Criminal Liability of Artificial Intelligence in the Iranian Legal System: A Legal–Jurisprudential Analysis of Emerging Challenges and a Comparison with Selected Legal Systems

1. Ahmad Reza Khazaei*: Department of Jurisprudence and Fundamentals of Islamic Law, CT.C., Islamic Azad University, Tehran, Iran

*Correspondence: ahm.khazaei@iau.ac.ir

Abstract

The expansion of artificial intelligence technologies, particularly learning, autonomous, and decision-support systems, has confronted criminal law with fundamental questions. The principal issue is determining which person or persons should bear criminal liability when the operation of an intelligent system results in the commission of an offence, bodily, financial, or reputational harm, a violation of privacy, or the generation of criminal content. In Iranian criminal law, criminal liability is founded on principles such as the legality of crimes and punishments, the personal nature of criminal responsibility, legal capacity, volition, the mental element, imputability, and causation. In Imamiyyah jurisprudence, doctrines and rules such as direct perpetration, causation, destruction of property, liability for damage, the rule of no harm, the rule of inducement or deception, the prohibition against harming others, and the requirement to establish intent and free choice in criminal liability and civil liability also play a significant role in analysing harmful conduct. Employing a descriptive–analytical method and adopting legal, jurisprudential, and comparative approaches, this study examines the status of artificial intelligence within the Iranian legal system, analyses the challenges associated with its criminal liability in light of jurisprudential foundations and criminal-law principles, and briefly considers the approaches adopted by the European Union, the United States, and the United Kingdom. The findings indicate that, under the current legal framework, artificial intelligence cannot be recognised as possessing independent criminal liability in the conventional legal sense, because such systems lack rational agency, moral will, criminal intent, legal capacity, and the ability to undergo punishment. Nevertheless, the natural or legal persons involved in the design, production, training, marketing, supervision, and operation of an artificial intelligence system may, depending on the circumstances, be held liable on the basis of criteria such as control, foreseeability, fault, causation, and attribution. Accordingly, the enactment of comprehensive artificial intelligence legislation in Iran, with due regard to the principles of criminal law, jurisprudential rules, and the regulatory requirements applicable to high-risk technologies, is an undeniable necessity.

Keywords: artificial intelligence, criminal liability, Iranian criminal law, Imamiyyah jurisprudence, causation, destruction of property, cybercrime, comparative law, legal personality.

Received: 02 March 2026
Revised: 07 July 2026
Accepted: 15 July 2026
Initial Publication 24 July 2026
Final Publication 01 November 2026

Citation: Khazaei, A. R. (2026). Criminal Liability of Artificial Intelligence in the Iranian Legal System: A Legal–Jurisprudential Analysis of Emerging Challenges and a Comparison with Selected Legal Systems. *Legal Studies in Digital Age*, 5(6), 1-11.

1. Introduction

Technological advancement has always led to transformations in legal rules. Just as the Industrial Revolution, the development of transportation, the emergence of the Internet, and the expansion of electronic commerce compelled legal systems to enact new regulations, artificial intelligence has now confronted criminal law with new challenges. Artificial intelligence systems are used in fields such as medicine, transportation, banking, commerce, education, security, industry, public services, and even the criminal justice system. By analysing extensive datasets, these systems can identify patterns and, in certain cases, make decisions without direct human intervention.

In traditional criminal law, liability is founded on the conduct of a human being who possesses volition, freedom of choice, understanding, and intent. The Islamic Penal Code likewise attributes criminal liability to a person who possesses legal capacity, attributable intent or fault, and has committed criminal conduct. In Islamic jurisprudence, criminal liability and liability arising from harm are also analysed on the basis of doctrines such as direct perpetration, causation, destruction of property, and the establishment of intent or fault. Accordingly, the emergence of systems that operate with a degree of self-learning capacity and independence has raised an important question: when harmful or criminal conduct is committed not directly by a human being but through an intelligent system, can the same traditional rules be applied?

For example, when an autonomous vehicle causes the death of a pedestrian, an artificial intelligence-based medical system provides an incorrect diagnosis, a banking algorithm makes a discriminatory decision, or an intelligent tool is used for forgery, fraud, defamation, the production of deepfakes, or computer intrusion, determining criminal liability requires a precise analysis of the roles of the programmer, manufacturer, supplier, owner, user, supervisor, and even the provider of the training data. In such cases, the issue is not merely technological; it is directly related to criminal justice, legal certainty, the preservation of public order, and the protection of citizens' rights.

The purpose of this study is to examine criminal liability arising from artificial intelligence through legal and jurisprudential approaches within the structural framework of the article. Accordingly, the concepts and general foundations of artificial intelligence are first explained. The foundations of criminal liability in Iranian law and Imamiyyah jurisprudence are then examined. Subsequently, the principal challenges associated with the criminal liability of artificial intelligence in the Iranian legal system are analysed. Finally, the approaches of selected legal systems and potential legislative solutions for Iran are considered.

2. Concepts and General Principles

2.1. The Concept of Artificial Intelligence

Artificial intelligence is a branch of computer science concerned with designing systems capable of performing tasks that previously required human intelligence, including learning, reasoning, pattern recognition, data analysis, prediction, decision-making, and natural language processing. The principal difference between intelligent systems and traditional software is that machine-learning systems can use new data to develop new patterns and modify their behaviour (Ghavamipour Sarshkeh & Mahmoudi, 2024).

From a legal perspective, the significant characteristic of artificial intelligence is its "relative autonomy in decision-making." As the degree of autonomy increases, attributing harmful conduct to a human being becomes more difficult. Nevertheless, technical autonomy does not amount to legal independence or criminal capacity. In jurisprudence, the mere production of an effect by an instrument does not render that instrument subject to legal duties or moral responsibility. Rather, it is necessary to determine which person acted as the direct perpetrator, cause, instructing party, supervisor, or negligent actor in bringing about the result (Javanmard & Heydarifard, 2025).

2.2. The Historical Development of Artificial Intelligence

The emergence of artificial intelligence as a scientific discipline is generally attributed to the Dartmouth Conference of 1956. Since then, advances in computer processing power, the development of the Internet, the production of big data, progress in deep-learning algorithms, and the expansion of cloud services have facilitated the widespread application of artificial

intelligence. Today, artificial intelligence has progressed beyond simple tools and plays a role in sensitive medical, financial, security, industrial, and judicial decisions (Ghavamipour Sarshkeh & Mahmoudi, 2024).

The legal significance of this development lies in the fact that the closer the decisions of a system come to affecting individuals' fundamental rights, the greater the need for regulation, supervision, transparency, and the determination of liability. For this reason, many legal systems have attempted to establish a balance between supporting innovation and preventing potential harm.

2.3. Types of Artificial Intelligence

Artificial intelligence may be divided into three general categories. The first is narrow artificial intelligence, which is designed to perform a specific task, such as voice assistants, facial-recognition systems, machine-translation systems, and image-analysis tools. The second is artificial general intelligence, which is theoretically capable of reasoning and making decisions across different domains in a manner comparable to human beings but has not yet been realised in practice. The third is artificial superintelligence, which is primarily theoretical and future-oriented and refers to systems that may surpass human cognitive capacities (Meghdadi & Pourcheriki, 2024).

From the perspectives of criminal law and jurisprudence, distinguishing between these categories is important because liability arising from a limited and controllable instrument is not identical to liability arising from a self-learning and unpredictable system. Nevertheless, in all three circumstances, until the legislature recognises legal personality and independent legal capacity for such a system, the principal focus of analysis remains the natural or legal persons involved in creating, controlling, and operating the system.

2.4. Applications of Artificial Intelligence

The applications of artificial intelligence have expanded into medicine, transportation, industry, banking, education, security, commerce, media, and judicial proceedings. In medicine, this technology is used to diagnose diseases, analyse medical images, recommend treatments, and conduct robotic surgery. In transportation, autonomous vehicles and intelligent traffic-control systems are prominent examples. In banking, algorithms are used for credit assessment, fraud detection, and risk management. In cyberspace, artificial intelligence can also be used to generate content, analyse data, and identify criminal activities (Reyshahri et al., 2025).

Despite these benefits, risks such as algorithmic error, data-driven discrimination, violations of privacy, cyberattacks, the production of deepfakes, document forgery, digital extortion, and the dissemination of false information have also increased. Therefore, the analysis of criminal liability associated with artificial intelligence must address both its legitimate use and its criminal misuse.

2.5. Criminal Liability Associated with Artificial Intelligence

The criminal liability associated with artificial intelligence concerns the possibility of attributing a crime or a criminal consequence resulting from the operation of an intelligent system to the responsible person or persons. Under the current state of Iranian law, as well as most other legal systems, artificial intelligence itself is not a direct subject of criminal liability because it lacks volition, knowledge, intent, freedom of choice, legal capacity, and the capacity to undergo punishment. Nevertheless, the individuals and companies involved in designing, producing, training, supplying, maintaining, supervising, and using the system may be held liable on the basis of fault, intent, negligence, recklessness, failure to comply with governmental regulations, causation, or direct perpetration (Ghavamipour Sarshkeh & Mahmoudi, 2024; Javanmard & Heydarifard, 2025).

From a jurisprudential perspective, an intelligent system should, at the present stage, be regarded primarily as an "instrument" or a "technical cause," rather than as an independent moral agent. When a person uses artificial intelligence to commit an offence, the system constitutes an instrument of the offence, and liability is attributable to the user. When harm arises from a design defect, inadequate training, defective data, or insufficient supervision, the doctrines of causation,

destruction of property, inducement or deception, and liability must be examined in relation to the manufacturer, programmer, or operator.

3. Foundations of Criminal Liability in Iranian Law

3.1. The Concept of Criminal Liability

Criminal liability refers to a person's obligation to answer for criminal conduct for which the law has prescribed punishment or a preventive or rehabilitative measure. Such liability is not established merely by the occurrence of a harmful result. It also requires the existence of the legal element, the material element, the mental element, criminal capacity, and the attributability of the conduct. In the Iranian legal system, the principle of legality of crimes and punishments, the personal nature of criminal liability, the principle of fault, and the requirement to establish causation constitute the principal foundations of criminal liability (Ardabili, 2022).

From the perspective of Islamic jurisprudence, legal obligation and criminal liability are founded on reason, maturity, freedom of choice, and knowledge. The principle of "lifting the pen" in relation to persons lacking legal capacity demonstrates the connection between liability, understanding, and volition. Therefore, any extension of criminal liability to emerging technologies must be approached cautiously and in light of these foundations. Although artificial intelligence is technically capable of processing information and making decisions, it does not possess reason in the jurisprudential sense, moral freedom of choice, or blameworthy intent. Consequently, its independent liability is incompatible with the present foundations of criminal law and Islamic criminal jurisprudence.

3.2. Constituent Elements of an Offence

Three fundamental elements are required for the commission of an offence. The first is the legal element, according to which no act or omission constitutes an offence unless the law recognised it as such and prescribed a sanction before its commission. This principle precludes an expansive interpretation to the detriment of the accused and is particularly important in the context of artificial intelligence because neither the system nor the persons associated with it may be punished merely on the basis of general concerns in the absence of an explicit legal provision.

The second is the material element, which concerns externally observable conduct. In offences involving artificial intelligence, the material element may take the form of designing a harmful algorithm, training a system with unlawful data, supplying an unsafe product, using an intelligent tool for criminal purposes, failing to exercise supervision, or failing to implement security updates.

The third is the mental element, which includes intent, knowledge, mens rea, or, in unintentional offences, negligence, recklessness, and failure to comply with applicable regulations. In cases involving artificial intelligence, the mental element must be sought not in the system itself but in the associated natural or legal persons. The court must therefore determine whether the relevant person knew or ought to have known of the risk, possessed the ability to exercise control, breached a legal or professional duty, and could have foreseen the result.

3.3. The Principle of the Personal Nature of Criminal Liability

The principle of the personal nature of criminal liability requires that no person be punished for the conduct of another. In the context of artificial intelligence, this principle prevents mere membership in the chain of production or use of a system, without proof of an effective and attributable role, from becoming a basis for liability. Accordingly, the liability of the programmer, manufacturer, company manager, owner, user, or supervisor must be assessed separately and on the basis of each person's actual role (Meghdadi & Pourcheriki, 2024).

Islamic jurisprudence also distinguishes between a direct perpetrator and a cause. If a user directly employs a system to commit an offence, the user is the direct perpetrator or, at minimum, the principal offender. However, when the result arises from a design defect or a failure of supervision, the manufacturer or operator may be regarded as a cause. Where a cause and a

direct perpetrator concur, jurisprudential and legal rules require the identification of the stronger and more effective causal contribution.

3.4. Conditions for the Establishment of Criminal Liability

The establishment of criminal liability under Iranian law requires legal capacity, volition, knowledge or fault, causation, and attributability. Artificial intelligence does not possess any of these conditions in the human and legal sense. Therefore, the recognition of direct criminal liability for the system is impossible without a fundamental change in the law.

Nevertheless, legal and jurisprudential rules allow the liability of associated persons to be analysed. If a programmer knowingly designs an algorithm for criminal use, the programmer's liability may be examined on the basis of intent. If a manufacturer markets a high-risk product without conducting the necessary tests, liability may arise from fault and causation. If a user knowingly employs the system to commit an offence, direct liability rests with that person. Moreover, if a manager or supervisor, despite being aware of the risk, fails to suspend or rectify the system, that omission may be examined within the framework of criminal liability.

3.5. The Relationship Between Criminal Liability and Technological Advancement

Criminal law cannot remain indifferent to technological developments, but it must not abandon its fundamental principles on the pretext of technological change. The appropriate solution is for the legislature to formulate specific regulations for artificial intelligence systems while preserving principles such as the legality of crimes and punishments, the personal nature of criminal liability, the principle of fault, and the requirement to establish mens rea or negligence.

Criteria such as the degree of control, foreseeability, the risk level of the system, the person's role in the decision-making chain, the possibility of prevention, compliance with professional and technical standards, algorithmic transparency, and the recording of system decisions may play a decisive role in determining liability. These criteria are compatible with the jurisprudential foundations of causation and liability because, in Islamic jurisprudence, a person who causes harm and whose customary causation and fault, transgression, or negligence are established may, depending on the circumstances, be held liable.

4. Challenges Associated with the Criminal Liability of Artificial Intelligence in the Iranian Legal System

4.1. The Absence of Independent Legal Personality for Artificial Intelligence

Under Iranian law, persons are divided into natural and legal persons, and the legislature has not yet recognised independent legal personality for artificial intelligence. The legal personality of companies and institutions is a legal construct whose effects are limited to those determined by law. Therefore, a simple analogy between a company and artificial intelligence cannot justify the recognition of independent criminal personality for an intelligent system.

From a jurisprudential perspective, criminal liability is also connected to legal obligation, reason, volition, and susceptibility to blame. Although artificial intelligence may demonstrate complex and unpredictable behaviour, it lacks moral consciousness and the capacity to comply with legal duties. Accordingly, recognising criminal personality for artificial intelligence under current conditions is compatible neither with jurisprudential foundations nor with the structure of the Islamic Penal Code. The legislature may, however, prescribe specific criminal liability or administrative and financial sanctions for legal persons that own or operate such systems.

4.2. The Challenge of Establishing Mens Rea

Mens rea, criminal intent, and awareness of the consequences of conduct are fundamental concepts in criminal law. Artificial intelligence makes decisions on the basis of data, models, and algorithms and lacks moral intention. Consequently, concepts such as intent, motive, malice, deception, or an intention to cause harm cannot be legally attributed to a system.

The correct approach is to seek the mental element in the associated persons. If a developer or user knowingly employs a system to commit an offence, mens rea may be established. If a person foresaw, or should reasonably have foreseen, a risk but failed to take the necessary measures, liability for an unintentional offence or fault-based liability may arise. This analysis is

also consistent with Islamic jurisprudence because, in cases of direct destruction, liability is generally established without the need to prove an intention to cause harm, whereas the establishment of intent or fault is of greater importance in criminal liability.

4.3. Difficulty in Attributing Criminal Conduct

One of the principal challenges is attributing criminal conduct within a complex chain of actors. The production and operation of an artificial intelligence system may involve a programmer, model designer, data supplier, hardware manufacturer, supplying company, owner, operator, end user, and technical supervisor. In such circumstances, attributing the result to a particular person requires a precise technical and legal analysis.

Under Iranian law, causation and attributability must be established. In Islamic jurisprudence, when several causes contribute to the occurrence of harm, the role of each cause and the strength of its contribution must be assessed. A court may not therefore hold every participant in the chain liable merely because a harmful result has occurred. Instead, it must determine which conduct, with what degree of influence, played what role in bringing about the result.

4.4. Liability of the Manufacturer

A manufacturer or developing company may be held liable when a design defect, security weakness, manifest error in training the model, absence of safety testing, provision of inaccurate information, or supply of a high-risk product without adequate warning has contributed to a criminal or harmful result. In such circumstances, liability may be assessed on the basis of causation, professional fault, failure to comply with regulations, and, in certain cases, the criminal liability of legal persons.

From a jurisprudential perspective, if a manufacturer causes harm and the result is customarily attributable to that manufacturer, the rules of causation and liability may be invoked. Furthermore, if a purchaser or user acts in reliance on confidence created by the manufacturer and inducement or deception is involved, the rule of inducement may also be considered in analysing civil liability and its consequential effects. Nevertheless, the criminal liability of the manufacturer requires proof of criminal fault, knowledge, or intent within the limits prescribed by law.

4.5. Liability of the Programmer

A programmer or algorithm designer may be held liable when that person's effective role in creating the risk or result is established. If the programmer knowingly designs code or an algorithm for the commission of an offence, such as a tool for criminal deepfakes, intelligent malware, or an intrusion system, direct criminal liability or complicity in the offence may be considered. If the error resulted from technical negligence or a breach of professional standards, unintentional criminal liability may arise where there is an applicable legal provision and a causal relationship.

However, the mere fact of being a programmer is insufficient to establish liability. Machine-learning systems may, after training or updating, exhibit behaviour that was unforeseeable at the time of design. Criteria such as the degree of control, foreseeability, compliance with standards, and awareness of the risk must therefore be assessed separately in each case.

4.6. Liability of the Operator or User

In many cases, the user or operator is the most significant responsible person because that individual or entity deploys the system in practice. When a person uses artificial intelligence to forge a document, generate criminal content, commit fraud, conduct computer intrusion, disseminate false information, defame another person, violate privacy, or incite the commission of an offence, the system is merely the instrument of the offence, and primary liability rests with the user (Reyshahri et al., 2025).

When the operator is an organisation or company, liability may, within the limits prescribed by law, arise not only for the natural person who made the decision but also for the legal person. In high-risk systems in particular, the operator must ensure human oversight, event logging, security updates, user training, and the suspension of the system when it enters a dangerous condition. Failure to comply with these requirements may constitute fault and causation.

5. Criminal Liability Associated with Artificial Intelligence in Selected Legal Systems

5.1. The Importance of Comparative Study

Comparative study enables the legislature to benefit from the experience of other legal systems and avoid repeating their mistakes. Artificial intelligence is a transnational phenomenon, and its effects are not confined to national borders. Therefore, examining the approaches of the European Union, the United States, and the United Kingdom may assist in developing Iran's criminal policy.

Nevertheless, the use of foreign experience should not lead to unprincipled imitation. The Iranian legal system has distinctive legal and jurisprudential foundations, and any comparative model must be compatible with the principles of the Constitution, the Islamic Penal Code, Imamiyyah jurisprudence, human dignity, privacy, and criminal justice.

5.2. The European Union's Approach

Through the adoption of its artificial intelligence regulation, the European Union has implemented a risk-based approach. Under this framework, certain applications of artificial intelligence are prohibited because they pose serious threats to fundamental rights, certain systems are classified as high-risk and subjected to stringent requirements, and lower-risk applications are subject to less burdensome requirements, such as transparency obligations. The regulation entered into force on August 1, 2024, while the full application of most of its provisions is scheduled to occur progressively (Ghavamipour Sarshkeh & Mahmoudi, 2024).

Importantly, the European Union has not recognised independent criminal liability for artificial intelligence as an offending person. Instead, it imposes obligations on providers, importers, distributors, deployers, and other persons involved in the artificial intelligence supply chain. This approach is relevant to Iran because, rather than granting criminal personality to the system, the liability of associated persons may be regulated on the basis of risk level, control, and fault.

5.3. The Approach of the United States

The United States does not yet have a single comprehensive federal law governing the criminal liability associated with artificial intelligence. The issue is primarily addressed through sector-specific regulations, guidelines issued by specialised agencies, product-liability rules, civil liability, computer-crime legislation, and general principles of criminal law. In criminal proceedings, when a user employs a system to commit an offence, direct liability rests with the user. When a design defect or the supply of an unsafe product contributes to the result, the liability of the company or manufacturer is examined within the relevant legal frameworks (Javanmard & Heydarifard, 2025).

A significant feature of the United States approach is its emphasis on the liability of natural persons and organisations and its reluctance to recognise independent liability for the system. This demonstrates that even in legal systems with more advanced technological capacities, traditional foundations of criminal liability have not been entirely abandoned.

5.4. The Approach of the United Kingdom

The United Kingdom has adopted a principles-based and relatively flexible approach to artificial intelligence regulation. Its policy documents emphasise safety, transparency, fairness, accountability, privacy, and the possibility of challenging automated decisions. Rather than enacting a single comprehensive statute applicable to every field, this approach relies to a certain extent on sectoral regulators and specialised standards.

Despite this difference in regulatory policy, the United Kingdom has not recognised independent criminal liability for artificial intelligence and continues to attribute liability to natural persons or organisations. This experience is important for Iran because it demonstrates that sector-specific regulation and professional standards can be used alongside comprehensive legislation (Ghavamipour Sarshkeh & Mahmoudi, 2024).

5.5. The Legal Position in Iran

Iran has not yet enacted specific legislation concerning the criminal liability associated with artificial intelligence. Consequently, potential cases must be addressed through the Islamic Penal Code, computer-crime legislation, electronic-commerce legislation, the Civil Liability Act, regulations governing legal persons, the Code of Criminal Procedure, and general legal principles (Javanmard & Heydarifard, 2025).

These laws may be applied in certain circumstances. For example, the criminal use of artificial intelligence in cyberspace may be prosecuted under existing computer-crime provisions. However, matters such as autonomous vehicles, robotic surgeons, independent decision-making algorithms, high-risk systems, defective training data, algorithmic transparency, and distributed liability throughout the supply chain require clearer and more specialised regulations.

5.6. Legal Recommendations for the Iranian Legislature

In light of legal and jurisprudential foundations, it is recommended that the Iranian legislature undertake the following measures: first, enact comprehensive artificial intelligence legislation based on levels of risk; second, provide precise definitions of an artificial intelligence system, a high-risk system, a provider, an operator, a supervisor, training data, and an automated decision; third, determine the liability of natural and legal persons on the basis of control, foreseeability, fault, causation, and attribution; fourth, require high-risk systems to record decisions and remain subject to auditing; fifth, prescribe proportionate criminal, administrative, and civil sanctions; sixth, amend computer-crime legislation to address offences such as deepfakes, intelligent forgery, and the misuse of training data; and seventh, establish specialised supervisory mechanisms and cooperation among legal scholars, Islamic jurists, computer specialists, and executive bodies.

Such legislation must avoid hasty criminalisation. The principles of proportionality, penal minimalism, transparency, support for innovation, and prevention of harm must be considered simultaneously. From a jurisprudential perspective, the rules of no harm, destruction of property, causation, inducement, preservation of the social order, and the prohibition against harming others may provide an appropriate theoretical foundation for regulating liability in the field of artificial intelligence.

6. Analysis of Emerging Dimensions of Criminal Liability Associated with Artificial Intelligence, Future Challenges, and Legislative Solutions

6.1. Criminal Liability Associated with Artificial Intelligence in Medicine

Medicine is one of the most important areas in which artificial intelligence is applied. Intelligent systems are used to diagnose diseases, analyse medical images, recommend treatments, predict the course of diseases, and perform robotic surgery. In this field, a system error may result in bodily injury or the death of a patient, making the determination of liability particularly important.

When artificial intelligence merely serves as an advisory tool for a physician and the final decision is made by the physician, primary liability, depending on the circumstances, rests with the physician or medical institution because the physician is required to assess the system's output in light of professional knowledge. However, if the system is designed or supplied in a manner that allows it to make consequential medical decisions without human oversight, the liability of the manufacturer, developing company, medical institution, and technical supervisor must also be examined (Javanmard & Heydarifard, 2025).

From a jurisprudential perspective, human life and health are among the most important legally protected interests, and medical intervention without compliance with technical standards may give rise to liability. If harm results from a physician's fault, a system defect, or the medical institution's negligence, the rules of causation, destruction of property, and liability may be relevant to the analysis. From a criminal-law perspective, it is also necessary to determine whether negligence, recklessness, or failure to comply with medical and technical regulations has been established.

6.2. Criminal Liability Associated with Autonomous Vehicles

Autonomous vehicles operate using cameras, sensors, radar, digital maps, and decision-making algorithms. If such vehicles cause death or injury, the roles of the driver or human supervisor, manufacturing company, software supplier, vehicle owner, and person responsible for maintenance must be examined.

If the driver or supervisor had the ability to intervene but failed to do so, that person's liability may be considered. If the accident resulted from a software defect, defective design, inadequate updating, or insufficient warnings, the liability of the manufacturer or developer may arise. If the vehicle owner failed to carry out necessary repairs or updates, that omission may also be relevant to causation (Ghavamipour Sarshkeh & Mahmoudi, 2024).

In Islamic jurisprudence, if an instrument is under a person's control and that person is negligent in maintaining or using it, liability may arise. The same logic should be applied to autonomous vehicles. Rather than treating the system itself as responsible, the analysis should focus on those persons who customarily possessed the capacity to control or prevent the harmful result.

7. The Role of Artificial Intelligence in Cybercrime

Artificial intelligence may be used as an instrument for committing cybercrime. The production of intelligent malware, phishing attacks, identity forgery, deepfake production, document forgery, extortion, computer intrusion, unauthorised access, dissemination of false information, and privacy violations are among the most significant conceivable examples (Reyshahri et al., 2025).

In such cases, criminal liability generally rests with the person who used the system to commit the offence. If the developer knowingly designed and supplied the tool for criminal use, the developer's liability may also be examined under the doctrines of direct perpetration, complicity, participation, or causation. Existing computer-crime legislation covers some of these forms of conduct, but amendment and supplementation of the legislation are necessary to address emerging technologies such as deepfakes and intelligent forgery.

7.1. The Challenge of Electronic Evidence in Artificial Intelligence-Based Offences

In offences involving artificial intelligence, proving the offence and the causal relationship is difficult because the system's decisions may result from millions of calculations and complex interactions among data. In certain deep-learning systems, even specialists cannot easily explain the precise reason for a particular output. This condition, sometimes described as the "algorithmic black box," creates difficulties for criminal proceedings.

To address this problem, high-risk systems should possess event-logging capabilities, auditability, documentation of training data, reporting mechanisms, a reasonable degree of explainability, and the capacity to provide authorised forensic experts with access to the necessary information. These requirements facilitate the discovery of the truth and help prevent both wrongful convictions and the evasion of liability by the person actually responsible.

7.2. Arguments for and Against Granting Legal Personality to Artificial Intelligence

Some scholars have proposed granting a limited form of legal personality to highly advanced systems. They argue that as autonomy increases, attributing every result to a human being becomes increasingly difficult. Nevertheless, this position faces serious obstacles in criminal law because punishment is connected to moral blameworthiness, volition, legal capacity, and the ability to undergo punishment (Javanmard & Heydarifard, 2025).

The prevailing view is that granting criminal personality to artificial intelligence would not only fail to resolve the problem but might also reduce the actual liability of companies and natural persons. From a jurisprudential perspective, legal obligation and blame have no meaning in relation to an entity lacking reason and free choice. Therefore, the more appropriate solution is to regulate the liability of persons involved in the artificial intelligence lifecycle with greater clarity and precision.

7.3. The Necessity of Comprehensive Artificial Intelligence Legislation in Iran

As the use of artificial intelligence expands, the absence of clear legislation may result in inconsistent judicial practice, legal uncertainty, reduced public confidence, and difficulties in compensating harm. Although existing Iranian laws may be invoked in certain cases, they are insufficient to address every issue associated with artificial intelligence. Comprehensive legislation must establish connections among criminal law, civil liability, data protection, privacy, cybersecurity, technological ethics, and technical standards.

In drafting such legislation, attention to jurisprudential foundations is essential. The rules of no harm, destruction of property, causation, inducement, preservation of the social order, prohibition against causing harm, the obligation to prevent probable serious harm, and the duty to observe trustworthiness in handling data may provide appropriate jurisprudential foundations for accountability in the field of artificial intelligence.

7.4. The Role of the Judiciary in Addressing Offences Arising from Artificial Intelligence

Alongside the legislature, the judiciary plays a significant role in managing the challenges posed by artificial intelligence. Cases involving this technology require technical knowledge, specialised expertise, and a precise understanding of the foundations of criminal liability. Establishing specialised judicial branches, training judges and law-enforcement officers, developing digital-evidence laboratories, formulating specialised guidelines, and employing independent experts may improve the quality of proceedings.

From the perspective of a fair trial, the court must be capable of distinguishing the role of each person within the system's operational chain and must avoid the generalised and unsupported attribution of liability. The accused must also have effective access to technical evidence and the opportunity to challenge expert reports.

7.5. The Role of Education and Public Awareness

Preventing offences involving artificial intelligence cannot be achieved through punishment alone. Educating users, programmers, company managers, physicians, engineers, judges, lawyers, and official experts plays an important role in reducing risk. Universities may train specialists by establishing interdisciplinary courses in technology law, the jurisprudence of emerging technologies, and the criminal liability of intelligent systems.

Public awareness of the risks associated with deepfakes, intelligent fraud, privacy violations, data misuse, and unjustified reliance on algorithmic outputs also constitutes an important instrument of social prevention.

7.6. The Future of Criminal Liability Associated with Artificial Intelligence

As intelligent systems become increasingly autonomous, criminal law will be required to define concepts such as fault, foreseeability, control, causation, human oversight, and safety standards with greater precision. Nevertheless, technological complexity must not lead to the abandonment of fundamental principles. The principles of legality of crimes and punishments, the personal nature of criminal liability, the requirement to establish the mental element or fault, and the prohibition against punishment without attribution must continue to be preserved (Javanmard & Heydarifard, 2025).

The future of criminal liability associated with artificial intelligence will probably move towards hybrid models combining the criminal liability of natural persons, the criminal liability of legal persons, administrative sanctions, civil liability, mandatory insurance, technical standards, and ex ante supervision of high-risk systems. Such a model would also be more consistent with Iran's legal and jurisprudential foundations than the recognition of independent criminal liability for an artificial intelligence system.

8. Conclusion

Artificial intelligence is one of the most significant contemporary technological phenomena. In addition to its extensive benefits, it has confronted criminal law with new challenges. The present analysis demonstrates that the Iranian legal system, on the basis of the Islamic Penal Code and the general principles of criminal law, attributes liability to a person who possesses

volition and legal capacity and whose intent or fault and attributable conduct have been established. In Imamiyyah jurisprudence, criminal liability and liability for harm are likewise analysed on the basis of reason, freedom of choice, direct perpetration, causation, destruction of property, fault, and the customary relationship between conduct and harm.

Accordingly, under the current legal framework, artificial intelligence cannot be assigned independent criminal liability because an intelligent system lacks moral volition, reason in the jurisprudential sense, mens rea, legal capacity, and the capacity to undergo punishment. This does not, however, mean that no liability exists for offences or harms arising from artificial intelligence. Liability must be attributed to the natural or legal persons involved in designing, producing, training, supplying, supervising, maintaining, and operating the system, provided that causation, fault or mens rea, and the attributability of the conduct to those persons are established.

The comparative analysis also demonstrated that the European Union, the United States, and the United Kingdom, despite differences in their regulatory approaches, have not recognised independent criminal liability for artificial intelligence. Instead, they primarily emphasise the liability of natural persons and organisations, safety standards, transparency, accountability, and supervision. These experiences may be useful for Iran, particularly because the Iranian legal system can draw upon jurisprudential rules such as the rule of no harm, destruction of property, causation, and inducement to develop a defensible domestic framework for liability arising from artificial intelligence.

Ultimately, the enactment of comprehensive artificial intelligence legislation in Iran is necessary. While preserving the fundamental principles of criminal law and jurisprudential foundations, such legislation should specify the liability of manufacturers, programmers, developing companies, operators, and users; subject high-risk systems to supervision; require algorithmic transparency and the recording of decisions; prescribe proportionate sanctions for misuse involving deepfakes, intelligent forgery, privacy violations, and emerging forms of cybercrime; and facilitate the safe, responsible, and Sharia-compliant use of this technology.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Ardabili, M. A. (2022). *General Criminal Law* (Vol. 1). Mizan Publishing.

Ghavamipour Sarshkeh, M., & Mahmoudi, M. (2024). An Introduction to Legal Frameworks for the Criminal Liability of Artificial Intelligence Systems. *Quarterly Journal of Legal Studies*.

Javanmard, M., & Heydarifard, S. M. (2025). Criminal Liability of Autonomous Artificial Intelligence with Emphasis on the Mental Element in Light of Comparative Studies. *Quarterly Journal of Legal Research*.

Meghdadi, M., & Pourcheriki, F. (2024). A Comparative Study of the Criminal Liability of Artificial Intelligence in the Legal Systems of Iran and Saudi Arabia. *Journal of Comparative Legal Studies*.

Reyshahri, M., Amirian Farsani, A., & Jalilian, M. (2025). Legal and Criminal Dimensions of Artificial Intelligence in the Criminal Justice System. *Quarterly Journal of Legal Studies*.