to insure against risk, monitor performance, and compensate victims. Eidenmüller's account of robots and the law of humans suggests that liability should consider who benefits from autonomous systems and who can efficiently manage their risks (19). This reasoning is compatible with risk-based liability and may be especially important for high-risk AI systems used in transportation, medicine, infrastructure, finance, and public administration. In Iraqi and Iranian law, courts may analogize such systems to dangerous objects or hazardous activities, particularly where the AI creates abnormal risks for third parties. European liability proposals also distinguish high-risk AI from ordinary systems and support stricter responsibility for operators of high-risk technologies (20). Such an approach could be adapted to Iraqi and Iranian law without necessarily abandoning the doctrinal foundations of civil liability.

Privacy and informational harm require separate attention because AI systems often process large volumes of personal data. Harm may arise from unauthorized data use, profiling, surveillance, identity inference, discriminatory classification, or disclosure of sensitive information. Mortazavi and Khodaeifam emphasize that AI use can affect personal privacy and generate civil liability where individuals suffer harm from improper data processing or intrusive automated systems (17). In Iranian law, privacy interests may be protected through civil liability principles, constitutional values, and sectoral rules, while Iraqi law may similarly address privacy harms through general principles of damage and unlawful conduct. The difficulty is that informational harm may be intangible, cumulative, and difficult to quantify. Gless's discussion of AI and legal responsibility indicates that legal systems must adapt to harms produced by algorithmic decision-making and automated processing, not only physical injuries (8). Therefore, compensation mechanisms must recognize non-material harm and loss of control over personal data as serious civil injuries.

The problem of causation is particularly complex in medical AI, autonomous vehicles, and algorithmic financial systems. Suppose an autonomous vehicle causes an accident after interpreting sensor data incorrectly. The harm may result from sensor failure, software error, environmental conditions, insufficient training data, driver inattention, or defective maintenance. Suppose an AI medical system recommends an incorrect treatment. The injury may result from poor training data, defective clinical integration, a physician's unreasonable reliance, or the hospital's failure to update the system. Bertolini's work on AI and civil liability indicates that multiple actors and uncertain causal pathways make ordinary liability analysis insufficient unless legal systems develop clearer allocation rules (15). In Iraqi and Iranian law, causation doctrines must therefore distinguish between direct causes, contributing

causes, intervening causes, and legally relevant risk creation. Where multiple causes combine, courts should avoid an all-or-nothing approach that leaves victims uncompensated merely because technical causation is complex.

Contractual liability also has a significant role. Many AI systems are provided through service agreements, licenses, subscription contracts, or professional service arrangements. A supplier may promise that an AI system performs at a certain level of accuracy, security, or reliability. If the system fails, the injured contractual party may claim breach of contract. However, AI providers often use disclaimers, limitation-of-liability clauses, and terms of service to restrict responsibility. Finck's analysis of EU consumer law is relevant because it shows that consumer protection concerns arise when technologically complex systems are offered under contractual terms that users cannot meaningfully negotiate or understand (14). In Iraqi and Iranian law, courts may need to scrutinize such clauses where they conflict with public order, good faith, mandatory liability rules, or protection of weaker parties. Contractual liability alone is insufficient, however, because many AI victims are third parties who never contracted with the provider.

The comparative analysis of Iraqi and Iranian law suggests that both systems possess flexible general principles but lack AI-specific clarity. Iraqi law may rely on general harmful-act liability, fault, compensation, and judicial discretion. Iranian law may rely on civil liability statutes, Civil Code principles, and jurisprudential doctrines of harm and guarantee. Yet neither system has a comprehensive legislative framework identifying duties of AI developers, operators, deployers, and users. Vatankhah's discussion of AI in civil procedure shows that AI is already entering legal processes and generating both opportunities and challenges for courts and legal institutions (24). This reinforces the need for legal modernization not only in substantive civil liability but also in evidentiary procedure. If courts are to adjudicate AI-related disputes, they must have access to expert evidence, technical documentation, algorithmic audit reports, and standards of explainability. Without procedural adaptation, substantive rights may remain ineffective.

Comparative and International Approaches to AI Civil Liability and Prospects for Legal Reform

Comparative and international approaches to AI civil liability provide useful models for Iraqi and Iranian law, although they cannot be transplanted mechanically. The European approach is especially important because it has moved toward risk classification, transparency duties, operator responsibility, and special liability mechanisms for high-risk AI. The European Parliament's report on a civil liability regime for artificial intelligence reflects the view that ordinary civil liability rules may be inadequate where AI systems operate autonomously and create significant risks (20). Bertolini's study for European legal affairs similarly argues that AI civil liability requires careful differentiation between types of systems, levels of risk, and responsible actors (15). For Iraq and Iran, the relevance of these approaches lies not in adopting European law wholesale but in understanding how comparative systems identify high-risk technologies, allocate burdens of proof, and protect injured persons in technically complex cases.

Strict liability is one of the most important reform models. Under strict liability, the injured party does not need to prove fault; it is sufficient to prove damage, causation, and the connection between the harm and a risk-bearing activity or system. Wagner's analysis of liability rules for autonomous AI supports the idea that strict or semi-strict liability may be appropriate where autonomous systems create risks that are difficult for victims to investigate (6). Eidenmüller also suggests that risk allocation must account for the fact that autonomous technologies may produce social benefits while imposing costs on individuals who did not consent to the risk (19). In Iraqi and Iranian law, strict liability could be introduced for high-risk AI systems such as autonomous vehicles, medical AI, industrial robotics,

public infrastructure AI, biometric identification systems, and algorithmic systems affecting fundamental rights. Such liability would not necessarily apply to all AI systems, because low-risk applications should not be subjected to excessive burdens.

Presumed fault offers another possible reform path. Under this approach, the claimant proves harm and the involvement of an AI system, while the developer, operator, or deployer must prove that reasonable care was taken. This model is less radical than strict liability because it preserves fault as the foundation of responsibility, but it adjusts the burden of proof to reflect informational asymmetry. Finck's work on AI and consumer law supports this concern because injured users often lack technical knowledge and access to internal system information (14). Scherer's analysis also suggests that regulatory systems must account for institutional competence, meaning that responsibility should be placed on actors capable of understanding and controlling AI risks (2). For Iraqi and Iranian courts, presumed fault could be especially useful where the defendant controls the technical evidence. If a hospital, bank, transport company, or platform uses AI, it should be required to show that the system was properly selected, tested, supervised, updated, and monitored.

Mandatory insurance is another important mechanism. AI-related harms may be severe, and responsible actors may be unable or unwilling to compensate victims fully. Insurance can distribute risk, guarantee compensation, and encourage safer practices through underwriting standards. Hubbard's analysis of sophisticated robots emphasizes that insurance may form part of a balanced liability system that supports innovation while protecting injured parties (16). Barfield's discussion of autonomous robots likewise indicates that liability and insurance should be considered together because robotic harms may involve uncertain causation and multiple actors (13). In Iraqi and Iranian law, mandatory insurance could be required for high-risk AI operators, especially in transportation, medical devices, industrial automation, and public service systems. Insurance would not eliminate liability but would ensure that victims are not deprived of compensation due to insolvency, evidentiary difficulty, or corporate avoidance.

Product liability reform is also necessary. Traditional product liability often focuses on physical products and tangible defects, but AI requires recognition of algorithmic defects, data defects, training defects, cybersecurity vulnerabilities, and failure to update. Marchant's work on AI and tort law shows that future liability disputes will increasingly involve harms that cannot be reduced to conventional manufacturing defects (3). Lemley similarly argues that autonomous AI creates liability problems because systems may act in ways that neither developer nor user specifically anticipated (7). For Iraqi and Iranian law, product liability reform should clarify that software, AI models, and AI-enabled services may be subject to liability when they produce unreasonable risks. The law should also recognize post-deployment duties, because an AI system may become unsafe after release due to new data, adversarial attacks, changed conditions, or discovered bias. A producer that fails to update or warn users after learning of risks should not escape liability merely because the system was initially functional.

Transparency and explainability obligations are central to liability reform. Without explainability, injured parties cannot prove causation, courts cannot assess fault, and regulators cannot evaluate risk. Floridi's ethical framework identifies explicability as a core principle of good AI governance (22). Calo's policy analysis likewise suggests that AI law must respond to the specific informational problems created by automated systems (11). In civil liability terms, explainability does not require that every system be perfectly interpretable in technical detail, but it does require meaningful documentation, auditability, recordkeeping, and traceability. Iraqi and Iranian law could impose obligations on developers and operators to preserve logs, document training data sources, identify known

limitations, record system updates, and provide courts with technical explanations when harm occurs. These duties would strengthen both prevention and compensation.

Human oversight should also be treated as a legal duty. AI systems should not be deployed in high-risk contexts without appropriate supervision by qualified persons. Turner's analysis of AI regulation emphasizes the continuing role of human responsibility even where machines perform autonomous functions (12). Gless similarly points to the challenge of assigning responsibility when automated systems intervene in legal or practical decision-making (8). In Iraqi and Iranian law, failure to maintain meaningful human oversight could be treated as negligence. A hospital that uses AI diagnosis without physician review, a court that relies on algorithmic assessment without judicial scrutiny, or a public authority that uses automated decision-making without appeal mechanisms may breach a duty of care. Vatankhah's work on AI in civil procedure is relevant here because it shows that AI can affect legal processes themselves, creating a need for procedural safeguards and professional accountability (24).

The question of AI legal personality should not be adopted as the primary reform solution. Although electronic personality has been discussed in some contexts, it risks weakening accountability by placing formal responsibility on a system that lacks assets, conscience, and social responsibility. Chesterman's critique of AI legal personality is persuasive because it shows that legal personality is not merely a convenient label but a legal institution with broader implications (9). Solaiman's comparison between robots and corporations also demonstrates that artificial legal personality is justified only when it serves clear legal purposes and is supported by institutional mechanisms (10). In Iraqi and Iranian law, a more appropriate approach would be to impose liability on natural and legal persons who create, own, operate, benefit from, or control AI systems. AI should be treated as a legally relevant source of risk rather than an independent bearer of responsibility.

The international literature also shows that AI liability must be connected with governance, literacy, and institutional capacity. Sezavar and colleagues' work on AI literacy among teachers points to a broader social reality: professionals increasingly interact with AI systems without necessarily possessing adequate understanding of their limitations (23). In legal terms, this suggests that training and competence should affect liability. A professional user who deploys AI in a sensitive field without sufficient knowledge may be negligent. Montazeri and Shakrian's discussion of pharmaceutical AI likewise illustrates that sector-specific expertise is essential when AI affects health and safety (5). For Iraq and Iran, legal reform should therefore be accompanied by professional standards, licensing requirements, technical training, and institutional audit systems. Civil liability alone cannot regulate AI effectively unless it is supported by preventive governance.

A suitable reform model for Iraqi and Iranian law should be hybrid. It should preserve fault-based liability for ordinary AI uses where negligence can be identified, adopt presumed fault where technical opacity prevents victims from proving internal defects, and impose strict liability for high-risk AI systems whose operation creates serious risks for life, health, property, privacy, or fundamental rights. Keshavarz's analysis supports the view that Iranian law can draw from European documents while adapting reform to domestic legal principles (4). Mortazavi and Khodaeifam's focus on privacy-related civil liability indicates that reform must also include non-physical harms (17). A hybrid model would be compatible with Iraqi and Iranian legal traditions because it would not abolish existing doctrines but would clarify how they apply to AI. It would also prevent two undesirable extremes: leaving victims uncompensated because fault is impossible to prove, and imposing unlimited liability that suppresses technological development.

The reform should also include evidentiary rules. Courts should be authorized to order disclosure of technical documentation, appoint AI experts, require algorithmic audit reports, and draw adverse inferences where defendants fail to preserve or provide relevant technical evidence. Abbott's argument about the reasonable computer shows that courts may need new standards to evaluate computational conduct (18). Balkin's robotics law framework similarly indicates that law must adapt institutional practices to technologies that reorganize relations between humans and machines (21). In Iraqi and Iranian courts, judges will need procedural tools to understand AI systems without becoming dependent on the parties' private experts. Specialized judicial training, expert panels, and technical guidelines could improve consistency and fairness. Without evidentiary modernization, even the best substantive liability rules may fail because claimants cannot prove what happened.

Toward a Comparative Liability Model for Iraq and Iran

A comparative liability model for Iraq and Iran should begin from the shared premise that civil liability must remain victim-centered while also maintaining fairness toward innovators and users. AI development produces social benefits, including improved diagnosis, efficient transportation, administrative automation, educational personalization, and economic optimization. However, these benefits cannot justify shifting the cost of harm to individuals who suffer injury without meaningful ability to prevent or understand the risk. Floridi's ethical approach to AI emphasizes that beneficial AI must be aligned with justice, non-maleficence, and explicability (22). Translating this ethical principle into civil liability means that those who create and profit from AI systems should bear corresponding duties of care, transparency, monitoring, and compensation. In Iraqi and Iranian law, this principle can be expressed through doctrines of harm prevention, fault, guarantee, and responsibility for risk.

The first element of the proposed model is classification of AI systems according to risk. Not all AI systems require the same liability regime. A simple recommendation system used for entertainment does not create the same legal danger as AI used in surgery, autonomous driving, financial trading, biometric surveillance, or judicial decision support. The European Parliament's liability framework is useful because it distinguishes high-risk AI from other systems and considers stricter rules where the probability and severity of harm are greater (20). Scherer's work also supports risk-sensitive regulation because AI systems vary widely in complexity, autonomy, and potential harm (2). Iraqi and Iranian legislators could adopt a similar classification model, defining high-risk AI by reference to the nature of the sector, the degree of autonomy, the type of protected interest affected, the scale of deployment, and the difficulty of human oversight. This would allow the law to impose heavier duties where they are justified while avoiding unnecessary burdens on low-risk innovation.

The second element is a duty-of-care framework for AI actors. Developers should be required to design systems according to accepted technical standards, test them in realistic conditions, document limitations, reduce foreseeable bias, protect cybersecurity, and provide clear warnings. Operators should be required to deploy systems only in suitable contexts, maintain human oversight, monitor performance, preserve logs, and suspend use when serious risks appear. Professional users should be required to understand the limits of AI outputs and avoid blind reliance. Calo's roadmap is relevant because it stresses that AI policy must identify the practical contexts in which AI systems interact with law and society (11). Turner's regulatory analysis likewise supports the continuing importance of human responsibility even when AI performs autonomous functions (12). In Iraqi and Iranian law, these duties could be codified or developed judicially through standards of reasonable conduct.

The third element is differentiated liability. Ordinary AI systems could remain subject to fault-based liability, where the injured party proves negligence, damage, and causation. Medium-risk systems could be subject to presumed fault, requiring the defendant to prove that reasonable care was exercised. High-risk systems should be subject to strict liability, particularly where they operate autonomously and may cause serious harm. Wagner's model of autonomous AI liability supports differentiated legal treatment based on the level of risk and the need for effective compensation (6). Bertolini's civil liability study also suggests that AI liability should not be governed by one undifferentiated rule but should reflect system type and risk level (15). For Iraq and Iran, this differentiated model is preferable because it respects existing civil liability principles while providing stronger protection in cases where traditional proof burdens are unrealistic.

The fourth element is recognition of data-related liability. AI systems depend on data, and defective, biased, incomplete, unlawful, or poorly governed data may produce harmful outputs. A credit-scoring AI trained on discriminatory data may deny loans unfairly; a medical AI trained on unrepresentative data may misdiagnose certain populations; an educational AI may misclassify students due to culturally biased indicators. Finck's consumer-law analysis shows that AI harms may arise from informational asymmetry and opaque automated processing (14). Mortazavi and Khodaeifam's analysis of privacy and AI-related civil liability further supports the need to recognize informational harm as a compensable legal injury (17). Iraqi and Iranian law should therefore impose duties on data controllers, developers, and operators to ensure lawful data acquisition, data quality, privacy protection, bias mitigation, and documentation. Where data defects contribute to harm, liability should not be limited to the final user if earlier actors created the risk.

The fifth element concerns medical and pharmaceutical AI. This area deserves specific regulation because AI errors may directly affect life, bodily integrity, and health. Montazeri and Shakrian show that AI use in pharmaceuticals generates complex civil liability problems involving producers, medical professionals, institutions, and technology providers (5). In both Iraqi and Iranian law, medical AI should be treated as high-risk when it affects diagnosis, treatment, drug prescription, surgery, or patient monitoring. Hospitals and medical institutions should be required to validate systems, train users, maintain human review, and inform patients when AI materially contributes to decision-making. Physicians should not be relieved of professional responsibility merely because an AI system recommended a course of action, but developers and suppliers should also be liable where technical defects, inadequate warnings, or poor data governance contributed to the injury. This shared responsibility model is more realistic than placing the entire burden on either the doctor or the software provider.

The sixth element concerns AI in legal and administrative procedures. AI may be used to classify cases, predict litigation outcomes, assist judicial research, automate public services, or support administrative decisions. Vatankhah's analysis of AI in civil procedure identifies both opportunities and challenges, showing that legal systems must ensure fairness, transparency, and procedural accountability when AI enters adjudicative contexts (24). In Iraqi and Iranian law, AI should not replace judicial reasoning or administrative discretion in matters affecting rights without meaningful human review. If an automated legal or administrative system causes harm through unlawful denial of benefits, discriminatory classification, procedural exclusion, or erroneous decision-making, liability should attach to the institution deploying the system. Gless's work on AI in criminal sentencing and civil liability reinforces the broader point that algorithmic involvement in legal decisions requires special safeguards (8). Civil liability should therefore be connected with due process, appeal rights, and explainability.

The seventh element is rejection of independent AI liability in favor of human and institutional responsibility. While the legal personality debate is theoretically interesting, it should not dominate reform in Iraq and Iran. Chesterman's critique demonstrates that AI legal personality may create conceptual confusion and practical evasion of accountability (9). Solaiman's analysis likewise shows that legal personality should not be granted merely because robots or AI systems resemble autonomous actors (10). In the Iraqi and Iranian contexts, responsibility should remain attached to legal persons and natural persons who design, deploy, own, operate, supervise, or profit from AI systems. AI itself may be treated as a source of risk, an instrument, a product component, or a technological process, but not as an independent debtor of compensation. This approach better protects victims and preserves doctrinal coherence.

The eighth element is mandatory documentation and auditability. A party that deploys AI should be required to preserve evidence necessary for liability analysis. This includes system logs, update histories, data governance records, testing reports, warnings, user instructions, and records of human intervention. Abbott's work suggests that assessing computational reasonableness requires evidence about how the system was expected to perform and how it actually performed (18). Lemley's discussion of autonomous AI reinforces the importance of understanding the system's behavior over time because autonomy complicates prediction and control (7). Iraqi and Iranian courts should be empowered to require disclosure of such evidence subject to confidentiality protections. Where a defendant fails to preserve essential records, courts should be able to presume that the missing evidence would have supported the claimant's case. This evidentiary rule would reduce the imbalance between injured persons and technology providers.

The ninth element is compensation and insurance. Civil liability should not be purely symbolic; it must produce actual compensation. High-risk AI operators should maintain insurance or financial guarantees sufficient to cover foreseeable harms. Eidenmüller's risk-allocation analysis supports placing responsibility on those who benefit from robotic and autonomous systems (19). Hubbard's work also supports integrating liability with insurance to manage innovation-related risks (16). In Iraq and Iran, mandatory insurance could first be introduced in sectors where AI-related harm is most foreseeable and severe, such as autonomous transportation, healthcare, industrial robotics, and infrastructure management. Compensation funds could also be considered where causation is uncertain but the harm is clearly linked to a class of high-risk AI systems. Such mechanisms would protect victims without requiring every case to depend on difficult proof of individual fault.

The final element is legal education and institutional capacity. AI liability cannot function effectively if judges, lawyers, experts, regulators, and professional users lack sufficient understanding of AI systems. Sezavar and colleagues' work on AI literacy highlights the broader educational dimension of AI governance (23). Balkin's robotics law perspective also suggests that law must evolve institutionally as machines become embedded in social relations (21). Iraqi and Iranian legal systems should therefore develop judicial training, expert registries, interdisciplinary research centers, and regulatory guidance. Civil liability reform should not be limited to statutory amendment; it must also include procedural modernization, professional standards, and public awareness. Without such institutional capacity, courts may either overestimate AI and treat it as infallible or underestimate its complexity and treat it as an ordinary tool. Both approaches would distort liability analysis.

Conclusion

The civil liability arising from the use of artificial intelligence systems represents one of the most important challenges facing contemporary private law. AI systems alter the traditional relationship between human conduct, harmful outcome, and legal responsibility because they may operate with autonomy, opacity, adaptive capacity, and distributed technical control. These characteristics do not eliminate human responsibility, but they make responsibility more difficult to identify through classical legal categories. The central challenge for Iraqi and Iranian civil law is therefore not whether AI-related harm should be compensable, but how liability should be attributed when harm emerges from complex interaction among developers, manufacturers, operators, users, data providers, institutions, and automated systems.

The analysis shows that existing Iraqi and Iranian civil liability rules provide a valuable foundation but are not fully sufficient for advanced AI systems. General doctrines of fault, damage, causation, compensation, harmful act, guarantee, and responsibility for risk can be interpreted to cover many AI-related harms. Where a developer negligently designs a system, where an operator deploys it without supervision, where a professional relies on it unreasonably, or where an institution uses it in a context that creates foreseeable danger, traditional liability can operate effectively. However, these doctrines become strained where the injured person cannot prove the internal cause of the harm, where the system's behavior changes after deployment, where multiple actors contribute to the risk, or where the harm results from opaque algorithmic processing.

The comparative examination of Iraqi and Iranian law indicates that both systems need a more explicit and risk-sensitive liability framework. A purely fault-based model is inadequate for high-risk AI because it places an excessive evidentiary burden on victims who lack access to technical information. At the same time, a universal strict liability model would be too broad because not all AI systems create the same level of danger. The most appropriate solution is a hybrid model that preserves fault-based liability for ordinary cases, applies presumed fault where technical opacity and informational asymmetry make proof difficult, and imposes strict liability for high-risk AI systems capable of causing serious harm to life, health, property, privacy, or fundamental rights.

The proposed model should identify the duties of all major actors in the AI lifecycle. Developers must design, test, document, and update systems responsibly. Manufacturers and integrators must ensure that AI-enabled products are safe and accompanied by adequate warnings. Operators must deploy systems only in appropriate contexts and maintain monitoring and human oversight. Professional users must understand the limits of AI and avoid blind reliance on automated outputs. Data providers and controllers must ensure data quality, legality, privacy protection, and bias mitigation. Institutions that benefit from AI systems should not be allowed to externalize the costs of harm onto individuals who neither created nor controlled the risk.

The conclusion also confirms that AI should not be treated as an independent legal person for purposes of civil liability. Granting AI legal personality would not solve the compensation problem and could obscure the responsibility of human and institutional actors. AI systems do not possess moral agency, social accountability, or independent assets sufficient to justify making them primary bearers of liability. The more coherent approach is to treat AI as a legally relevant source of risk and to allocate responsibility among those who design, own, operate, deploy, supervise, and benefit from it. This approach preserves the human-centered structure of civil law while adapting it to technological complexity.

For Iraqi and Iranian legal systems, reform should include several concrete measures. Legislators should define high-risk AI systems and establish special liability rules for them. Courts should be given authority to order disclosure of technical documents, system logs, audit reports, update histories, and data governance records. Evidentiary presumptions should be introduced where the defendant controls the information necessary to prove causation or fault. Mandatory insurance should be required for high-risk AI activities, particularly in transportation, medicine, industrial robotics, infrastructure, and automated public services. Professional standards should be developed for AI use in medicine, law, finance, education, and administration. Judicial and regulatory institutions should receive technical training so that AI-related disputes can be resolved with accuracy and consistency.

The study ultimately concludes that civil liability law must evolve from a narrow focus on individual fault toward a broader model of risk governance, institutional responsibility, and effective compensation. AI systems should be encouraged where they serve human welfare, efficiency, and innovation, but their benefits must not be purchased at the expense of uncompensated harm. Iraqi and Iranian law can respond to this challenge by building on their existing civil liability principles while introducing modern rules for autonomy, opacity, data-related harm, high-risk deployment, and evidentiary access. Such reform would preserve doctrinal continuity while ensuring that private law remains capable of protecting rights in the age of intelligent systems.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Russell S, Norvig P. Artificial Intelligence: A Modern Approach: Pearson; 2021.
2. Scherer M. Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. Harvard Journal of Law and Technology. 2016;29(2):353-400.

3. Marchant G. Artificial Intelligence and the Future of Tort Law. *Journal of Tort Law*. 2018;11(1):1-25.
4. Keshavarz E. The Basis of Civil Liability for Factors Related to the Performance of Artificial Intelligence Systems in EU Documents and Iranian Law. *Legal Research Quarterly*. 2025;1(2):27-36.
5. Montazeri M, Shakrian A. Civil Liability for the Use of Artificial Intelligence in Pharmaceuticals. *Medical Law Scientific Research Journal*. 2024;18(59):487-501.
6. Wagner G. Liability Rules for Autonomous Artificial Intelligence. *Common Market Law Review*. 2019;56(3):645-80.
7. Lemley M. Liability for Autonomous Artificial Intelligence. *University of Illinois Law Review*. 2021(5):1545-80.
8. Gless S. Artificial Intelligence in Criminal Sentencing and Civil Liability. *Artificial Intelligence and Law*. 2016;24(2):107-29.
9. Chesterman S. Artificial Intelligence and the Limits of Legal Personality. *International and Comparative Law Quarterly*. 2020;69(4):819-44.
10. Solaiman SM. Legal Personality of Robots, Corporations, Identities and the Human Right to Identity. *Artificial Intelligence and Law*. 2017;25(2):155-79.
11. Calo R. Artificial Intelligence Policy: A Primer and Roadmap. *University of California Davis Law Review*. 2017;51(2):399-435.
12. Turner J. *Robot Rules: Regulating Artificial Intelligence*: Palgrave Macmillan; 2019.
13. Barfield W. Liability for Autonomous and Artificially Intelligent Robots. *Paladyn Journal of Behavioral Robotics*. 2018;9(1):193-203.
14. Finck M. Liability for Artificial Intelligence and EU Consumer Law. *European Review of Private Law*. 2019;27(2):237-58.
15. Bertolini A. Artificial Intelligence and Civil Liability. *European Parliament Legal Affairs Study*. 2020.
16. Hubbard FP. Sophisticated Robots: Balancing Liability, Regulation, and Innovation. *Florida Law Review*. 2014;66(5):1803-72.
17. Mortazavi SM, Khodaeifam H. Investigating the effects of using artificial intelligence on personal privacy and the resulting civil liability. *Modern Fiqh and Law Quarterly*. 2026;6(22):1-14.
18. Abbott R. The Reasonable Computer: Disrupting the Paradigm of Tort Liability. *George Washington Law Review*. 2020;86(1):1-45.
19. Eidenmüller H. The Rise of Robots and the Law of Humans. *Oxford Legal Studies Research Paper*. 2017(27):1-33.
20. European P. Civil Liability Regime for Artificial Intelligence. *European Union Legal Affairs Committee Report*. 2020.
21. Balkin J. The Path of Robotics Law. *California Law Review Circuit*. 2015;6:45-60.
22. Floridi L. AI4People—An Ethical Framework for a Good AI Society. *Minds and Machines*. 2018;28(4):689-707.
23. Sezavar M, Sezavar S, Sadraei M, Doostifar H, editors. *Artificial Intelligence Literacy in Elementary School Teachers*. Second International Conference on Law, Management, Educational Sciences, Psychology, and Educational Planning Management, Tehran; 2024.
24. Vatankhah P, editor *The role of Artificial Intelligence in civil procedure: Challenges and opportunities*. Seminar of the Judiciary Lawyers Center; 2025; Isfahan.