

AI-Fabricated Legal Personality: Agency Without Intent and the Legal Effects of Contracts

1. Reza Farajpour[✉]: Department of Law, Yas.C., Islamic Azad University, Yasuj, Iran

*Correspondence: r.farajpour@iau.ac.ir

Abstract

The expansion of generative models and autonomous artificial intelligence agents has given rise to an emerging form of forgery: the creation or appropriation of the identities of natural and legal persons and the conclusion of contracts in their names without any underlying human intent. Using an analytical-critical method and a comparative approach, this article first demonstrates why the fundamental concepts of legal personality, capacity, and agency in Iranian law are founded upon attributable intent and why the statistical output of an algorithm cannot be accommodated within any of these legal categories. It then examines the legal status of contracts concluded under machine-generated false identities and concludes that such contracts are absolutely void due to the absence of contractual intent and legal capacity, although invalidity alone provides no adequate remedy for a good-faith contracting party. The article makes two principal contributions. First, it develops a three-stage test for the attribution of liability, designed to allocate losses among the developer, operator, and intermediary platform on the basis of the legal doctrines of inducement, direct destruction of property, and indirect causation. Second, it formulates the paradigm of an “advanced instrument accompanied by a chain of liability,” which addresses existing legal gaps without conferring legal personality upon machines. Finally, ten legislative, technical, and institutional measures are proposed for the Iranian legal system.

Keywords: artificial intelligence, identity forgery, legal personality, contractual intent, civil liability, electronic contract.

Received: 01 March 2026

Revised: 12 July 2026

Accepted: 19 July 2026

Initial Publication 27 July 2026

Final Publication 01 November 2026



Copyright: © 2026 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Citation: Farajpour, R. (2026). AI-Fabricated Legal Personality: Agency Without Intent and the Legal Effects of Contracts. *Legal Studies in Digital Age*, 5(6), 1-14.

1. Introduction

Information technology has brought the legal world to an unprecedented turning point. Artificial intelligence—a phenomenon that is neither a living being nor endowed with human will—has moved beyond the confines of laboratories at a pace few could have predicted and has become firmly embedded in the economy, commerce, healthcare, and social relations. Its presence, however, is not invariably directed toward beneficial ends; its potential for misuse is no less significant than its beneficial applications.

Among the various forms of misuse, the fabrication of legal identity occupies a distinctive position. This concept refers to a situation in which an intelligent system—ranging from a large language model to an advanced chatbot or autonomous agent—

fabricates the identity of a natural or legal person and, in that person's name, concludes contracts, assumes obligations, or performs legal acts. What distinguishes this phenomenon from traditional forms of identity forgery is its scale, speed, and resistance to detection.

The history of law is not unfamiliar with identity forgery. From document forgery in ancient Rome to identity fraud in the digital age, human societies have developed various mechanisms to counter it. Nevertheless, generative artificial intelligence—particularly models such as GPT, Claude, and Gemini—has introduced an unprecedented quality of fabrication: identities that are indistinguishable from real human beings not only in appearance, but also in their informational, communicative, and behavioral characteristics.¹

The Iranian legal system possesses a framework consisting of the Civil Code enacted in 1928 and its subsequent amendments, the Electronic Commerce Act of 2003, and the Computer Crimes Act of 2009. This framework, however, was designed for the pre-artificial-intelligence era. It does not provide explicit and adequate answers to such fundamental questions as whether a contract concluded by a machine-generated false identity is void or merely ineffective pending ratification, and who must compensate a good-faith party for the resulting loss.

This article seeks, through an analytical-critical approach and by drawing upon the experience of leading jurisdictions, to clarify the dimensions of this challenge and identify possible solutions. To this end, it first examines the foundational concepts of legal personality, agency, and will from the perspective of Iranian law. It then analyzes the nature and forms of AI-based fabrication of legal identity. Subsequently, the effects of this phenomenon on contracts and civil liability are examined, and international approaches are studied comparatively. Finally, solutions are proposed to address the existing legal gaps.

2. Conceptual Framework: Legal Personality, Agency, and Will

2.1. Legal Personality in Iranian Law: Foundations and Elements

Legal personality is one of the central concepts of legal science and refers to an entity upon which the legal system confers the capacity to possess rights and bear obligations. Under Iranian law, persons are either natural persons or juridical persons, each of which is governed by its own specific rules.

The Iranian Civil Code links the commencement and termination of the capacity to enjoy rights to human life. Under Article 956, the capacity to possess rights begins when a human being is born alive and ends upon death. This provision establishes an important foundation: the capacity that constitutes a prerequisite of personality inherently belongs to a living human being. In the next step, Article 958 of the same Code recognizes every human being as entitled to civil rights, while prohibiting the total waiver of such rights or the complete deprivation of the ability to exercise them. This rule clearly demonstrates that, within the logic of the Civil Code, the enjoyment of rights is connected to living humanity rather than to every entity capable of action.

Juridical persons likewise possess a clearly defined legal status. Article 588 of the Commercial Code permits them to enjoy all rights and assume all obligations that the law recognizes for individuals, except those that, by their nature, are exclusive to human beings, such as parental and filial rights and duties.

The central point emphasized by this study is that both forms of personality—natural and juridical—rest upon a common foundation: the existence of attributable will. In a natural person, will is intrinsic and internal; in a juridical person, it is manifested through decision-making organs such as the board of directors, the general assembly, and the chief executive officer. An artificial intelligence system, regardless of its complexity, lacks will in the legal sense. Its outputs are products of statistical computation rather than the intent and consent that the Civil Code recognizes as fundamental conditions for the validity of a transaction. Recent comparative legal research similarly confirms that neither Iranian law nor European Union law provides a sound positive-law basis for recognizing an independent legal personality for intelligent systems, and that the consequences of such recognition would outweigh its potential benefits (Farajpour, 2025b).

¹ The concept of intention of creation has deep roots in Islamic jurisprudence. Early jurists, including Sheikh Ansari in *Makasib* and Mirza Na'ini in *Munyat-ul-Talib*, have linked that any offer or acceptance that has a serious intention to create a legal effect is only a word, not a contract. Therefore, the output of an algorithm in the form of a contractual offer is devoid of the true intention of creation.

2.2. *Will in Legal Philosophy and Its Distinction from Algorithmic Computation*

Classical legal philosophy, from Kant to Hegel, has understood will as the capacity of a rational being to make free and conscious decisions. In Iranian civil law, which has been deeply influenced by Islamic jurisprudence, the concepts of intent—meaning a conscious intention to perform an act—and consent—meaning internal satisfaction with that act—constitute the two essential components of legal will.

Allameh Na’ini and, subsequently, Professor Katouzian emphasized in their analyses of contracts that the intent to create legal effects constitutes an essential element of every contract. In its absence, what appears outwardly to be a contract is, in reality, fictitious and legally ineffective (Katouzian, 2019).

From the perspective of cognitive science, artificial intelligence performs processes that resemble decision-making but are fundamentally different in nature: they involve the statistical processing of data patterns. When a language model produces a sentence, it is actually predicting the most probable sequence of words on the basis of its training, rather than willing to say something or intending to assume an obligation (Danaher, 2020). This fundamental distinction between computation and will constitutes the theoretical foundation of this article and has an important legal consequence: any contract concluded by artificial intelligence without the express and specific authorization of the identity holder lacks genuine intent to create legal effects.¹

2.3. *Agency in Iranian Law: Types and Conditions*

Agency refers to an act performed by one person, the agent, in the name and on behalf of another person, the principal, with direct legal consequences for the principal. Iranian law recognizes several forms of agency.

The first is contractual agency, or mandate, regulated by Articles 656 to 683 of the Civil Code. The Civil Code defines mandate as a contract by which one party appoints another as a substitute for the performance of an act. Article 662 imposes two important restrictions: agency is permissible only in matters that the principal is legally capable of performing, and the agent must also possess the legal capacity necessary to perform the same act. The subject matter of the agency must also be specific and lawful under Article 664. As will be demonstrated, these capacity-based restrictions prevent machines from being accommodated within the legal structure of mandate.

The second is statutory agency, which the law assigns to designated persons such as guardians, custodians, or trustees. Articles 1180 to 1194 of the Civil Code regulate guardianship, while Articles 1218 to 1254 govern custodianship.

The third is organizational agency, which is defined within juridical persons through articles of association and internal regulations. For example, under Article 125 of the 1968 Amendment to the Commercial Code, the chief executive officer is the legal representative of a joint-stock company.

An artificial intelligence system has no place in any of these forms of agency. It cannot be a principal because it lacks legal capacity; it cannot be an agent in the legal sense because it neither comprehends the act nor possesses the capacity to perform it; and it cannot qualify as a statutory or organizational representative. This theoretical gap lies at the root of the existing legislative deficiency.

2.4. *The Theory of Algorithmic Agency: Definition, Dimensions, and Criticisms*

In response to the expanding use of artificial intelligence in legal domains, some scholars have advanced the concept of algorithmic agency. Allen was a leading contributor to this debate and argued that intelligent systems may act on behalf of human beings at three distinct levels (Allen, 2019).

At the first level, instrumental agency, artificial intelligence is merely a tool in human hands, such as order-processing software that executes predefined transactions. In this context, liability is unambiguous: the human user is responsible. At the second level, delegated agency, artificial intelligence operates within general instructions but enjoys relative autonomy in making detailed decisions, as in the case of a trading robot that buys and sells within a specified price range. At the third level, autonomous agency, the system makes decisions and acts without direct instructions in response to environmental conditions.

¹ Same as the previous source; also see Katouzian's analysis of the intention of the contract being a pillar in the fulfillment of the contract (Katouzian, 2019, Vol. 1).

Identity fabrication appears at this third level: an intelligent agent, without authorization, fabricates an identity and concludes a contract.

Critics of this theory, whose position is also adopted in the present study, argue that even at the third level no genuine agency exists, because agency requires both the agent's legally cognizable will and the principal's authorization, rather than merely the capacity for algorithmic decision generation (Muller, 2022). This distinction has practical consequences. If artificial intelligence is called an agent, it must be explained whose agent it is and from where its authority derives.¹ Experience with decision-support systems in adjudicatory contexts, including video assistant referee systems in sports, also demonstrates that legal systems ultimately attribute algorithmic error to the institutions and human actors behind the system rather than to the system itself (Farajpour, 2025a).

3. AI-Fabricated Legal Identity: Nature, Types, and Mechanisms

3.1. Definition and Nature of the Phenomenon

AI-fabricated legal identity is a situation in which an intelligent system, whether deliberately programmed by a person or employed as an instrument of misuse, fabricates the identity of an existing natural or legal person—or even creates an entirely fictitious identity—and then performs legal acts in the name of that identity. It may conclude a contract, assume an obligation, or confirm a transaction.

The difference between this phenomenon and traditional identity forgery is not merely formal; it concerns depth and scope. In terms of scale, while a human forger can ordinarily conceal themselves behind only one false identity at a time, an artificial intelligence system can create and manage thousands of fabricated identities simultaneously. In terms of quality, human fabrications typically leave detectable traces, whereas advanced models can generate identities that even experts may be unable to distinguish from authentic ones. In terms of endurance, a human forger becomes fatigued, while an intelligent system can operate continuously, around the clock.

3.2. Types of AI-Based Legal Identity Fabrication

A. Fabrication of the Identity of a Known Natural Person

In this form, artificial intelligence uses publicly available information—such as social media profiles, academic publications, and news reports—or leaked data to reconstruct the identity of a real and recognizable individual. The fabricated identity is then used in commercial interactions, contractual negotiations, or transaction confirmations.

A striking example was reported in 2023, when fraudsters used artificial intelligence to imitate the voice of the chief executive officer of a reputable company and instructed the company's financial manager to transfer USD 25 million to a designated account. The transfer was subsequently completed (European Banking Authority, 2023). In that incident, neither a document nor a signature was forged; what was fabricated was the vocal identity of a real human being.

B. Fabrication of the Identity of a Juridical Person, Company, or Organization

In this form, the system pretends to be the official representative of a company or organization. This type of fabrication is particularly dangerous in business-to-business commerce because commercial contracts are often concluded without face-to-face identity verification and through email or digital platforms.

From the perspective of Iranian law, the closest legal category is the unauthorized transaction regulated by Articles 247 to 256 of the Civil Code. A transaction concerning another person's property, unless conducted under guardianship, testamentary authority, or agency, is not legally effective. Even the owner's internal satisfaction is insufficient; the transaction becomes valid and effective only if the owner or their legal successor subsequently ratifies it. A fundamental difference, however, exists between a traditional unauthorized transaction and machine-based fabrication. In the former, the unauthorized actor is a natural person with actual will who acts for themselves or another; in AI identity fabrication, the unauthorized actor possesses neither legally cognizable will nor a genuine identity.

¹ The theory of algorithmic agency has been developed more in common law countries. In EU law, the term "electronic agent" was introduced in the 2000 E-Commerce Directive, but it has not yet reached a legally enforceable definition. Critics, including the authors, consider true agency to be dependent on self-awareness and volition, which algorithms lack; see Müller, V. C. (2022). Legal personhood for artificial agents. *Philosophy and Technology*, 35(2).

C. Creation of an Entirely Fictitious Identity

This form of fabrication may generate the most complex legal challenge. Artificial intelligence creates an entity that has no external existence: a name, background, profile, and even documents that are not registered in any official system but are designed so convincingly that they deceive the counterparty. These entirely fictitious personalities may become counterparties to online contracts. From the perspective of Iranian law, such a contract lacks one of its parties from the outset—the fabricated party does not exist—and therefore directly conflicts with the essential requirements for the validity of a transaction, particularly the requirement that the parties possess legal capacity.¹

D. Forgery of Digital Signatures and Documents

Advances in image-generation models and natural language processing have made it possible to forge digital signatures, company seals, and even public-key certificates. In this form, artificial intelligence does not necessarily fabricate the identity itself; rather, it fabricates the document by which the identity is proven (Mirsky & Lee, 2021). Under Iranian law, this issue intersects with the electronic-signature regime established by the Electronic Commerce Act of 2003. Article 14 recognizes a secure electronic signature as valid, while Article 15 makes its validity dependent upon four fundamental conditions: the signature must be unique to the signatory, identify the signatory, be created by the signatory or under the signatory's exclusive control, and be linked to the data message in such a manner that any subsequent alteration is detectable. AI-based forgery of a digital signature undermines each of these requirements: exclusivity disappears, the true identity is not established, and no exclusive human control exists.

3.3. Technical Mechanisms: Deeper Understanding for More Accurate Legal Analysis

One of the principal deficiencies of existing legal analyses is their disregard for technical mechanisms. A legal scholar who does not understand how a deepfake is produced will be unable to identify liability accurately in related cases. A concise but precise explanation of these mechanisms is therefore necessary. Large language models are trained on billions of parameters and can imitate virtually any writing style. To fabricate an identity, a simple prompt may suffice: “You are the chief executive officer of Company X; negotiate in that person's role.” Drawing upon publicly available information about that individual—including interviews, leaked emails, and published writings—the model performs the role. Audio and visual deepfakes are generated through diffusion models and generative adversarial networks. With five to ten seconds of a person's authentic voice, it is possible to generate a highly natural synthetic voice. Tools such as ElevenLabs and VALL-E have made this capability widely accessible. When combined with language models, these technologies create a complete digital human whose voice, image, and text are indistinguishable from those of a real person (Verdoliva, 2020). Autonomous agents constitute the most advanced manifestation of this technology. Such agents independently browse the internet, collect information, complete forms, and may even sign online contracts. These agents, technically classified within multi-agent systems, possess a substantial capacity for scalable identity fabrication.

3.4. Documented Examples and Real Cases

In February 2024, a Hong Kong court considered a case in which an employee of a financial company transferred USD 25 million after participating in a video conference in which all participants, including the chief executive officer, were deepfakes. The case, which attracted extensive attention in international legal media, demonstrated that digital identity fabrication had moved beyond theoretical speculation (Hong Kong Police, 2024).²

Although no comprehensive official statistics on AI-based digital identity fabrication have been published in Iran, the Iranian Cyber Police reported in 2023 a substantial increase in cybercrimes involving digital identity and identified numerous cases in which fabricated identities were created on messaging platforms for the conclusion of fictitious contracts. Nevertheless, most of these cases have been addressed through a criminal-law approach—computer forgery—rather than through civil liability.

¹ Although Article 247 of the Civil Code foresees a transaction involving prying eyes, its enforcement depends on the existence of a “real owner or representative.” In the scenario of a completely fictitious identity, there is no such owner, nor is there any human-willed prying eyes at all. This serious void of the indiscriminate nature of a transaction without any real parties is one of the blind spots of the Civil Code in the face of artificial intelligence.

² The Hong Kong case in February 2024 was a watershed moment, showing that digital identity fraud is no longer a purely academic concern. What is striking is that the employee at the financial firm did not suspect the colleagues he saw on the video conference because he knew them; this means that the usual psychological shields (suspicion of strangers) are ineffective against deepfakes from acquaintances. Hong Kong Police Force, Press Release, February 4, 2024.

4. Legal Effects of Contracts Concluded Through AI-Fabricated Identities

4.1. *Analysis of the Contract's Legal Status: Absolute Voidness or Non-Effectiveness?*

The Iranian Civil Code distinguishes between void transactions and transactions that are ineffective pending ratification. A void transaction is legally ineffective from the outset and cannot be cured by subsequent authorization. An ineffective transaction produces no legal effect unless and until it is ratified by the owner or other entitled person.

The relevant criteria are the essential conditions for the validity of a transaction set out in Article 190 of the Civil Code: the parties' intent and consent, their legal capacity, a definite subject matter, and a lawful purpose. The question is therefore which requirement is absent in a contract concluded by an AI-generated false identity. First, the actual identity holder has no intent because no authorization was granted. Second, the fabricated party lacks legal capacity because either that party does not exist at all, in the case of an entirely fictitious identity, or the act was performed without the authorization of the real identity holder, in the case of identity appropriation. These two defects render the contract void at its foundation. In his analysis of Articles 190 to 217 of the Civil Code, Shahidi states that whenever one of the essential elements of a transaction, such as intent or capacity, is absent, the transaction is absolutely void and cannot be cured by subsequent ratification (Shahidi, 2017). This conclusion applies fully to contracts fabricated through artificial intelligence.

One exception, however, deserves attention. If the actual identity holder, after becoming aware of the contract, confirms it, can the defect be cured? Under the rules governing unauthorized transactions, the answer is affirmative, but only where the identity holder is a real person whose identity has been appropriated. It cannot apply to entirely fictitious identities because no owner exists who could ratify the transaction.

4.2. *The Effect of Identity Fabrication on Declared and Actual Will*

One of the most complex issues in contract law is that, in AI-based identity fabrication, the declared will expressed in the contractual text corresponds to no actual will. This situation is incompatible with both classical theories: the will theory, which gives primacy to internal intention, and the declaration theory, which prioritizes the external manifestation of intention.

Iranian law, in both judicial practice and Islamic jurisprudence, is more closely aligned with the will theory. Article 191 of the Civil Code makes the formation of a contract dependent upon the intent to create legal effects, provided that such intent is accompanied by a means indicating its existence. The absence of genuine intent to create legal effects invalidates an AI-fabricated contract at its foundation.

4.3. *Protection of the Good-Faith Party: The Legal Gap and a Proposed Solution*

The principal difficulty arises because the voidness of the contract ultimately harms the good-faith party. A person who, in reliance on an AI-fabricated identity, has delivered goods, provided services, or transferred money possesses no valid contract once voidness is declared and must seek compensation through other claims, such as unjust payment or restitution for benefits conferred. French law, which has profoundly influenced Iranian civil law, developed the doctrine of appearance capable of creating rights to address this problem. Under this doctrine, a person who reasonably relies upon an appearance created by another receives legal protection even where that appearance is false (Starck et al., 2019). Iranian law contains foundations for such a doctrine. Article 683 of the Civil Code provides that where the principal has notified a third party of the agency, the dismissal of the agent without notifying that third party is ineffective against them. This provision implicitly supports the doctrine of apparent authority. The difference, however, is that Article 683 concerns a situation in which the principal personally created the appearance, whereas in machine-based identity fabrication the original identity holder played no role in creating it. The solution proposed in this study is a presumption of platform liability: whenever identity fabrication occurs through a digital platform and that platform has failed to conduct adequate identity verification, the platform should be liable to compensate the good-faith party, regardless of whether the contract is declared void.

4.4. *Civil Liability Analysis: Applicable Theories*

A. Liability of the AI Developer

Is a company that developed the model liable when the model is used to fabricate an identity? The answer depends on the circumstances. The foundation of the analysis is the general rule of civil liability under Iranian law. Article 1 of the Civil Liability Act of 1960 provides that any person who, without legal authorization, intentionally or negligently causes harm to another person's life, health, property, liberty, dignity, commercial reputation, or any other legally protected right, thereby producing material or moral loss, is liable to compensate the damage arising from that act. Applying this rule to an AI developer requires three elements: a harmful act attributable to the developer, actual damage, and a causal relationship between them. The first element is controversial. Does designing a model capable of being used for identity fabrication constitute a harmful act in itself? If the developer deliberately incorporated such a capability or failed to respond to known forms of misuse, the answer may be affirmative. Recent comparative analyses of civil liability for artificial intelligence in automated decision-making likewise treat the ordinary foreseeability of misuse as a central criterion for attributing liability to developers (Reza Farajpour et al., 2025).

B. Liability of the AI Operator

The operator is the person who deploys the system within a product or service. If the operator knowingly uses artificial intelligence to fabricate an identity, full responsibility lies with that person, and criminal sanctions may apply in addition to civil liability. The Computer Crimes Act of 2009 criminalizes the production, transmission, publication, or distribution of false or fabricated information through computer or telecommunications networks where it is undertaken with the intent to deceive or endanger public security and tranquility. It provides for imprisonment from 91 days to two years, a fine ranging from five million to forty million rials, or both penalties.

C. Liability of the Intermediary Platform

Digital platforms on which identity fabrication occurs may be liable where they have failed to conduct adequate identity verification. Article 47 of the Electronic Commerce Act recognizes the liability of intermediary service providers where they knew of an infringement and failed to act, but it does not impose an obligation of continuous identity verification. The European Union's approach under the 2022 Digital Services Act is considerably more stringent. Very large platforms must implement risk-assessment systems and take measures to prevent fraud and identity fabrication; failure to comply may result in fines of up to 6% of the company's worldwide annual turnover.

4.5. Allocation of Liability in Cases of Multiple Causes and the Three-Stage Attribution Test

In most AI identity-fabrication cases, several actors simultaneously contribute to the loss: the model developer, the operator, the platform, and sometimes the injured party through negligence in verifying identity. In such cases, Iranian law relies on the doctrine of indirect causation and the Civil Liability Act. Recent decisions of the Supreme Court, including a judgment of Branch 32 in Case No. 32/88/2023, have tended toward allocating liability in proportion to each actor's contribution.

The principal innovation of this study is the proposed three-stage test for the attribution of liability. This test may guide judges in cases involving machine-based identity fabrication by posing three successive questions. The first stage is the source test: did the error originate in the architecture and training of the model, which falls within the developer's sphere; in configuration and deployment, which falls within the operator's sphere; or in an unprotected transactional environment, which falls within the platform's sphere? The second stage is the ordinary-foreseeability test: was the relevant misuse foreseeable to a reasonable actor in the position of each of these three parties, and were proportionate preventive measures adopted? The third stage is the effective-control test: which actor possessed the closest and most effective control over the process at the moment the harm occurred? The answers to these questions are consistent both with the rule of *ghurur*, under which a deceived party may recover from the deceiver, and with the doctrines of direct and indirect causation. The result should be joint and several liability toward the injured party, followed by an internal allocation among responsible actors in proportion to their respective degrees of fault. A complementary legislative proposal is to codify this principle expressly in a future Iranian artificial intelligence statute.

5. Comparative Analysis: Approaches of Leading Legal Systems

A study of major legal systems reveals that, despite differences in regulatory instruments, a clear convergence has emerged: no established legal system grants personality to machines, and all seek responsibility within the human and corporate chain behind the system (R. Farajpour et al., 2025).

5.1. *European Union: Leadership in Artificial Intelligence Regulation*

5.1.1. *The 2024 Artificial Intelligence Act: The World's First Comprehensive AI Legislation*

Regulation (EU) 2024/1689, which entered into force in July 2024 and is expected to become fully applicable by 2026, constitutes the world's first comprehensive artificial intelligence legislation. The legislative history of this instrument demonstrates that ethical considerations—from transparency and the prohibition of deception to the protection of human dignity—formed its central foundation (Farajpour et al., 2024). Its most prominent feature is a risk-based approach: systems are not regulated uniformly but are classified into four categories according to the risks they impose on society.

The first category is unacceptable risk, which is prohibited entirely. Article 5 excludes from the European Union market systems that use subliminal techniques or exploit the vulnerabilities of persons or groups in a manner that materially distorts behavior and causes significant harm. Digital identity fabrication for the purpose of concluding contracts may readily fall within this category. The second category, high risk, includes systems used in sensitive fields such as critical infrastructure, legal and financial services, and identity verification. Such systems must be registered, undergo risk assessment, and remain under continuous supervision. The Act's most important mechanism for addressing identity fabrication is the transparency obligation under Article 50: systems that interact with human beings must clearly disclose their non-human identity. Violations may result in fines of up to EUR 15 million or 3% of worldwide annual turnover, whichever is higher.

5.1.2. *The Artificial Intelligence Liability Directive: A Transformation in the Law of Evidence*

Alongside the principal Act, the proposed Artificial Intelligence Liability Directive, whose legislative process has undergone considerable fluctuation, introduced an important development in European civil liability law: a presumption of causation in artificial intelligence claims. Under this approach, if the injured party demonstrates that the system was probably defective and that the defect probably caused the damage, a presumption arises and the developer must prove the contrary. This reversal of the burden of proof is of fundamental importance because direct proof of defects is often impossible for injured parties in AI litigation, particularly because source code is generally confidential.

5.2. *United States: A Sectoral and State-Based Approach*

The United States has not yet enacted comprehensive federal artificial intelligence legislation. In contrast to the European Union, its approach is innovation-oriented and generally grounded in limited intervention in the free market. Nevertheless, several existing laws and regulations are relevant. At the federal level, the October 2023 Executive Order on Safe and Trustworthy Artificial Intelligence imposed certain transparency and security requirements and required developers of powerful models to share safety-testing results with the government. It is, however, an executive order rather than legislation, and its binding force is limited. In the field of digital identity fabrication, the Identity Theft Enforcement and Restitution Act of 2008 recognized aggravated identity theft as an independent offense carrying an additional two-year term of imprisonment. California, the leading state in technology regulation, has enacted several relevant laws: AB 730 of 2019 prohibited the misuse of deepfakes in elections; AB 602 of 2022 granted individuals a right to bring civil actions against unauthorized use of their image or voice in deepfakes; and SB 1047 pursued safety-assessment requirements for powerful models. In contract law, Section 153 of the Restatement (Second) of Contracts, which recognizes mistake as to identity, may be applicable. A contract concluded because one party was mistaken about the identity of the other is voidable where the other party knew of the mistake or where the mistake arose from fraud—both of which are present in machine-based identity fabrication.

5.3. *United Kingdom: A Common-Law Interpretive Approach*

Following its withdrawal from the European Union, the United Kingdom has pursued an independent path. Its 2023 White Paper on artificial intelligence regulation states that the country will adopt an innovation-oriented approach, will not enact a single comprehensive statute, and will instead rely on sectoral regulators, including the Financial Conduct Authority for financial matters, the Information Commissioner's Office for data protection, and the Competition and Markets Authority for competition.

English common law nevertheless provides useful doctrines for addressing identity fabrication. The doctrine of non est factum allows a person who signed a document because of signature forgery or deception to deny being bound by it, although it imposes a strict condition: the signatory must not have acted negligently. The Misrepresentation Act 1967 is also significant. A person who has entered into a contract on the basis of a false representation, including fabricated identity, may seek rescission and damages, provided that the falsity of the representation and reliance upon it are established. Both requirements are evident in machine-based identity fabrication. In its 2023 report on smart contracts and digital assets, the Law Commission of England and Wales also proposed that mistake as to identity, developed in classical cases such as *Cundy v. Lindsay* (1878), should be reconsidered for the era of digital fabrication.

5.4. *China: Rapid and Centralized Regulation*

China has acted with exceptional speed in regulating artificial intelligence. The Interim Measures for the Management of Generative Artificial Intelligence Services, effective from August 2023, constituted the world's first specific regulation of generative artificial intelligence. Article 4 enumerates prohibited forms of content, while Article 14 requires providers to ensure that generated content does not lead to identity fabrication, fraud, or disruption of social order. Violations may result in service suspension and substantial penalties. In contract law, Article 148 of the 2021 Chinese Civil Code recognizes fraud as a ground for avoiding a contract. A party who enters into a transaction as a result of the other party's fraud may request judicial annulment, a rule directly applicable to digital identity fabrication.

5.5. *Estonia: A Successful Model of Digital Identity*

With a population of approximately 1.3 million, Estonia possesses one of the world's most advanced digital-identity systems. The national X-Road infrastructure, operational since 2001, has digitized 99% of government services and has raised transactional security to an exceptional level. The mandatory national smart card contains two separate cryptographic keys: one for identity authentication and another for electronic signatures, making identity fabrication technically extremely difficult (Naeimi & Habibi, 2023).

More significantly, the Estonian Identity Documents Act of 1999, as amended in 2023, expressly recognizes the use of artificial intelligence to forge digital signatures both as a criminal offense and as a basis for full civil liability. This model offers valuable guidance for Iran.

6. **The Status of Iranian Law: Capacities, Limitations, and Fundamental Gaps**

6.1. *Existing Capacities within the Iranian Legal System*

Contrary to initial impressions, the Iranian legal system possesses capacities that, through creative interpretation, may be used to address machine-based identity fabrication.

The first is the no-harm principle, a rule of Islamic jurisprudence whose underlying rationale is reflected in the general rule of civil liability and which provides a strong foundation for imposing liability wherever harm has been caused, even in the absence of an express statutory provision. The second is the rule of ghurur, under which the deceived party may recover from the deceiver. This rule provides an Islamic jurisprudential and legal basis for holding an identity fabricator liable toward a good-faith party, and Katouzian regards it as an important liability-generating doctrine (Katouzian, 2019).¹ The third capacity

¹ The rule (the arrogant person returns to the one he has deceived) has been discussed in various jurisprudential texts, including Jawaher al-Kalam (Vol. 37, p. 41) and Makasib al-Shaykh Ansari. Professor Katouzian (General Rules of Contracts, Vol. 1, p. 315) considers this rule to be the jurisprudential basis of the

is an expansive interpretation of negligence under the general rule of civil liability, which may extend to developers who fail to implement necessary preventive safeguards. The fourth consists of Articles 51 to 56 of the Electronic Commerce Act, which provide certain preliminary consumer protections in electronic transactions.

6.2. *Serious Limitations of the Existing Legal System*

These capacities do not justify complete optimism because fundamental deficiencies impede an effective response.

The first limitation concerns the definition of a secure electronic signature. Although the Electronic Commerce Act defines such a signature, the mechanism for establishing its reliability—particularly in the face of machine-based forgery—remains unclear, and the 2007 Implementing Regulation did not remedy this deficiency. The second limitation is the absence of a legal definition of artificial intelligence in any statute or regulation, a definitional gap that makes the application of existing laws to intelligent systems extremely difficult. The third relates to evidentiary law. Digital-identity disputes require technical expertise, but Articles 257 to 265 of the 2000 Code of Civil Procedure were not designed for digital litigation. The fourth is the absence of a specialized regulator. The Supreme Council of Cyberspace performs certain functions, but it does not possess the technical and specialized competence required in this field.

6.3. *Analysis of the 2009 Computer Crimes Act from the Perspective of AI Identity Fabrication*

The Computer Crimes Act contains seven chapters, and its third chapter, comprising Articles 67 to 71, addresses computer forgery and falsification. Under Article 67, any person who, with the intent to deceive or harm another, creates, alters, deletes, or conceals data in a manner that makes it appear authentic commits a computer-related offense.

At first sight, this rule applies to machine-based identity fabrication. The central difficulty, however, is proving the “intent to deceive” where artificial intelligence has acted autonomously, because the machine itself possesses no intent and the requisite intention must therefore be located in a human user. From a civil-law perspective, the criminalization of the production and dissemination of false or fabricated information under the third chapter provides criminal sanctions, but it does not expressly regulate compensation for the injured party. The victim must therefore initiate a separate civil action, a duality that complicates the process of obtaining redress.

6.4. *Review of Iranian Judicial Practice*

Despite numerous reported incidents, no coherent body of Iranian judicial precedent has developed in this field, for several reasons. First, many victims refrain from bringing claims because of the absence of appropriate evidentiary mechanisms. Second, judges have not received sufficient training in advanced digital crimes. Third, where proceedings are initiated, the criminal route—usually through a complaint to the Iranian Cyber Police—is generally preferred over a civil claim. Nevertheless, certain decisions of the Supreme Court and appellate courts concerning the broader field of electronic-document forgery may provide the foundation for future AI-related jurisprudence. One example is a 2022 judgment of Branch 36 of the Supreme Court in a criminal case involving the forgery of a company seal in digital documents, which expressly held that digital forgery requires independent judicial expert examination and thus contributed to the development of an adjudicatory infrastructure.

7. **Comprehensive Solutions: Legislative, Technical, and Institutional**

7.1. *Legislative Package*

7.1.1. *First Solution: Enactment of a Comprehensive Iranian Artificial Intelligence Act*

The most important solution is the enactment of comprehensive national legislation addressing five principal areas. The first is definition and classification: the statute should precisely define an artificial intelligence system, a generative system, and an

theory of improper recourse. Its application in our discussion is that whoever makes or makes available the means of deception is liable to the deceived, even if he himself did not directly deceive.

autonomous agent, and classify systems according to risk, following the European model but adapting it to Iranian conditions through four categories: minimal, moderate, high, and unacceptable risk. The second is transparency: every system interacting with users must disclose its non-human identity, and this obligation must be supported by adequate sanctions, including monetary penalties and suspension of operations. The third is a liability regime: joint and several liability should be imposed on developers, operators, and platforms toward injured parties, accompanied by a presumption of liability that places the evidentiary burden on the stronger party, in accordance with the three-stage test proposed in this study. The fourth is the establishment of a compensation fund financed through levies imposed on artificial intelligence operators to cover losses that cannot be attributed to a specific responsible actor. The fifth is the creation of an independent national regulator with sufficient authority and resources for supervision and enforcement.

7.1.2. Second Solution: Amendment of the Electronic Commerce Act

The Electronic Commerce Act of 2003 requires substantial modernization, including the addition of a chapter entitled “Digital Identity Verification and Artificial Intelligence,” containing two proposed rules. First, digital platforms on which contracts exceeding a statutory threshold—for example, fifty million rials—are concluded should be required to implement multi-factor authentication, and failure to comply should render the platform liable toward the injured party. Second, the use of artificial intelligence in the contract-formation process should require prior disclosure to the counterparty unless expressly authorized by law.

7.1.3. Third Solution: Amendment of the Civil Liability Act

A chapter entitled “Liability Arising from Artificial Intelligence” should be added to the Civil Liability Act of 1960. It should provide that developers, operators, and platforms using intelligent systems are jointly and severally liable for losses caused through those systems unless they prove that all reasonable preventive measures were implemented. The final allocation of liability among them should be determined by the court.

7.1.4. Fourth Solution: A National Digital-Identity System

Drawing upon Estonia’s successful experience, Iran should establish a national system integrating civil-registration databases, police records, and the Companies Registration Organization within a unified and secure architecture, so that the identity involved in every digital transaction can be verified. The system should employ public-key cryptography and multi-factor authentication. Every citizen should possess a digital-identity wallet, without which their contractual identity would not be legally valid. The costs of establishing the system could be financed through levies imposed on operators in the digital economy.

7.1.5. Fifth Solution: Mandatory Watermarking in Generative Artificial Intelligence

Model developers should be required to embed digital watermarks in all generated content. Such watermarks should be non-removable by users, detectable by standardized government tools, and capable of encoding provenance information, including the time of production and the generating system. The C2PA technology developed by Adobe, Microsoft, and other companies provides a suitable model.

7.1.6. Sixth Solution: Specialized Judicial Expertise in Artificial Intelligence

The Judiciary should establish a National Center for Judicial Expertise in Artificial Intelligence to provide accurate technical analysis in digital-identity fabrication cases. The center should cooperate with leading universities in the country. In parallel, the qualification requirements for artificial intelligence experts should be expressly defined in both civil and criminal procedural legislation.

7.1.7. *Seventh Solution: Specialized Technology Courts*

The experience of specialized courts in various countries demonstrates that expert adjudication of technology disputes is both faster and more accurate. Iran should establish specialized technology-law branches in the courts of Tehran, Isfahan, and Mashhad. Judges assigned to these branches should complete mandatory training in technology law, digital forensics, and the fundamentals of artificial intelligence. A special procedural framework should also define the duration of expert examination and the evidentiary value of digital evidence.

7.1.8. *Eighth Solution: A Digital-Loss Compensation Fund*

Following the model of existing compensation mechanisms, such as the Bodily Injury Compensation Fund under Article 10 of the 2016 Compulsory Insurance Act, a fund should be established to compensate losses arising from artificial intelligence where, despite reasonable efforts by the injured party, no specific responsible actor can be identified or effectively pursued.

7.1.9. *Ninth Solution: Education and Awareness-Building*

At the societal level, public digital-literacy programs focusing on the detection of identity fabrication should be designed and implemented. At the professional level, artificial intelligence law should be incorporated into the curricula of law schools. The Judiciary should also provide continuous education for judges in this field.

7.1.10. *Tenth Solution: International Cooperation*

Digital identity fabrication is transnational in nature. Iran should cooperate with regional countries, including members of the Economic Cooperation Organization and the Developing-8, in exchanging information and experience. It should contribute to the development of international technical standards for digital-identity verification, such as ISO/IEC 24760, and establish judicial-cooperation protocols with jurisdictions in which perpetrators are likely to be located.

8. **Theoretical Evaluation: Searching for an Appropriate Legal Paradigm for Artificial Intelligence**

8.1. *Three Competing Paradigms*

The international legal literature presents three principal paradigms concerning the legal status of artificial intelligence, and selecting an appropriate approach is impossible without understanding them.

The first paradigm regards artificial intelligence as a tool: an advanced instrument, but merely an instrument, in human hands, with full responsibility imposed upon the human beings who design, supply, or use it. This paradigm is the most compatible with existing legal systems. The second paradigm treats artificial intelligence as an agent: certain advanced systems possess a degree of agency sufficient for them to be regarded as legal actors rather than mere tools, a position defended by Allen and by Chopra and White (Allen, 2019; Chopra & White, 2011). The third and most radical paradigm grants personality to machines: it proposes conferring a limited form of legal personality upon advanced artificial intelligence, analogous to juridical personality. This proposal was advanced by the European Parliament in 2017 and was subsequently abandoned.

8.2. *Critique of the Legal-Personality Paradigm for Artificial Intelligence*

This study strongly maintains that granting legal personality to artificial intelligence, even in a limited form, would constitute a strategic error that would aggravate rather than resolve existing problems. Recent comparative studies of Iranian and European Union law support this conclusion (Farajpour, 2025b).

The first reason is the risk of evasion of liability. If the machine is treated as a person, developers and operators may argue that the artificial intelligence made an independent decision and that they therefore bear no responsibility, a phenomenon

described by Bryson and colleagues as a liability shield (Bryson et al., 2017).¹ The second reason is incompatibility with the philosophy of Islamic law. In Islamic jurisprudence, which forms a foundation of Iranian law, personality is linked to being a legally accountable subject: an entity capable of understanding, choosing, and answering for its conduct. A machine possesses none of these characteristics. The third reason is the risk of abuse. Legal personality could allow machines to own assets and thereby enable wealth to be placed beyond the reach of creditors, a possibility that would be economically hazardous.

8.3. *The Proposed Paradigm: An Advanced Instrument with a Chain of Liability*

This study proposes the paradigm of an “advanced instrument with a chain of liability.” Under this approach, artificial intelligence is treated as an instrument that, like motor vehicles or pharmaceuticals, is subject to a specialized liability regime. The chain of liability extends from the developer, through the distributor and operator, to the end user, with each link bearing responsibility in proportion to its contribution. The three-stage attribution test discussed in Section 4 provides the procedural mechanism for implementing this paradigm in litigation. This framework is compatible with Iranian law and does not require a fundamental paradigmatic transformation; it requires only explicit legislative recognition.²

9. Conclusion

AI-based fabrication of legal identity is no longer a hypothetical or remote scenario, nor is it a phenomenon that legal systems can afford to address belatedly. With the expansion of generative models and autonomous agents, this threat has moved beyond theory and entered practical reality. New incidents are being documented continuously, and legal systems that respond earlier will suffer less harm.

The present study examined this phenomenon from multiple perspectives and reached several conclusions. First, artificial intelligence lacks legally cognizable will, and any contract concluded through an identity fabricated by such a system is absolutely void because it lacks intent and capacity, two fundamental conditions for the validity of transactions under the Civil Code. Second, the Iranian legal system is vulnerable on four principal fronts: the absence of a legal conception of algorithmic agency, the lack of a specialized artificial intelligence liability regime, the inadequate protection of good-faith parties against digital identity fabrication, and the absence of any legal obligation to disclose machine identity during interactions. Third, international experience—particularly the European Union Artificial Intelligence Act, Chinese regulations, and Estonia’s digital-identity system—demonstrates that effective countermeasures are possible and that tested solutions already exist. Fourth, this article proposed ten measures across legislative, technical, and institutional domains, the most important of which are the enactment of comprehensive artificial intelligence legislation centered on chain-based liability, the establishment of a national digital-identity system, and the creation of specialized technology-law judicial branches. Fifth, the proposed paradigm of an advanced instrument with a chain of liability, together with the three-stage attribution test, is both compatible with the Islamic jurisprudential and legal foundations of Iran and practically implementable. It also provides a basis for addressing future challenges extending beyond identity fabrication. Ultimately, law has always followed technological development; this time, however, given the speed of change in artificial intelligence, legal systems cannot wait for emerging challenges to generate their own legislative solutions. The need for preventive legislation is more urgent than ever.³

Ethical Considerations

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

¹ Granting legal personality to AI has a history: the European Parliament proposed electronic personality for autonomous robots in its 2017 resolution (2015/2103(INL)), but it was shelved following the objections of over 150 AI experts and lawyers in an open letter to the European Commission (2018). The main reason for the opposition was the risk of a liability shield for manufacturers; see: Bryson, Diamantis & Grant (2017).

² The advanced tool paradigm with a chain of responsibility is inspired by the product liability system in European Union law (Directive 85/374/EEC and amended in 2024); a system in which each link from production to distribution and exploitation has its share of responsibility. Adaptation of this framework to the rules of no harm, waste and attribution in Islamic jurisprudence is quite possible and there is no need to accept concepts alien to Iranian law.

³ The comparison of the speed of legislation is instructive: the European Union took just three years from 2021 to finalize the AI law in July 2024, and China implemented its generative AI regulations in less than two years from proposal; Iran is still at the study design stage. Every day of this delay is more costly, as bad actors exploit legal loopholes.

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

- Allen, T. (2019). The Law of Agency and Artificial Intelligence: Rethinking Liability Attribution. *Oxford Journal of Legal Studies*, 39(4), 771-803. <https://doi.org/10.1093/ojls/gqz025>
- Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the People: The Legal Lacuna of Synthetic Persons. *Artificial Intelligence and Law*, 25(3), 273-291. <https://doi.org/10.1007/s10506-017-9214-9>
- Chopra, S., & White, L. F. (2011). *A Legal Theory for Autonomous Artificial Agents*. University of Michigan Press.
- Danaher, J. (2020). Welcoming Robots into the Moral Circle: A Defence of Ethical Behaviourism. *Science and Engineering Ethics*, 26(4), 2023-2049. <https://doi.org/10.1007/s11948-019-00119-x>
- European Banking Authority. (2023). *Report on the Use of Artificial Intelligence in Financial Services: Cybersecurity Risks and Fraud*.
- Farajpour, R. (2025a). Legal and Comparative Analysis of Civil Liability of Artificial Intelligence in Automated Decision-Making. *AI and Tech in Behavioral and Social Sciences*, 3(3), 1-9. <https://doi.org/10.61838/kman.aitech.3.3.4>
- Farajpour, R. (2025b). The Role of Civil Liability in Artificial Intelligence Laws from the Perspective of Major Global Legal Systems. *Journal of Law and Political Studies*, 5(1), 182-196. <https://doi.org/10.48309/jlps.2025.518711.1353>
- Farajpour, R., Amerinia, M., & Gorjinia, M. (2024). Ethical Requirements in the Process of Adopting the European Union Artificial Intelligence Act. *Cyber Law Studies*, 3(4), 37-53. <https://doi.org/10.71488/cyberlaw.2025.1127854>
- Farajpour, R., Amerinia, M. B., & Pourjavaheri, A. (2025). The Role of Artificial Intelligence in Arbitration and Legal Challenges Arising from Automated Decisions in Sports. *AI and Tech in Behavioral and Social Sciences*, 3(2), 21-28. <https://doi.org/10.61838/kman.aitech.3.2.3>
- Farajpour, R., Mahmoudi-Moghaddam, S. M., Babaei, D., Rostami, H., & Kiani, M. (2025). Legal Effects and Consequences of Granting Legal Personality to Artificial Intelligence Systems in Iranian and European Union Law. *New Research in Islamic Humanities Studies*, 4(Special issue), 1-28. <https://doi.org/10.22034/api.2026.2087166.1696>
- Katouzian, N. (2019). *General Rules of Contracts* (10th ed., Vol. 1). Enteshar Co.
- Mirsky, Y., & Lee, W. (2021). The Creation and Detection of Deepfakes: A Survey. *Acm Computing Surveys*, 54(1), 1-41. <https://doi.org/10.1145/3425780>
- Muller, V. C. (2022). Legal Personhood for Artificial Agents: Why It Is Not Needed and What Is Needed Instead. *Philosophy and Technology*, 35(2), 45. <https://doi.org/10.1007/s13347-022-00547-7>
- Naeimi, M., & Habibi, M. (2023). Legal Analysis of Digital Signature Forgery in Light of the Electronic Commerce Act. *Journal of Islamic Law*, 20(79), 187-221.
- Shahidi, M. (2017). *Effects of Contracts and Obligations* (6th ed.). Majd Scientific and Cultural Assembly.
- Starck, B., Roland, H., & Boyer, L. (2019). *Civil Law: Obligations: Tort Liability* (8th ed.). LexisNexis.
- Verdoliva, L. (2020). Media Forensics and Deepfakes: An Overview. *IEEE Journal of Selected Topics in Signal Processing*, 14(5), 910-932. <https://doi.org/10.1109/JSTSP.2020.3002101>