

How to cite this article:
Jasim Ali, S. & Gandomkar, R. (2027). Conditions for Civil Liability Arising from Artificial Intelligence under Iraqi and Iranian Law: A Comparative Study. *Journal of Historical Research, Law and Policy, 5*(2), 1-17. https://doi.org/10.61838/jhrlp.482

Article history:
Original Research

Dates:
Submission Date: 07 July 2026
Revision Date: 15 October 2026
Acceptance Date: 22 October 2026
First Pubication Date: 01 November 2026
Final Publication Date: 01 March 2027

Conditions for Civil Liability Arising from Artificial Intelligence under Iraqi and Iranian Law: A Comparative Study

1. Saifuldeen. Jasim Ali[1]: Ph.D. Candidate, Faculty of Law, University of Qom, Qom, Iran
2. Rezahossein. Gandomkar[2*]: Professor, Department of Private Law, University of Qom, Qom, Iran

*corresponding author's email: Rh.gandomkar@qom.ac.ir

ABSTRACT

The rapid development of artificial intelligence has created significant challenges for traditional rules of civil liability, particularly where autonomous and self-learning systems cause harm without a clearly identifiable human error. This study examines the conditions for establishing civil liability arising from artificial intelligence under Iraqi and Iranian law through a comparative legal approach. The research focuses on the traditional elements of civil liability, namely fault, damage, and causation, and evaluates their adequacy in addressing harms generated by autonomous technological systems. Particular attention is given to the difficulty of attributing fault where an artificial intelligence system produces an unpredictable output, the recognition and assessment of emerging forms of damage, and the problem of proving causation in situations characterized by algorithmic opacity and multiple contributing actors. The study further analyzes the attribution of liability among users, operators, developers, manufacturers, and institutions involved in the design and deployment of artificial intelligence systems. Under Iraqi law, the analysis highlights the potential adaptation of rules concerning responsibility for things and machinery through a functional concept of technological custody and control. Under Iranian law, the study emphasizes the relevance of compulsory guarantee, direct destruction, indirect causation, and the doctrine of the stronger cause in determining the party to whom the harmful result should legally be attributed. The comparative analysis demonstrates that neither legal system requires a complete abandonment of traditional civil-liability principles; however, both require doctrinal adaptation and clearer legislative guidance. The study concludes that liability should be allocated according to effective control, causal contribution, capacity to prevent harm, and benefit derived from the technological activity, while joint liability and evidentiary presumptions may be necessary in complex cases involving multiple actors and opaque algorithmic processes.

Keywords: *Artificial Intelligence; Civil Liability; Fault; Damage; Causation; Iraqi Law; Iranian Law; Comparative Law*

Introduction

Artificial intelligence has moved from the domain of experimental computing into fields in which automated systems participate directly in decisions capable of affecting property, physical integrity, economic interests, and legally protected expectations. The legal importance of this transformation does not arise merely from the increasing sophistication of computer programs, but from the degree of autonomy with which contemporary artificial intelligence systems may process information, identify patterns, generate recommendations, and in some

© 2027 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.

circumstances produce outputs without immediate human determination of each step in the decision-making process. Artificial intelligence may broadly be understood as the development of computational systems capable of performing functions that conventionally require aspects of human intelligence, such as learning, reasoning, pattern recognition, prediction, and decision-making (1). Modern machine-learning systems differ significantly from traditional deterministic software because their behavior may develop through training data and complex computational relationships rather than through a complete set of explicit instructions drafted in advance by a programmer. This technical development has substantial consequences for civil liability because traditional legal rules generally assume that harmful conduct can ultimately be traced to the behavior of an identifiable natural or legal person.

The growing autonomy of artificial intelligence therefore presents a structural challenge to conventional civil liability. In ordinary cases of human conduct, the court identifies the person responsible for an act, determines whether the person's conduct was wrongful or negligent when such a requirement exists, establishes the existence of legally compensable damage, and examines whether a causal relationship connects the wrongful conduct to that damage. Artificial intelligence complicates each of these stages. Where an intelligent system changes its responses on the basis of accumulated data, the eventual harmful output may not correspond directly to a specific instruction issued by the programmer, manufacturer, owner, operator, or user. The opacity of certain machine-learning systems creates an additional difficulty because the internal sequence through which an output was generated may not be readily intelligible even to technically sophisticated observers. The interpretability problem has therefore become central to legal discussions of artificial intelligence, particularly because highly accurate computational models may remain difficult to explain in terms accessible to human decision-makers (2). This difficulty is especially serious in civil litigation, where the claimant must ordinarily demonstrate the facts upon which liability is based.

The problem is not that artificial intelligence necessarily eliminates human involvement. On the contrary, an AI system is developed, trained, manufactured, marketed, purchased, deployed, maintained, updated, supervised, and used through a network of human and institutional activities. The difficulty lies in determining which of these activities should become legally decisive when a harmful result occurs. A defective training dataset may originate with one party, the underlying software architecture with another, hardware components with a manufacturer, system configuration with an institutional operator, and the final operational decision with an individual user. Civil liability systems developed primarily around human acts and conventional physical objects must therefore address harms arising from an interconnected technological process in which several actors may contribute to risk without any one actor having complete control over the final output. The legal inquiry consequently shifts from the simple question of who physically caused the harm to the more difficult questions of who created, controlled, intensified, or should legally bear the relevant technological risk.

This problem is particularly important in Iraqi and Iranian law because the two systems share important civil-law characteristics while relying on different doctrinal foundations in the organization of non-contractual liability. Iraqi civil law reflects a combination of codified civil-law doctrine and principles influenced by Islamic jurisprudence. The general structure of Iraqi civil liability developed through rules concerning unlawful acts, damage, causation, responsibility for things, and multiple parties contributing to harmful consequences. Al-Sanhuri's analysis of civil obligations profoundly influenced the systematic understanding of liability throughout Arab civil-law systems and emphasizes the relationship between wrongful conduct, injury, and legally relevant causation (3). Iraqi legal scholarship similarly treats civil liability as a mechanism through which the person whose legally attributable conduct

causes damage becomes obligated to repair that damage (4). These general principles are sufficiently broad to address conventional technological harm, but artificial intelligence raises the question whether they remain adequate where autonomous behavior makes proof of personal fault exceptionally difficult.

Iranian law presents a different but related doctrinal framework. Civil liability is influenced both by codified statutory rules and by Imami jurisprudential doctrines governing compulsory guarantee, direct destruction, causation, and responsibility for harmful consequences. Katouzian's treatment of obligations outside contract explains that Iranian civil liability cannot be reduced entirely to a single universal fault principle because different forms of responsibility rest on different legal and jurisprudential foundations (5). The rules of compulsory guarantee may impose responsibility in circumstances where the decisive consideration is the attribution of destruction or causation rather than proof of subjective blame. This feature potentially provides Iranian law with greater conceptual flexibility in addressing technologically generated harm. At the same time, the autonomy of artificial intelligence creates difficulty in determining whether the harmful result should be legally attributed to the user, operator, producer, programmer, institutional controller, or another participant in the technological chain.

Imami jurisprudence provides important conceptual tools for this inquiry. The distinction between direct destruction and indirect causation has long been used to determine which person should bear responsibility when several acts contribute to damage. Classical jurisprudential sources analyze the conditions under which liability follows from destruction of another person's property or interests and the circumstances in which an indirect cause may become legally responsible (6). The jurisprudential treatment of causation also recognizes situations in which the apparent immediate actor does not necessarily constitute the legally stronger cause of the damage (7). These principles become relevant in the AI context because the individual physically using an intelligent system may be the immediate participant in the event, while the decisive technological cause may originate in the system's design, training, configuration, or algorithmic malfunction.

The legal question is therefore not whether traditional civil liability should be abandoned in the age of artificial intelligence. Rather, the central issue is whether its established conditions can be interpreted and adapted in a manner capable of protecting injured parties without imposing arbitrary liability on persons who had no meaningful capacity to prevent the harmful event. Civil liability must preserve a balance between compensation, fairness, technological development, and legal certainty. An excessively strict requirement of proving individualized human fault may leave victims uncompensated where opaque autonomous systems prevent identification of the precise error. Conversely, automatic attribution of every AI-related harm to the immediate user could impose disproportionate responsibility on a person who merely relied on a system that appeared to function correctly. The comparative examination of Iraqi and Iranian law is therefore valuable because it reveals different doctrinal pathways through which liability may be reconstructed without necessarily creating an entirely new legal personality for artificial intelligence.

The legal personality of artificial intelligence is not the primary solution to this problem. Current civil liability theory remains centered on natural and legal persons capable of bearing rights, duties, and financial obligations. Treating an intelligent machine as an independently liable entity would not automatically solve the compensation problem because liability is meaningful only where a person or legally recognized entity possesses assets or insurance against which the injured party may recover. The more practical inquiry concerns the allocation of responsibility among the human and institutional actors that create and benefit from AI-generated risks. Khader's analysis of civil liability arising from medical robots illustrates how advanced technologies can place pressure on traditional rules of

attribution when autonomous systems intervene between the conduct of professionals and the eventual damage (8). Although medical applications provide particularly visible examples, the underlying problem extends to artificial intelligence generally wherever autonomous or semi-autonomous systems participate in decisions capable of causing legally cognizable harm.

Against this background, the objective of this study is to examine the conditions for establishing civil liability arising from artificial intelligence under Iraqi and Iranian law and to determine whether the traditional requirements of fault, damage, and causation remain capable of addressing harms generated by autonomous and learning systems. The study also seeks to identify the persons to whom such harm may legally be attributed and to evaluate whether doctrines concerning custody, direct and indirect causation, stronger causation, and multiple responsible parties can provide satisfactory solutions. The comparative approach is based on the doctrinal structure of Iraqi civil liability and the statutory and Imami jurisprudential foundations of Iranian law. The analysis concentrates on non-contractual civil liability and excludes broader questions concerning criminal liability, intellectual property, administrative regulation, data governance, and the general ethics of artificial intelligence except where necessary to explain the operation of civil liability.

The research proceeds from the proposition that artificial intelligence does not render traditional civil liability irrelevant, but exposes weaknesses in rules originally developed on the assumption that harmful decisions are transparent and predominantly human. The analysis therefore focuses on the degree to which existing rules can accommodate technological autonomy and on the points at which legislative clarification becomes necessary. The comparison between Iraq and Iran is especially useful because Iraqi law offers doctrines concerning responsibility for things and machinery, whereas Iranian law provides a developed jurisprudential framework concerning destruction, causation, and compulsory guarantee. Examining these approaches together makes it possible to identify both common difficulties and distinct doctrinal advantages in dealing with AI-related harm.

Legal Foundations of Civil Liability for Artificial Intelligence in Iraqi and Iranian Law

Civil liability for artificial intelligence cannot be evaluated adequately without first identifying the legal characteristics of the technology that distinguish it from conventional instruments. Traditional machines generally perform functions predetermined by mechanical construction or explicit commands. Where a conventional machine causes damage, legal analysis can ordinarily focus on a manufacturing defect, maintenance failure, operational negligence, or misuse. Artificial intelligence systems, particularly those based on machine learning and deep learning, introduce a more complex relationship between human control and technological output. Such systems may process large quantities of data, detect statistical relationships, and alter the manner in which they generate predictions or recommendations as a result of training. Russell and Norvig describe artificial intelligence through the broader concept of intelligent agents capable of perceiving environments and selecting actions directed toward specified goals (1). From the perspective of civil liability, the legally significant characteristics are therefore not intelligence in a philosophical sense but functional autonomy, adaptability, complexity, and the reduced ability of human actors to predict individual outputs.

The distinction between conventional automation and learning systems is important because responsibility for a conventional program can usually be traced to explicit instructions. If a programmer directs a system to perform a particular action under particular circumstances, an erroneous result can potentially be examined against that predetermined instruction. Machine-learning systems may instead generate outputs through complex mathematical

relationships developed from training data. The resulting model may perform successfully in most situations while producing an unexpected harmful output in an unusual case. The interpretability problem described in machine-learning literature demonstrates that the reasons for a model's decision may not always be capable of straightforward human explanation (2). In civil liability, this creates a proof problem because the injured person may be able to establish that an AI system produced a harmful outcome but remain unable to identify precisely which technical defect, data deficiency, design decision, or operational intervention produced that outcome.

Iraqi civil law approaches non-contractual harm through the general law of obligations. The basic purpose of civil liability is compensatory: where legally attributable conduct causes damage to another, the person responsible must repair the resulting injury. Al-Hakim's explanation of the sources of obligations situates harmful acts among the principal sources from which an obligation to compensate may arise (4). The conventional analysis therefore requires an examination of wrongful conduct or another recognized basis of responsibility, the existence of damage, and a causal relationship between the legally relevant conduct and the damage. Al-Dhanoun explains civil fault through the deviation of conduct from the standard legally required in comparable circumstances, thereby linking liability to an objective evaluation of behavior (9). This framework functions effectively where the harmful event can be connected to the conduct of a natural person whose behavior can be compared with an expected standard of care.

Artificial intelligence challenges this model because the system itself cannot readily be subjected to the human standard of fault. A machine does not possess legal consciousness, moral discernment, or personal duties in the conventional sense. It would therefore be conceptually artificial to describe an algorithm as negligent in precisely the same manner as a human being. The legal inquiry must instead move outward from the machine to the persons responsible for designing, manufacturing, deploying, supervising, maintaining, or using it. A programmer may be negligent in developing code; a manufacturer may release an inadequately tested system; an operator may fail to perform necessary updates; an institution may deploy a system outside its intended environment; and a user may disregard warnings or rely unreasonably on an AI output. In such cases, ordinary fault principles remain applicable because the conduct under examination is human or institutional rather than algorithmic.

The more difficult case occurs where none of these actors can be shown to have departed from an established standard of care and the damage nevertheless results from an autonomous AI output. Iraqi doctrine then faces a tension between the compensatory purpose of civil liability and the claimant's burden of identifying a legally attributable basis of responsibility. The Iraqi approach to responsibility for things and mechanical devices provides an alternative doctrinal route. The civil-law tradition has long recognized that certain objects generate risks that justify shifting the evidentiary burden away from the injured party. Al-Sanhuri's broader treatment of liability for things explains the movement from exclusively fault-centered responsibility toward forms of liability associated with control, custody, and the creation of risk (3). This concept becomes particularly significant for artificial intelligence because control over an intelligent system may justify responsibility even where the injured person cannot prove the precise internal technological defect.

Custody, however, must be reconsidered in the context of AI. Traditional custody assumes meaningful physical and operational control over an object. The custodian can inspect it, maintain it, prevent misuse, and often understand the risks associated with its operation. An advanced AI system may be physically located within an institution while its software, training, updates, remote services, and algorithmic processes remain controlled by other parties. Physical possession therefore does not necessarily correspond to effective technological control. The

party that operates the hardware may have little influence over the architecture of the software, while the manufacturer or developer may retain significant control through updates and technical restrictions. Consequently, applying the ordinary concept of custody mechanically could result in responsibility being imposed on the party least capable of preventing the defect.

Iranian civil liability is based on a combination of statutory rules and jurisprudential principles concerning compulsory guarantee. Katouzian emphasizes that obligations arising outside contract encompass several doctrinal bases and cannot always be explained exclusively through subjective fault (5). Iranian law distinguishes circumstances in which liability follows from the direct destruction of another's protected interest from situations involving indirect causation. This distinction is especially important because direct destruction traditionally creates a particularly strong basis for guarantee. The person to whom destruction is legally attributed may be obligated to compensate even where intentional wrongdoing is absent. Katouzian's analysis of compulsory guarantee therefore demonstrates the objective characteristics of certain forms of Iranian civil responsibility (10).

The jurisprudential foundation of direct responsibility can be traced to classical principles concerning the destruction of another's property or protected interests. Al-Muhaqqiq Al-Hilli discusses liability arising from destructive acts as part of the broader jurisprudential system of guarantee (6). Similar discussions in major Imami jurisprudential works emphasize that the obligation to compensate may follow from the attribution of destruction independently of a modern negligence analysis (7). This objective dimension offers a potential advantage in AI cases because the injured party may not need to reconstruct the mental state of a responsible person. Nevertheless, it immediately produces another problem: if the immediate harmful act was generated by an autonomous machine, to whom should that act be attributed for the purpose of guarantee?

If AI is legally treated as an instrument, the harmful act may be attributed to the person or legal entity using the system. This approach is comparatively simple when the system merely executes human commands. It becomes less convincing when the system's autonomous output could not reasonably have been anticipated by the user. Attributing every outcome to the operator would effectively transform the operator into an insurer of the system's behavior, regardless of the operator's technical capacity or degree of control. Iranian law must therefore distinguish between cases in which AI functions as a subordinate instrument and those in which the decisive causal contribution lies in the design, programming, training, or technological architecture created by another party.

The doctrine of indirect causation provides greater flexibility for this purpose. Imami jurisprudence has long addressed cases in which a person does not directly inflict the harm but creates the conditions through which the damage occurs. The legal significance of the indirect cause depends upon the relationship between that cause and the ultimate harmful event. Al-Hurr Al-Amili's compilation of jurisprudential traditions contains foundational materials concerning guarantee and harmful causation within the Imami tradition (11). These principles support a legal analysis that looks beyond physical immediacy and examines the effective contribution of different actors to the production of damage.

The comparison between Iraqi and Iranian law therefore reveals two potentially complementary approaches. Iraqi law can respond to AI risk through the doctrines of fault and responsibility associated with custody or control of dangerous or mechanically complex things. Iranian law can employ the jurisprudential distinction between direct destruction and indirect causation and may, in appropriate circumstances, impose guarantee without requiring proof of conventional subjective fault. Neither system, however, completely resolves the problem of autonomous AI. Iraqi law must determine who qualifies as the meaningful custodian where control is technologically distributed, while

Iranian law must identify the person to whom destruction or causation should legally be attributed where an algorithm intervenes between human conduct and damage.

The legal foundations of both systems therefore remain relevant but require functional interpretation. The appropriate inquiry should concentrate not only on physical possession or immediate action but also on technological control, capacity to prevent harm, creation of risk, economic benefit, and the role of each participant in the design and operation of the AI system. This approach preserves continuity with established civil-liability doctrine while recognizing that artificial intelligence changes the factual structure within which those doctrines operate. The conditions of liability must accordingly be examined in greater detail through the traditional elements of fault, damage, and causation and through the specific attribution problems created by autonomous decision-making.

Conditions for Establishing Civil Liability for AI-Related Harm

The first major condition associated with civil liability is fault, although its role differs depending on the applicable doctrinal basis. In traditional civil liability, fault expresses the idea that a person has failed to conform to the conduct reasonably expected under the circumstances. Al-Dhanoun treats civil fault as a departure from the required behavioral standard, thereby combining the objective assessment of conduct with the legal obligation to exercise appropriate care (9). This concept remains readily applicable where AI-related damage can be traced to human negligence. A developer who fails to test foreseeable failure conditions, an operator who ignores required maintenance, an institution that deploys a system outside the environment for which it was designed, or a user who disregards clear warnings can all be evaluated according to conventional standards of conduct. Artificial intelligence does not eliminate fault in these circumstances; it merely creates new factual settings in which negligence may occur.

The difficulty appears where the harmful AI output develops despite reasonable conduct by identifiable human actors. Machine-learning systems may exhibit behavior that was not explicitly programmed and may respond unexpectedly to unusual data. The system's operation can therefore create a gap between human conduct and the harmful event. Russell and Norvig's account of intelligent systems demonstrates that advanced agents operate through interactions between goals, environmental information, learned models, and decision processes rather than through a simple sequence of fixed human commands (1). Where the harm results from an internal model response that could not reasonably have been predicted, it may be impossible to characterize the programmer, operator, or user as personally negligent. Requiring proof of fault in every such case could therefore deprive the injured person of compensation even though the technological activity created the risk that materialized.

The problem becomes more pronounced because artificial intelligence itself cannot coherently bear personal fault under existing civil law. Fault is a legal characterization linked to a person who is subject to duties and whose conduct can be judged against a required standard. An algorithm does not possess legal personality, patrimony, or independent civil obligations. Describing an AI system as "negligent" may be useful colloquially, but it does not identify a legally responsible debtor. The relevant legal task is thus to determine whether the fault lies in human conduct surrounding the AI system or whether liability should arise on an objective or presumed basis independently of individual fault. Khader's analysis of liability arising from robotic medical technologies highlights precisely this difficulty, particularly where an automated system contributes to injury even though the professional operator may have followed ordinary procedures (8).

Under Iraqi law, the difficulty of proving personal negligence creates a strong argument for relying on forms of responsibility based on custody and control rather than exclusively on proven fault. The general civil-law approach recognizes that persons responsible for machinery or things requiring special care may bear liability because of the risks connected with their control. Al-Sanhuri's analysis of responsibility for things reflects the broader juridical movement toward protecting victims where the mechanism causing harm lies within the sphere of another person's control (3). Applied to AI, this approach could reduce the claimant's evidentiary burden because the injured person would need to establish the system's causal role and the defendant's legally relevant control rather than reconstruct every technical error inside the algorithm.

Yet presumed or custody-based liability cannot be applied without qualification. If the hospital, company, employer, or other operator had no practical capacity to inspect or modify the AI model, treating that operator as exclusively responsible may be unjust. The legal meaning of control should therefore include not merely possession but the authority to determine deployment, maintenance, updates, data inputs, operational limits, and continued use. Where different parties control different components of the AI system, liability may need to be distributed rather than concentrated in the physical possessor. This conclusion follows from the technological structure of modern AI, in which the entity using the system may depend continuously on developers, manufacturers, cloud-service providers, or software suppliers.

Iranian law offers a different route because direct destruction may produce responsibility without a conventional inquiry into fault. Katouzian explains that certain forms of compulsory guarantee are based on attribution of the harmful result rather than negligence in the ordinary sense (10). This may provide stronger protection for victims where the direct harmful act can be legally attributed to an identifiable person. However, autonomous AI makes attribution itself difficult. If a person activates an AI system that subsequently makes an independent and unforeseeable decision, it is debatable whether the entire harmful result should be considered the person's direct act. A legal fiction that automatically equates activation with direct destruction would ignore the system's autonomous contribution.

Imami jurisprudential doctrine provides a more nuanced distinction between direct and indirect causation. Where a person directly destroys another's property or protected interest, liability may arise through the direct attribution of the result. Where the person's conduct merely creates a condition that later produces harm, the rules of causation become relevant. Al-Muhaqqiq Al-Hilli's treatment of guarantee demonstrates the jurisprudential importance of distinguishing direct destructive conduct from indirect causal participation (6). AI systems often occupy precisely this intermediate position: the user initiates or relies on the system, but the harmful output emerges through technical processes created by other actors. The legal characterization of each participant must therefore depend on the strength and proximity of that participant's causal contribution.

Damage constitutes the second indispensable condition of civil liability. Technological novelty does not eliminate the requirement that a claimant demonstrate legally recognizable harm. AI may cause bodily injury, property damage, financial loss, loss of opportunity, reputational injury, or other forms of harm depending on the context in which it is deployed. Conventional physical and economic damage presents relatively familiar problems. If an autonomous system damages property or produces a decision resulting directly in measurable financial loss, the principal challenge is not the existence of damage but attribution and causation. More difficult questions arise where AI causes probabilistic, cumulative, or opportunity-based harm.

Cumulative damage may occur where an AI system repeatedly makes small erroneous decisions whose harmful effects become apparent only after time. A system may continuously classify, recommend, adjust, or prioritize in a manner that produces no immediately observable injury but gradually creates substantial loss. The legal difficulty concerns both proof and temporal attribution. The claimant must establish that the cumulative outcome constitutes actual damage and that the damage arose from the relevant AI behavior rather than from independent intervening factors. The complexity of these cases reinforces the importance of access to technical records because the passage of time may make reconstruction of the system's behavior increasingly difficult.

Loss of chance creates an additional challenge. In certain situations, AI does not directly produce the ultimate harmful condition but reduces the claimant's probability of obtaining a favorable outcome. Khader discusses this problem in relation to medical technologies, where an erroneous automated output may cause delayed intervention and thereby diminish the patient's opportunity for recovery (8). The same logic may extend to other AI contexts where a system deprives a person of a genuine opportunity. The legal issue is whether the lost opportunity is sufficiently real and measurable to constitute compensable damage rather than mere speculation. Civil liability should not compensate hypothetical possibilities, but neither should it deny recovery where the lost chance possessed substantial practical value before the AI-related event.

Iranian jurisprudential doctrine raises distinctive questions concerning loss of benefit because classical principles distinguish actual damage from the mere failure to obtain an expected advantage. Katouzian's treatment of civil liability reflects the continuing importance of this distinction in determining compensable loss (5). AI-related disputes may therefore require careful evaluation of whether the claimant has suffered destruction of an existing interest, deprivation of a sufficiently certain benefit, or merely frustration of an uncertain expectation. The issue should be resolved by examining the degree of certainty, the legal protection afforded to the interest, and the demonstrable effect of the AI system on the lost opportunity.

Causation is perhaps the most difficult condition in AI liability. Civil responsibility requires more than the coexistence of technological malfunction and damage; the claimant must establish a legally sufficient connection between the relevant conduct or risk and the injury. Traditional causation doctrine assumes that evidence can identify the sequence leading from conduct to result. AI disrupts this assumption because the internal operation of complex models may be difficult to interpret. Doshi-Velez and Kim emphasize the technical challenge of producing rigorous explanations for machine-learning outputs (2). In litigation, this means that the claimant may know which system produced the harmful decision but remain unable to demonstrate exactly why the system produced it.

The black-box problem therefore creates an asymmetry of information. The injured person ordinarily has less access to software architecture, training datasets, technical logs, internal validation records, and system updates than the developer or operator. If conventional burdens of proof are applied rigidly, the claimant may lose the case not because causation is absent but because the technical evidence needed to prove it remains inaccessible. A sound civil-liability framework should therefore distinguish between genuine uncertainty about causation and evidentiary uncertainty produced by technological opacity controlled by the defendant. Where the defendant controls the relevant information, evidentiary rules may need to permit presumptions or burden shifting once the claimant establishes a plausible connection between the AI system and the damage.

Multiple causation intensifies the problem. A harmful AI output may result from the interaction of flawed training data, inadequate model design, an erroneous update, inappropriate institutional configuration, and user reliance. Iraqi civil-law doctrine recognizes that several actors may contribute to one harmful result. Al-Sanhuri's analysis of

causation emphasizes the need to identify legally effective causes rather than treating every historical condition as equally decisive (3). In AI cases, however, separating productive causes from background conditions can be technically difficult because the system operates as an integrated network. The legal solution should therefore avoid demanding an artificial selection of a single cause where several factors materially contributed to the harm.

Iranian jurisprudence provides a particularly relevant conceptual framework for competing causes. The traditional relationship between direct and indirect causes permits responsibility to be assigned according to the comparative strength of causal contributions. Al-Najafi's jurisprudential analysis recognizes the importance of determining the cause to which the harmful result should legally be attributed when several contributing factors are present (7). This doctrine may be especially useful where the immediate human operator plays only a minor role and the decisive harmful condition originates in the system's design or algorithmic structure. Conversely, where the user knowingly disregards limitations or misuses the system, the user's conduct may become the stronger causal factor.

Accordingly, the traditional requirements of fault, damage, and causation remain conceptually applicable to artificial intelligence, but their operation requires adaptation. Fault must focus on the conduct of persons surrounding the AI system rather than on the machine itself. Damage must encompass technologically generated harms while maintaining the requirement of certainty and legal protection. Causation must respond to opacity, distributed control, and multiple contributing actors. The essential problem is therefore not the disappearance of the traditional conditions of civil liability, but the need to interpret them in a way that reflects the factual structure of autonomous and learning systems.

Attribution and Adaptation of Civil Liability for Artificial Intelligence: A Comparative Analysis

Once fault, damage, and causation are established, the decisive question becomes the attribution of liability. Artificial intelligence rarely operates in complete isolation from human and institutional actors. The development and operation of an AI system commonly involve software designers, manufacturers, data suppliers, owners, institutional operators, professional users, maintenance providers, and other participants. Each may exercise a different form of control and contribute differently to the risk. A legally coherent liability regime should therefore resist the temptation to identify one universal defendant for every AI-related harm. Responsibility should instead be allocated according to the role played by each actor in creating, controlling, or failing to prevent the risk that ultimately materialized.

The user or operator represents the most immediate potential defendant because that person directly employs the AI system. In straightforward cases, ordinary civil-liability principles are sufficient. A user who deliberately employs the system in an unauthorized manner, ignores clear warnings, fails to provide required supervision, or relies on outputs in circumstances where independent verification is required may be personally at fault. Al-Dhanoun's objective conception of fault provides a suitable basis for evaluating whether the operator's conduct departed from what a reasonably careful person would have done under comparable circumstances (9). The standard of care should nevertheless reflect the operator's actual professional role and the information reasonably available at the time. It would be inappropriate to require an ordinary operator to detect hidden algorithmic defects that specialized developers themselves could not identify.

The liability of developers and manufacturers arises from a different source. These actors participate in creating the technological architecture through which AI-related risks emerge. Where damage results from defective design, inadequate testing, foreseeable weaknesses in training data, insufficient warnings, or failure to correct known

problems, conventional principles can attribute responsibility to those actors. Russell and Norvig's account of AI development demonstrates that the behavior of intelligent systems depends upon design choices, learning methods, environmental models, data, and performance objectives established through human engineering (1). The autonomy of a system therefore does not sever all connection with its creators. Autonomy may reduce the predictability of individual outputs, but the capacity for autonomous behavior is itself a product of design and deployment decisions.

At the same time, manufacturer liability should not become absolute merely because the system contains artificial intelligence. The fact that an AI system caused harm does not necessarily establish that it was defective. No complex technology can be guaranteed never to produce an adverse result, particularly where the system operates in uncertain environments. The legal analysis must therefore distinguish between acceptable technological risk and unreasonable defect. This distinction can be informed by the state of technical knowledge, testing procedures, known limitations, accuracy rates, availability of safer alternatives, warnings, and the intended operational context. Where the system behaved within known and adequately disclosed limitations, the mere occurrence of damage should not automatically establish manufacturer liability.

The institutional operator occupies an intermediate position between developer and individual user. Hospitals, companies, public authorities, and other organizations decide whether to adopt AI systems, determine the environment in which they will be used, establish internal procedures, provide training, maintain technological infrastructure, and often derive economic or organizational benefits from deployment. Khader's examination of medical robots demonstrates the significance of institutional responsibility where advanced technology is integrated into professional services (8). Similar reasoning applies outside medicine. An institution that selects and operates an AI system cannot avoid all responsibility merely by arguing that the underlying algorithm was created by an external supplier. Where the institution controls deployment and benefits from the activity, it should bear responsibility for risks falling within its operational sphere.

Iraqi law's concept of responsibility for things and mechanical machinery provides an important basis for institutional liability. The doctrine reflects the proposition that a person who exercises custody over a potentially harmful object may bear responsibility for damage caused by it. Al-Sanhuri's civil-law analysis links liability for things to practical control and the obligation associated with managing risks created by objects under one's authority (3). Artificial intelligence, however, requires this doctrine to be understood functionally rather than purely physically. Digital custody should be associated with the power to operate, configure, update, supervise, suspend, or determine the purposes for which the AI system is used.

Physical possession alone is insufficient because control over modern AI may be fragmented. An institution may possess the hardware while the developer retains the ability to modify the algorithm remotely. A user may initiate a task while the system's data processing occurs through external infrastructure. The manufacturer may control safety updates, whereas the institutional operator controls the data supplied to the model. Consequently, several parties may simultaneously possess different dimensions of technological custody. Iraqi law should therefore interpret custody as effective control over the source of risk rather than the mere location of the machine. Such an interpretation would remain consistent with the protective rationale of responsibility for things while avoiding arbitrary concentration of liability.

Iranian law can approach attribution through the doctrines of direct destruction and indirect causation. The central question is whether the harmful result should be legally attributed to the immediate user or to another actor whose

contribution was more decisive. Katouzian's discussion of compulsory guarantee emphasizes that liability depends substantially on the legal attribution of harm and not merely on chronological proximity (10). This is especially important in AI cases because the person who presses a button or accepts a recommendation may be only the last actor in a much longer causal chain. If the user's conduct was reasonable and the harmful result originated from a hidden algorithmic defect, treating the user as the exclusive direct cause would be inconsistent with the substantive distribution of control.

The jurisprudential principle concerning the relationship between a direct actor and a stronger indirect cause provides a valuable analytical tool. Classical Imami sources recognize that legal responsibility may shift where the indirect cause is more powerful in producing the result than the immediate act. Al-Muhaqqiq Al-Hilli's treatment of causation supports the broader proposition that the factual immediacy of an act does not invariably determine ultimate guarantee (6). Al-Najafi likewise discusses the attribution of liability where direct and indirect causes interact, demonstrating that jurisprudential doctrine is capable of evaluating comparative causal strength (7). In an AI case, the manufacturer or developer may therefore constitute the stronger cause where a concealed system defect overwhelmingly determines the harmful outcome and the operator merely uses the technology in the ordinary manner.

This doctrine should nevertheless be applied carefully. It would be inappropriate to assume that developers are always the stronger cause merely because they created the system. The relevant inquiry concerns the specific harm. If a user modifies safety settings, supplies obviously unsuitable data, ignores repeated warnings, or employs the AI system for an unauthorized purpose, the user's intervention may become the decisive cause. Conversely, if the system produces a harmful outcome because of a concealed defect that the operator could neither discover nor prevent, responsibility should move toward the party with greater technological control. The principle of stronger causation therefore offers a flexible method for aligning liability with actual risk creation.

Multiple responsible parties create another important issue. AI systems are often products of integrated supply and operational chains, making exclusive liability inappropriate. Iraqi civil-law principles concerning several contributors to a harmful act can support joint responsibility where the conduct of multiple persons materially contributes to the same damage. Al-Hakim's analysis of civil obligations recognizes that the structure of liability may involve several debtors where the harmful event cannot fairly be attributed to one person alone (4). Joint liability can protect the injured person from the impossible burden of determining the exact percentage of technological responsibility attributable to each actor before obtaining compensation.

A similar result can be justified within Iranian jurisprudential principles governing multiple causes. The traditional law of guarantee contains mechanisms for determining responsibility where several acts combine in producing harm. Al-Hurr Al-Amili's compilation of jurisprudential materials reflects the longstanding concern of Imami law with assigning responsibility among persons whose conduct contributes to destructive outcomes (11). Modern AI disputes can draw on this foundation by recognizing that several actors may jointly create the risk and that internal allocation among defendants should not prevent the victim from receiving compensation.

The evidentiary structure of AI cases also requires adaptation. The black-box problem means that developers and operators may possess information unavailable to injured persons. Doshi-Velez and Kim's discussion of interpretability illustrates why the internal basis of machine-learning decisions may resist straightforward explanation (2). Where a claimant has established that an AI system operated within the defendant's sphere of control, that the system produced or materially contributed to a harmful output, and that the technical evidence

necessary to identify the exact defect remains under the defendant's control, rigid insistence on conventional proof may produce systematic under-compensation. Courts should therefore be able to draw reasonable evidentiary presumptions from the defendant's control of technical information, particularly where logging, testing, or documentation that should have been maintained is unavailable.

Objective or risk-based liability may be justified for certain categories of high-risk AI. The rationale does not rest on the idea that every AI application is inherently dangerous. Rather, some systems operate in environments where malfunction can create serious bodily, financial, or social harm and where the injured person is structurally unable to assess or control the technological risk. In such circumstances, the person or institution introducing the system into the relevant activity may reasonably be required to bear the risk of unexplained malfunction. Khader's analysis of advanced robotic systems illustrates how the complexity of autonomous technologies may justify moving beyond exclusively fault-based approaches when victim protection would otherwise be ineffective (8).

Risk-based liability should, however, remain connected to effective control and benefit. The party best positioned to prevent, distribute, or insure against the risk should generally bear the principal burden. This may be the manufacturer in cases of design defects, the institutional operator in cases of deployment failure, the individual user in cases of misuse, or several parties jointly where the harm results from their combined conduct. Such an approach is preferable to granting independent legal personality to artificial intelligence because it maintains responsibility within the network of persons who create and benefit from the technological activity.

Insurance can complement but should not replace civil liability. Where AI systems create high-value risks, compulsory or specialized liability insurance can ensure that compensation is available even when technical disputes over fault and causation are prolonged. Insurance also distributes technological risk across a broader economic base. Nevertheless, insurance should follow an intelligible legal allocation of responsibility rather than conceal uncertainty about who ought to bear the risk. Civil liability must continue to perform its preventive and normative functions by connecting harmful technological activity to actors capable of adopting safer practices.

The comparative analysis therefore indicates that both Iraqi and Iranian law possess doctrinal resources capable of addressing artificial intelligence without abandoning established civil-liability principles. Iraqi law can develop the concept of custody toward a functional understanding of technological control and can employ joint responsibility where several actors contribute to the harm. Iranian law can use the doctrines of direct destruction, indirect causation, stronger cause, and compulsory guarantee to attribute responsibility according to substantive causal power rather than mere physical immediacy. Both systems nevertheless require clearer legislative guidance concerning autonomous systems, evidentiary burdens, distributed control, and the relationship between fault-based and objective liability.

The most appropriate model is therefore a differentiated system of attribution. Human fault should remain relevant wherever identifiable negligence can be established. Custody-based or risk-based responsibility should operate where high-risk AI causes harm within the sphere of a person who controls and benefits from its deployment. Developers and manufacturers should bear responsibility for defects within their technological sphere. Operators and users should remain responsible for negligent deployment or misuse. Where several actors materially contribute to the same harm, joint liability should protect the claimant while permitting subsequent internal allocation among responsible parties. Such an approach preserves the fundamental objectives of civil liability while adapting them to the technical realities of artificial intelligence.

Conclusion

Artificial intelligence creates a distinctive challenge for civil liability because it inserts an autonomous or semi-autonomous technological process between human conduct and harmful consequences. The fundamental difficulty does not arise from the existence of technology itself, since civil-law systems have long addressed harm produced through machinery and complex activities. The principal difficulty is that advanced AI may produce outputs through processes that are partially unpredictable, adaptive, technically opaque, and distributed among several actors. These features weaken the traditional assumption that a harmful event can always be traced to one clearly identifiable person whose conduct can be evaluated through conventional notions of fault and causation.

The comparative analysis demonstrates that the traditional conditions of civil liability remain relevant to AI-related harm. Fault, damage, and causation have not become obsolete. Rather, artificial intelligence exposes limitations in the manner in which these concepts have conventionally been applied. Fault remains appropriate where a developer, manufacturer, operator, institution, or user fails to comply with the standard of care required in designing, testing, deploying, supervising, maintaining, or using an AI system. The fact that artificial intelligence is involved should not prevent ordinary negligence principles from applying where human error is identifiable. The more difficult cases are those in which no individual fault can be proved because the harmful output results from autonomous technological behavior that was neither directly commanded nor reasonably foreseeable.

In such cases, exclusive reliance on proven fault can undermine the compensatory function of civil liability. A claimant may be able to establish that an AI system caused or materially contributed to damage while being unable to identify the precise technical failure responsible for the outcome. This problem is intensified by the informational imbalance between victims and those who develop or operate AI systems. The technical records, training information, software architecture, testing history, and internal decision logs necessary to explain the harmful event may remain exclusively within the control of developers, manufacturers, or institutional operators. Civil liability therefore requires evidentiary flexibility where technological opacity would otherwise make compensation practically impossible.

Damage remains an indispensable condition. AI does not create an independent category of injury simply because the harmful instrument is technologically advanced. The claimant must still establish a legally protected loss. Nevertheless, AI may generate forms of harm that are cumulative, probabilistic, delayed, or connected to the loss of a genuine opportunity. These characteristics require courts to examine damage according to its substantive reality rather than restricting compensation to immediate physical or economic injury. The requirement of certainty should continue to exclude purely speculative claims, but it should not prevent compensation where the claimant can demonstrate a real and measurable loss caused by the operation of an AI system.

Causation represents the most serious doctrinal difficulty. AI systems may involve numerous participants, including developers, manufacturers, data providers, owners, institutional operators, maintenance providers, and individual users. The harmful result may emerge from interactions among several of these actors rather than from a single isolated act. It is therefore frequently artificial to search for one exclusive cause. Civil liability should recognize multiple causation where several contributions materially participate in producing the damage. The decisive legal inquiry should concern the strength, relevance, and preventability of each causal contribution.

Iraqi law possesses significant resources for responding to these challenges. The rules governing harmful acts, responsibility for things and machinery requiring special care, and multiple responsible persons can be interpreted

to encompass artificial intelligence. The concept of custody is particularly important but should not be restricted to physical possession. In the context of artificial intelligence, meaningful custody should be understood through technological and operational control. The party capable of determining whether a system is deployed, how it is configured, whether it is updated, what data it receives, whether it remains in operation, and how its risks are managed exercises a form of control more legally significant than mere physical possession.

This functional understanding of custody is necessary because control over AI systems is often fragmented. A company or institution may own the hardware while a developer controls the software. A user may activate the system while a manufacturer determines its safety architecture. An external provider may control updates or data-processing infrastructure. Iraqi law should therefore avoid automatically assigning all liability to the immediate possessor. Liability should correspond to the specific dimension of control that produced or could have prevented the harmful event.

Iranian law offers a different form of flexibility through its jurisprudential principles of compulsory guarantee, direct destruction, indirect causation, and the comparative strength of causes. These doctrines are particularly valuable because they do not always make personal fault the sole basis of responsibility. They allow legal analysis to focus on the person to whom the harmful result should substantively be attributed. This approach can accommodate situations in which the immediate user of an AI system is not the true source of the risk. Where an operator uses the system properly but a hidden algorithmic defect determines the harmful outcome, the developer, manufacturer, or other technologically controlling party may represent the stronger cause.

The distinction between direct and indirect causation should therefore be interpreted in a technologically realistic manner. The person who physically activates a system should not automatically be treated as the direct and exclusively responsible cause simply because that person's action is closest in time to the damage. The legal analysis should consider whether the operator had meaningful control over the harmful process, whether the output could reasonably have been anticipated, whether the system functioned within its intended environment, and whether another actor created a more powerful causal condition. This approach is capable of preserving the jurisprudential foundations of Iranian law while adapting them to autonomous systems.

The comparison also demonstrates that neither Iraqi nor Iranian law should recognize artificial intelligence itself as the principal civilly liable person. Granting an AI system independent liability would not resolve the underlying problem of compensation because the machine does not possess an independent patrimony in the ordinary legal sense. More importantly, such an approach could weaken accountability by allowing manufacturers, operators, and institutions to transfer responsibility to the technological system through which they conduct their activities. Civil liability should remain attached to the natural and legal persons who create, introduce, control, supervise, or economically benefit from AI-generated risks.

The preferable approach is a differentiated model of responsibility. Where personal negligence is established, fault-based liability should apply. Where high-risk artificial intelligence causes harm that cannot reasonably be explained because of system autonomy or technological opacity, the law should permit forms of presumed, custody-based, or objective liability against the person who exercises effective control over the relevant risk. Manufacturers and developers should bear responsibility for defects in design, training, testing, or warnings. Institutional operators should be responsible for inappropriate deployment, inadequate supervision, failure to maintain the system, and risks connected with the operational environment under their control. Individual users should be liable where their own misuse, unreasonable reliance, or failure to comply with required procedures materially causes the damage.

Where several persons contribute to the harmful event, joint liability offers the most effective method of victim protection. The injured person should not be required to reconstruct the exact internal percentage of responsibility among developers, manufacturers, institutions, and users before obtaining compensation. Once the claimant establishes that several parties materially contributed to the same indivisible harm, the law should permit recovery without making technological complexity an obstacle to compensation. The defendants may subsequently seek internal allocation according to their respective contribution, degree of control, and fault.

The burden of proof also requires reform. A claimant should be expected to establish the occurrence of damage, the involvement of the AI system, and a plausible causal relationship between the system and the injury. Once these elements are demonstrated, the burden should not remain entirely on the claimant where the decisive technical information is controlled by the defendant. Courts should be permitted to infer causation or defect where required technical records have not been preserved or disclosed. This approach would not eliminate the need for proof; it would correct the structural imbalance created by technological opacity.

Both legal systems would benefit from specific legislative provisions addressing high-risk artificial intelligence. Such legislation should clarify the persons potentially responsible, the circumstances in which objective or presumed liability applies, the meaning of control or custody in digital environments, the treatment of multiple causal actors, and the evidentiary consequences of inaccessible algorithmic processes. Legislative reform should not attempt to replace the entire law of civil liability with a technologically isolated regime. Its function should instead be to connect established principles to the factual characteristics of autonomous systems.

Compulsory liability insurance may also serve an important complementary role for particularly high-risk applications. Insurance would increase the practical availability of compensation and prevent insolvency from defeating valid claims. It would also allow risk to be distributed among those who introduce advanced AI systems into economically beneficial activities. Insurance, however, should supplement rather than replace responsibility. The allocation of legal liability must remain clear so that developers, manufacturers, operators, and users retain incentives to reduce preventable risks.

Ultimately, the central principle should be that technological autonomy must not create a zone of legal irresponsibility. The increasing ability of artificial intelligence to act without direct human instruction may change the factual route through which damage occurs, but it does not eliminate the need to identify persons legally responsible for creating and controlling the relevant risk. Iraqi and Iranian law both contain foundations capable of responding to this development, although those foundations require interpretation and legislative clarification. Iraqi law can expand the concept of custody toward effective technological control, while Iranian law can make productive use of its doctrines of compulsory guarantee and stronger causation.

A balanced civil-liability framework should therefore protect injured persons without imposing indiscriminate liability on every participant in the AI chain. Responsibility should follow control, causal contribution, capacity to prevent harm, and benefit from the technological activity. Such an approach preserves fairness between victims and technology providers while encouraging responsible innovation. Artificial intelligence should not be treated as a reason to abandon traditional civil-liability principles, but as a reason to refine their application so that compensation and accountability remain effective in increasingly autonomous technological environments.

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. 4th ed: Prentice Hall; 2020.
2. Doshi-Velez F, Kim B. Towards a Rigorous Science of Interpretable Machine Learning. arXiv preprint2017.
3. Al-Sanhuri ARA. The Mediator in Explaining the New Civil Law. Beirut: Dar Ihya Al-Turath Al-Arabi; 1958.
4. Al-Hakim AM. A Summary of the Explanation of Civil Law. Baghdad: Nadeem Press; 1963.
5. Katouzian N. Civil Liability: Obligations Outside Contract. 10th ed. Tehran: University of Tehran Press; 2011.
6. Al-Muhaqqiq Al-Hilli JfbA-H. Shara'i Al-Islam fi Masa'il Al-Halal wal-Haram. 2nd ed. Qom: Isma'iliyan Publications; 1988.
7. Al-Najafi MH. Jawahir al-Kalam fi Sharh Shara'i' al-Islam. 7th ed. Beirut: Dar Ihya' al-Turath al-Arabi; 1981.
8. Khader TW. Civil Liability Arising from the Use of Robots in the Field of Medicine. Journal of Law. 2020;44(2).
9. Al-Dhanoun HA. Al-Mabsout fi Al-Mas'ouliya Al-Madaniyya. Baghdad: Al-Taymis Printing and Publishing Company; 1991.
10. Katouzian N. General Rules of Compulsory Guarantee. 3rd ed. Tehran: University of Tehran Press; 2016.
11. Al-Hurr Al-Amili MbA-H. Wasa'il Al-Shi'a ila Tahsil Masa'il Al-Shari'a. 1st ed. Qom: Al Al-Bayt Foundation for the Revival of Heritage; 1994.