

Legal Liability of Artificial Intelligence Systems

المسؤولية القانونية للذكاء الاصطناعي

Dr. Radhia Sengouga ⁽¹⁾

Center university of Barika (Algeria)

radhia.sangouga@cu-barika.dz

Received
Apr – 03 - 2026

Accepted
Sep – 06 - 2026

Published
Oct – 31 - 2026

Abstract:

This research investigates the legal dimensions of liability arising from artificial intelligence (AI) technologies, analyzing the adequacy of traditional tort law principles in addressing the increasing autonomy of these systems within global legislative frameworks. The study focuses on evidentiary challenges linked to "algorithmic opacity" and the complexities of establishing causation. Furthermore, it proposes regulatory frameworks centered on mandatory insurance and centralized registration as mechanisms for risk management. The paper also explores the potential for granting limited legal personhood to intelligent entities, emphasizing the necessity of developing a flexible judicial system that balances the protection of civil rights with the promotion of technological innovation to keep pace with rapid digital transformations.

key words: Legal Liability, Legal Personhood, Artificial Intelligence, Tortious Damage, Causal Link, Compensation.

المخلص:

يستقصي هذا البحث المظاهر القانونية للمسؤولية الناشئة عن تقنيات الذكاء الاصطناعي، محلاً مدى قدرته النظرية التقليدية للضرر على استيعاب الاستقلالية المتنامية لهذه الأنظمة في ظل المقاربات الدولية وتركز الدراسة على التحديات الإثباتية المرتبطة بـ "الغموض الخوارزمي" وصعوبة إثبات الرابطة السببية، مع اقتراح أطر رقابية تعتمد على التأمين الإلزامي والتسجيل المركزي كآليات لإدارة مخاطر هذه الأنظمة الذكية مع إمكانية إسباغ الشخصية القانونية المحدودة على هذه الكيانات الذكية، والتركيز على ضرورة صياغة نظام قضائي مرن يوازن بين حماية الحقوق وتحفيز الابتكار التقني لمواكبة المتغيرات التكنولوجية المتسارعة.

الكلمات المفتاحية: المسؤولية القانونية، الشخصية القانونية، الذكاء الاصطناعي، الضرر، الرابطة

السببية، التعويض.

⁽¹⁾ Corresponding author: Dr. Radhia Sengouga,

e-mail: radhia.sangouga@cu-barika.dz

Introduction:

The contemporary world is witnessing an unprecedented technological surge driven by Artificial Intelligence (AI), which has transcended its role as a mere auxiliary tool to become a pivotal actor reshaping global economic and social structures. As the autonomous capabilities of these systems expand and permeate vital services, complex legal dilemmas have surfaced. While these technologies offer vast horizons for human welfare, they simultaneously engender significant risks manifested in damages resulting from their autonomous outputs whether in smart transportation medical diagnostics, or algorithmic bias. Consequently, the general rules of legal liability are facing an unprecedented historical test.

The importance of the Study:

The importance of this research stems from the urgent need to address the "legislative gap" created by the rapid evolution of AI in contrast to the relative inertia of traditional legal frameworks. Classic principles of tort liability, rooted in the concepts of fault and negligence, have become inadequate to encompass the "unforeseeable" nature of automated behavior. Accordingly, this study seeks to establish a legal framework that ensures a balance between fostering technological innovation and safeguarding civil rights, ensuring that the rights of injured parties are not lost within the intricacies of complex algorithms.

Research Objectives : This research aims to achieve the following specific objectives:

Conceptual Grounding: Categorizing AI systems from a legal perspective to determine how their degree of autonomy influences the nature of liability.

Procedural Redress: Deconstructing evidentiary barriers, particularly regarding the "causal link" in light of systemic complexity and proposing effective legal alternatives.

Legislative Forecasting: Formulating a comprehensive legal vision that adopts standards of transparency and disclosure while ensuring fair and efficient compensation mechanisms.

Research Problem: The core problem of this research revolves around the "Crisis of the Legal Actor". Given the interplay between the human intent of the designer or operator and the autonomous behavior of the system a fundamental question arises regarding the proper legal basis for accountability: Should we rely on "Objective Liability" (Strict Liability) based on risk as a solution for redress? Or does technological evolution necessitate the recognition of a "Legal Personality" for systems? Furthermore, how can an injured party establish a causal link when faced with systems characterized by technical opacity and a lack of human explain ability (The Black Box phenomenon) ?

Methodology: To encompass the various dimensions of this subject, the study employs a Comparative Analytical Method. This involves surveying modern trends in international legislation most notably the European Union Artificial Intelligence Act (EU

AI Act) and American legislative policies and benchmarking them against general jurisprudential principles and judicial precedents.

For a systematic treatment of the problem, the research is divided into two primary sections:

Section I: Examines the theoretical frameworks and substantive foundations of liability (the nature of AI systems, comparative liability theories and international trends).

Section II: Investigates applied aspects and remedial mechanisms (proving causation, insurance and registration systems, and proposals for legislative development, particularly at the national level).

Section I: Theoretical Foundations of Legal Liability for Artificial Intelligence Acts

Exploring the theoretical underpinnings of legal liability for AI-driven actions constitutes an essential analytical gateway to comprehending the intricate dilemmas emerging within this nascent field. Legal harms are no longer exclusively tethered to direct human agency; instead they have become increasingly intertwined with algorithmic decision-making processes characterized by varying degrees of autonomy. The significance of this section lies in its capacity to delineate the conceptual framework upon which the accountability of diverse stakeholders involved in the development operation or commercialization of these systems is predicated. Furthermore this inquiry facilitates an assessment of whether traditional civil and criminal liability doctrines remain robust enough to encompass the unique attributes of Artificial Intelligence, or if they necessitate structural adaptations to align with contemporary technological advancements.

A) Taxonomy of Artificial Intelligence Systems and its Impact on Liability Determination:

The classification of Artificial Intelligence (AI) systems constitutes a foundational step toward understanding the nature of each system and its degree of decisional autonomy a factor that directly influences the legal basis for liability when damages occur. AI systems do not possess a uniform level of complexity or capacity for learning and adaptation, consequently accountability varies depending on their specific functions and the extent of human intervention involved. Therefore, analyzing this taxonomy is not merely a technical exercise but carries profound legal significance. Such categorization facilitates the distinction between instances where liability is attributable to the designer, manufacturer or user, and those posing greater challenges due to the interactive or predictive nature of the system. Furthermore, this distinction enables researchers to assess the adequacy of traditional liability doctrines and the necessity of evolving these frameworks to align with the unique characteristics of autonomous intelligent systems.

1) Narrow Artificial Intelligence (Narrow AI):

Narrow Artificial Intelligence refers to systems engineered to perform specific functions within a strictly predefined and circumscribed scope, such as recommendation

algorithms or rule-based diagnostic tools. Their legal significance lies in the fact that their behavioral outputs remain inherently traceable to the designer or the operator. This traceability aligns the basis of liability with established doctrines governing design or operational defects. Consequently, any resulting damages are predominantly attributed to human agency rather than the purported "autonomy" of the machine.¹

2) Machine Learning Systems (ML):

Machine Learning systems are distinguished by their capacity to transcend mere automated execution, iteratively enhancing their performance based on data processing and empirical experience. This inherent characteristic poses a unique legal challenge: as the system's behavior becomes increasingly less predictable over time, the feasibility of attributing fault to a single, direct human act is significantly diminished. Consequently, there is an emerging necessity for a liability framework predicated on data quality training governance and continuous oversight.²

It can be inferred that Machine Learning (ML) systems diverge fundamentally from traditional automated frameworks due to their iterative evolution driven by data processing and empirical experience, a characteristic that renders their operational outputs inherently less foreseeable. This inherent unpredictability complicates the identification of specific failure points, as legal harm may not originate from a single discrete decision. Rather, it often stems from a complex causal chain involving data integrity, training methodologies, and validation protocols. Consequently, the paradigm of liability in this context shifts from a focus on the initial moment of deployment toward a continuous framework centered on "Duties of Care," rigorous governance, and persistent monitoring throughout the system's lifecycle.

3) Artificial General Intelligence (AGI):

Artificial General Intelligence (AGI) represents a conceptual framework for systems possessing a broad capacity for understanding, learning, and decision-making across diverse domains, closely approximating human cognitive abilities. Although this model remains largely theoretical at present, its legal significance lies in its potential to compel legal scholarship to re-examine the fundamental principles of Attribution and Liability in the face of highly autonomous entities. This conceptualization serves as a benchmark for testing the robustness of traditional liability doctrines against systems that transcend the conventional bounds of human foreseeability.³

In essence, AGI constitutes a more sophisticated paradigm than Narrow AI, as it presupposes a system's ability to perform multifaceted and adaptive cognitive functions. While this model currently resides within the sphere of theoretical discourse rather than established practical reality, its legal import is underscored by its challenge to the adequacy of existing liability frameworks as machine autonomy intensifies. This trajectory has prompted legal scholars to scrutinize the diminishing boundary between a mere technological tool and a Quasi-Autonomous Actor.

4) The European Risk-Based Classification of Artificial Intelligence:

The European Union has adopted a "Risk-Based Approach," wherein Artificial Intelligence is categorized into distinct classes based on the magnitude of its impact on fundamental rights, liberties and safety. This taxonomy dictates the varying legal obligations imposed on market actors, particularly concerning transparency, documentation and human oversight. Consequently, this reflects directly on the liability framework as the risk criterion serves as the foundational benchmark for the allocation of legal duties and sanctions.⁴

The risk-analysis methodology constitutes the structural pillar of the EU AI Act, where legal obligations and regulatory constraints are formulated in direct proportion to the potential severity of harm and the implications of system deployment. Under this framework, the EU has implemented a hierarchical four-tier classification. This spectrum begins with "Prohibited AI Systems" that infringe upon core values and human rights, and scales down to "Minimal Risk Systems" that are subject to fewer regulatory burdens. Such a hierarchy reflects the legislator's intent to strike a sophisticated balance between rigorous legal protection and the flexibility required for digital innovation.⁵

Furthermore, the classification of AI systems is a prerequisite for understanding the nature of each system and its degree of decisional autonomy factors that directly influence the determination of the legal basis for liability when damages arise. Since AI systems possess varying levels of complexity, learning capacity, and adaptability, their accountability fluctuates according to their specific function and the extent of human intervention.

Ultimately, the study of this taxonomy transcends mere technicality, carrying profound legal weight. It facilitates the distinction between instances where liability is attributable to the designer, manufacturer or user, and those posing greater challenges due to the system's interactive or predictive characteristics. Such a distinction enables researchers to evaluate the adequacy of traditional liability doctrines and the potential necessity for evolving these rules to align with the unique specificities of intelligent systems.

B) Traditional Liability Theories and Their Application to Artificial Intelligence:

This section is of particular importance as it highlights the capacity of traditional liability theories to encompass damages potentially caused by Artificial Intelligence (AI), notwithstanding that such damages may arise within a complex and indirect technical context. Accordingly, examining tortious, contractual, criminal and strict liability frameworks allows for determining the adequacy of existing legal rules or the necessity of adapting them to the unique nature of intelligent systems.

1) Tortious Liability:

Tortious liability is fundamentally predicated on the establishment of fault, damage and a causal link. In the context of Artificial Intelligence (AI), "fault" manifests in design flaws, inadequate training datasets, or a failure in post-deployment monitoring. Consequently, liability is not attributed to the system itself but rather to the natural or

legal person who breached the requisite duty of care. This conceptualization gains significant importance when damages result from negligence in algorithmic testing or allowing systems to operate without sufficient safeguards.⁶

Accordingly, tortious liability remains the most prominent framework for addressing AI-related harms, as its core elements—fault, damage and causation—are adaptable to instances of negligence in design, training or supervision. Numerous studies have demonstrated that most AI-related disputes can be traced back to a developer's or provider's failure to exercise "reasonable care," rather than to the machine as an autonomous entity. Therefore, while this form of liability remains valid and applicable, it necessitates more flexible evidentiary tools to accommodate technical complexities.

2) Contractual Liability:

Contractual fault constitutes the fundamental pillar of contractual liability, legally materialized upon the debtor's failure to fulfill obligations arising from the consensual relationship. This breach encompasses not only total non-performance but also partial or defective execution that fails to meet the standards of quality or safety stipulated in the agreement. Such fault is characterized as a deviation from the mandated conduct prescribed by the contract, resulting in prejudice to the creditor's interests and necessitating indemnification, provided the default stems from the debtor's will or negligence and absent proof of an external cause (*Force Majeure*) preventing fulfillment.⁷

In AI supply contracts, providers may be bound by express or implied warranties regarding performance, non-maleficence or fitness for a particular purpose. If a systemic defect results in damage, recourse may be sought against the party in breach regardless of the system's technical complexity.⁸

Autonomous vehicles serve as a prominent case study for the distribution of civil liability within leasing contracts, where the legal scope of obligation hinges on the vehicle's degree of technical autonomy. In this context, two primary scenarios must be distinguished:⁹

First: *Partial Autonomy and the Principle of Continuous Human Intervention*. In systems with limited automation (such as collision avoidance systems), effective control remains shared between "technical intelligence" and the "human element." Here, the lessee bears a legal obligation of vigilance and immediate intervention when the system detects exceptional circumstances (e.g., adverse weather), rendering their liability contingent upon a failure in the duty of supervision and intervention.

Second: *Contractual Liability Arising from Breach of Maintenance Obligations*. The lessee's obligations extend to technical preventive measures. If the contract stipulates specific periodic maintenance terms (e.g., technical inspections after certain distances), any negligence in executing these clauses constitutes a contractual fault and a breach justifying liability. Should an accident occur due to a technical malfunction that was preventable through maintenance, legal liability shifts entirely to the lessee as the "custodian" (*Garde*) in breach of contractual terms, thereby severing the causal link toward the lessor or producer.

In fully autonomous systems, liability shifts from the user's personal sphere to the intelligent system's technical domain, given the absence of effective human control. This transition necessitates the adoption of digital evidentiary mechanisms, such as "Black Box" recorders to decipher algorithmic decision-making and precisely identify the point of failure. Consequently, assigning liability for damages becomes dependent on the technical analysis of recorded data, facilitating the attribution of legal responsibility to the entity in charge of developing or operating the system.¹⁰

In conclusion, contractual liability becomes paramount when AI is the subject of a commercial or professional agreement, such as licensing or development contracts. In these instances, a breach of agreed warranties or failure to perform maintenance and updates serves as the basis for contractual claims. Specialized literature underscores that the relationship between developers and users in the AI ecosystem is predominantly governed by contract; thus, contractual liability assumes a critical role in the strategic distribution of technological risks.

3) Criminal Liability:

Criminal liability presents a more complex challenge, as criminal law typically presupposes the existence of specific intent (*Mens Rea*) or personal fault. Under the traditional legal paradigm the artificial intelligence system itself cannot be held criminally liable; rather, criminal acts are attributed to the individual who deployed, configured or deliberately utilized the system for illicit activities. Consequently, criminal responsibility remains inherently linked to the human agency exercising control over the technological tool.¹¹

Accordingly, AI systems lack criminal capacity due to the absence of "cognition" and "free will," the two fundamental pillars of criminal intent in traditional jurisprudence. Given that these systems function as executive tools operating according to pre-programmed algorithms, their "will" remains derivative of the inputs provided by their operators. Therefore, criminal liability for unlawful acts is ascribed to the natural or legal person (the programmer or user) as the "moral author" (*Auteur Moral*) who exercised control over the system's direction, so long as artificial intelligence remains devoid of full autonomous volition.¹²

4) Strict Liability:

Claimants face a fundamental challenge in establishing a causal link between faults arising from the use of Artificial Intelligence (AI) technologies and the resulting damage. The burden of proof lies with the injured party to demonstrate that a specific act was the direct and proximate cause of the outcome. Given the multiplicity of inputs and stakeholders, technical and human errors often intersect, necessitating the judiciary to isolate the "material fault" that effectively produced the damage from the aggregate of presented facts. Consequently, the causal link emerges as the most critical and complex element; the mere existence of fault or damage is insufficient unless a deterministic causal nexus is established between them.¹³

Strict liability (Liability without fault) is predicated on the attribution of damage regardless of a proven fault, particularly when the activity is inherently dangerous or involves means capable of inflicting significant harm. This paradigm is rooted in the "risk-distribution" theory, which assigns liability to the entity that benefits from or controls the activity. Regarding AI, this approach is deemed more appropriate for high-risk applications such as autonomous systems in transportation or medicine where the "opaque" nature of certain models renders the traditional requirement of proving fault exceptionally burdensome.¹⁴

The significance of strict liability lies in its capacity to ensure redress without the prerequisite of proving negligence, thereby alleviating the burden on the claimant when identifying a specific defect or point of failure is technically prohibitive. European parliamentary studies have proposed a risk-management approach that focuses on holding the party best positioned to control the risk accountable. This trend appears increasingly suitable for high-risk AI systems.

In conclusion, it is evident that traditional liability theories remain fundamentally valid for interpreting AI-generated damages, yet they require a degree of adaptation to address the specificities of this field. As system autonomy increases and technical architectures become more intricate, the necessity of evolving liability rules becomes paramount to ensure a balance between protecting the injured party and fostering technological innovation.

C) International and Comparative Principles in Regulating Liability:

The regulation of liability in the field of Artificial Intelligence (AI) demonstrates that this subject is no longer a purely domestic concern. Instead, it has become a focal point of international and comparative interest, given the cross-border legal implications of intelligent technologies. Accordingly, reviewing international principles and comparative legislative models aims to highlight various trends in liability management and to extract insights conducive to constructing a more effective and appropriate legal framework.

1) The European Approach:

The European approach is predicated on the principle that AI regulation must be risk-based and anchored in the protection of fundamental rights. This explains the significant emphasis on transparency, traceability and human oversight. Studies issued by the European Parliament have presented a clear conceptualization asserting that civil liability should be distributed according to the "capacity to control the risk," rather than merely the technical status of the system. This confirms that the European Union adopts a risk-oriented regulatory framework, establishing transparency, documentation and human intervention as paramount legal safeguards. Such a model reflects a commitment to "ex-ante" prevention rather than merely relying on the "ex-post" remediation of damages.¹⁵

2) The American Approach:

In the United States, there is currently no comprehensive federal AI legislation comparable to the European model. Instead, regulation relies on existing legal principles,

administrative directives and judicial oversight. The Federal Trade Commission (FTC) and other federal agencies have consistently asserted that there is no "AI exemption" from the law; consequently statutes governing competition, consumer protection and civil rights remain fully applicable to automated systems. The fundamental premise is to refrain from granting artificial intelligence a specialized legal carve-out, opting instead to integrate it within established legal frameworks. This approach renders liability in the American legal environment more closely tied to judicial pragmatism and the case-by-case characterization of disputes.¹⁶

3) OECD Principles [International Standards]:

The OECD Principles on Artificial Intelligence serve as a global benchmark, emphasizing alignment with human rights, transparency and accountability. These principles gain particular significance as they transcend mere ethical guidelines, offering a practical framework that can be leveraged in national legislation and the distribution of liability among various stakeholders. This underscores their role as a critical normative framework that places transparency and accountability at the core of AI regulation. Legal scholarship utilizes these principles to construct a balanced paradigm that fosters innovation while ensuring that actors do not evade liability. Therefore these principles do not merely provide fragmentary solutions; rather they offer a foundational reference for harmonizing comparative legislative trends.¹⁷

4) The Asian Approach:

Certain Asian nations, led by China, are shifting toward a more centralized regulatory framework characterized by stringent oversight particularly in the domains of generative AI and deep-learning systems. This trend demonstrates that AI regulation does not follow a singular global model; rather it is shaped by the legal and political philosophies of each state, oscillating between regulatory liberalism in some jurisdictions and rigorous preventive surveillance in others. Consequently, liability for artificial intelligence cannot be understood in isolation from a state's regulatory philosophy, where preventive protection may sometimes take precedence over regulatory freedom. This diversity underscores the absence of a unified global paradigm, revealing instead multiple approaches that vary between rigid oversight and flexible self-regulation.¹⁸

In summary, the diversity of international and comparative principles highlights that the regulation of AI liability remains in a formative stage, marked by a tension between preventive regulation and reliance on traditional rules. Therefore, harmonizing these disparate approaches is essential for establishing a global legal framework that enhances accountability without stifling technological progress.

To conclude this chapter, it can be asserted that the theoretical foundations of legal liability for artificial intelligence necessitate a precise classification of systems an adaptation of liability theories, and an assimilation of various international models. These elements constitute essential tools for addressing the practical challenges related to the evidentiary proof of damage and its equitable distribution.

Section II: Practical Challenges and Proposed Solutions for the Attribution of Liability

This section serves as a practical framework for addressing the challenges faced by the legal system in establishing causation and distributing liability for AI-generated damages, building upon the theoretical foundations analyzed in section I. It focuses on registration mechanisms, insurance schemes, and sanctions as pragmatic solutions, while offering legislative proposals that pave the way for the future of legal liability in the age of artificial intelligence.

A) Challenges in Establishing Causation for AI-Generated Damages:

In this section, we address one of the most intricate contemporary legal dilemmas, centered on the difficulty of proving the causal link between an automated act and the resulting damage. It highlights the practical hurdles encountered by the judiciary in the face of "Black Box" complexity and unpredictable algorithmic outcomes.

1) The "Black Box" Problem in Algorithms:

The "Black Box" concept represents one of the most formidable legal challenges in AI litigation, describing algorithms whose internal logic remains inscrutable to users and judges alike, despite the transparency of inputs and outputs. This phenomenon arises from the complexity of deep-learning models containing millions of parameters, rendering the tracking of an individual decision practically impossible. Consequently, the injured party faces significant difficulty in proving the specific "defect" necessary to establish liability, especially as corporations often refuse to disclose model details, citing "trade secrets" protections.

This opacity obstructs the application of traditional causation principles and undermines the principle of "equality before the law," as it grants a legal advantage to those possessing technical expertise. Furthermore, this issue necessitates the advancement of "Explainable AI" (XAI) frameworks, which mandate that developers provide simplified, human-understandable explanations for automated decisions.¹⁹

2) Damages Arising from Unforeseeable Behaviors:

AI-related harms are distinct in that they often stem from behaviors unanticipated by designers, such as the failure of autonomous driving systems in "edge cases" – rare scenarios involving extreme weather or sudden interactions with unpredictable elements. These anomalies complicate the establishment of causation as they may not result from a blatant design flaw but rather from "under-representation" in the training datasets. Consequently, it becomes arduous to discern whether the damage originated from systemic deficiencies, external factors or their convergence. This underscores the necessity for novel legal standards of liability tailored to unpredictability and highlights the imperative for rigorous, comprehensive testing protocols prior to the commercial deployment of critical systems.²⁰

3) The Role of Tech Corporations in Evidentiary Obstruction:

Technology firms play a pivotal role in the challenges associated with the burden of proof. While regulations such as the GDPR mandate transparency for high-risk systems, corporations frequently invoke "trade secret" protections to withhold algorithmic details and training data. This creates an inherent tension between the claimant's right to evidence and the innovator's intellectual property rights. Furthermore, privacy policies often hinder the forensic replication of incidents. Legal scholarship, therefore, advocates for obligating companies to maintain "incident logs" that provide sufficient technical detail without infringing on privacy. This conflict also suggests the need for "Technical Legal Guardians" to represent the interests of injured parties in dealings with tech giants.²¹

4) The Prohibitive Costs of Expert Testimony and Technical Tribunals:

Establishing causation necessitates the intervention of technical experts to deconstruct "Black Box" logic and interpret systemic behavior. However, the neutrality of experts and the prohibitive costs of their services constitute a significant barrier for individual litigants. To mitigate this, there are proposals to establish specialized "Technical Courts" endowed with the authority to access proprietary data under strict supervision, employing unified standards for evaluating digital evidence similar to Intellectual Property tribunals. Moreover, there is a pressing demand for the specialized training of judges in emerging technologies and the creation of judicial databases for technical evidence.²²

In conclusion, the challenges of establishing a causal link in AI-related damages reveal an urgent need to develop legal instruments capable of transcending "Black Box" complexity. Relying on specialized technical expertise and dedicated tribunals, while mandating corporate transparency, represents the most viable path toward establishing liability and achieving justice in the face of these sophisticated technological harms.

B) Practical Mechanisms for Ensuring Accountability and Redress for AI-Generated Damages:

This section serves as the pivotal transition from evidentiary challenges to pragmatic solutions aimed at ensuring accountability and compensation for AI-related harms. It focuses on registration protocols, insurance frameworks, and sanctioning regimes as functional instruments that shift the burden of liability from the injured party to the liable entity. Consequently, it represents a bridge between "ex-ante" prevention and "ex-post" remediation achieving a necessary equilibrium between legal protection and technological innovation.

1) Transparency Documentation and Mandatory Registration:

Transparency documentation and the mandatory registration of high-risk AI systems constitute essential tools for the attribution of liability. Providers are obligated to document training datasets, development processes, potential risks, and mitigation strategies thereby enabling the judiciary to assign liability based on objective evidence. Centralized registration facilitates the traceability of systems across the entire value chain.

from developer to end-user and partially shifts the burden of proof to the defendant. Empirical studies indicate that this approach significantly reduces the volume of protracted litigation.²³

2) Compulsory Insurance Against Artificial Intelligence Risks:

Compulsory insurance is proposed as a structural solution for distributing AI risks, analogous to mandatory motor vehicle insurance. This framework covers damages resulting from high-risk systems and incentivizes providers to develop safer technologies, as premiums are indexed to the degree of inherent risk. Such a mechanism ensures prompt redress for the injured party without the delays of lengthy judicial proceedings and serves as an economic catalyst for compliance with safety standards, whereby lower premiums are awarded to rigorously tested systems.²⁴

3) Collective Compensation Funds:

Collective compensation funds are introduced to address damages arising from AI systems with diffuse or systemic risks, structured as joint initiatives between governments and corporations similar to nuclear energy indemnity funds. These funds represent a model of collective responsibility suited to the complexity of this field, allocating risks to the parties most capable of absorbing them. Moreover, they alleviate the judicial burden, accelerate the indemnification process and offer a middle-ground solution between individual liability and collective immunity.²⁵

4) Administrative and Civil Sanctions:

Administrative and civil sanctions are imposed on entities failing to comply with regulatory requirements; for instance the EU AI Act (2024) stipulates fines of up to 6% of total global turnover for prohibited AI practices. These penalties encourage adherence to transparency and registration obligations while fostering a "culture of compliance" within the tech sector. Such sanctions serve as a more potent preventive deterrent than retroactive liability, ensuring a higher degree of voluntary institutional compliance.²⁶

In conclusion, practical mechanisms specifically registration, insurance and sanctioning regimes constitute an integrated toolkit for ensuring accountability and equitable redress for AI-related damages. By shifting the evidentiary burden from the claimant to the producer these instruments successfully balance the protection of civil rights with the continued promotion of innovation.

C) Legislative Proposals for the Future of Legal Liability in Artificial Intelligence:

This section constitutes the conclusion of the research, offering forward-looking proposals that transcend the current legal framework for regulating AI liability. It focuses on pioneering concepts such as "Limited Electronic Personhood," objective testing standards, and international cooperation. Accordingly it aims to establish an advanced legal framework that achieves a balanced justice between the protection of rights and the promotion of technological innovation.

1) Granting Limited Electronic Personhood:

There is a proposal to grant autonomous AI systems a "Limited Electronic Personhood" to hold them directly liable, analogous to the legal personality of corporations. This approach would shift the evidentiary burden from the injured party and enhance accountability; however, debates persist regarding the boundaries of this personhood for ultra-autonomous systems. This trend represents a paradigm shift from viewing AI as a mere tool to recognizing it as a quasi-autonomous agent.²⁷

Conversely, the jurisprudential school opposing the granting of legal personality to intelligent systems is rooted in objective concerns regarding the potential undermining of civil liability rules. Critics fear that such a move might lead to a decline in the standards of "due diligence" among manufacturers and users alike. Attributing legal consequences to a robot as an independent entity could be exploited as a "pretext" to exonerate human parties from their responsibility for design flaws or operational and update errors. Consequently, this perspective argues that conferring legal status upon machines would, in effect, allow the actual actors to evade punishment and compensatory obligations, thereby disrupting the principle of legal deterrence that mandates producers to ensure the safety and security of deployed technologies.²⁸

2) Objective Risk-Testing Standards:

It is imperative to develop objective pre-deployment testing standards that encompass diverse scenarios and long-term risk assessments. These standards should be developed through the collaboration of technical and legal experts, incorporating "stress tests" for rare incidents and "edge cases" as a preemptive tool for damage prevention.²⁹

3) International Cooperation for Standard Harmonization:

The nature of AI necessitates international cooperation to harmonize standards, such as the establishment of a high-level body to oversee cross-border liability, similar to nuclear energy regulations. Such cooperation is essential because digital harms are not confined by geographical borders; moreover, it fosters trust in trans-border technologies.³⁰

4) Developing Judicial Jurisprudence regarding Artificial Intelligence:

The judiciary plays a decisive role in developing "AI Jurisprudence" by interpreting existing rules and formulating new principles grounded in reasonableness and equity. This judicial activism serves to fill legislative lacunae until comprehensive legislation matures through various specialized courts.³¹

The proposed legislative recommendations represent a proactive vision for regulating AI liability, transcending traditional rules to offer an advanced framework that integrates electronic personhood, objective testing standards and coordinated international cooperation. They transition the legal system from a reactive stance of adaptation to one of proactive planning, emphasizing the necessary tandem between protecting the injured party and encouraging technological innovation. Ultimately, these proposals pave the way

for a judicial system capable of addressing future challenges related to autonomous and technologically advanced systems.

Conclusion:

The ambiguity surrounding the legal attribution of liability for Artificial Intelligence (AI) damages necessitates a paradigm shift from traditional models based on direct personal assignment to a hybrid framework. This framework distributes responsibility among the creator, the operator and the system itself through transparency, registration and insurance mechanisms. AI is not a fully autonomous legal agent but rather a hybrid tool that requires risk distribution across the entire value chain to achieve justice without stifling technological innovation.

The Results:

Adaptability of Traditional Rules: Traditional liability regimes (tortious, contractual, and strict liability) remain fundamentally valid but require adaptation to accommodate "Black Box" opacity and unpredictable automated behaviors.

The Risk-Based Paradigm: A risk-based approach is the most viable and pragmatic model for classifying intelligent systems and defining the subsequent legal duties associated with them.

Causation Hurdles: The challenges of establishing a causal link necessitate the intervention of specialized technical experts and the establishment of technical tribunals to interpret automated decision-making processes.

Global Regulatory Divergence: International and comparative regulation reveals a tension between preventive oversight (Europe) and judicial flexibility (USA) highlighting the need for harmonized standards for high-risk systems.

Recommendations:

Mandatory Centralized Registration: Establishing a national or international registry for all high-risk systems, accompanied by comprehensive transparency documentation detailing training datasets, inherent risks, and mitigation protocols.

Development of Compulsory Insurance: Implementing mandatory insurance schemes for high-risk systems, co-funded by governments and corporations, alongside collective compensation funds modeled after nuclear energy indemnity structures.

Establishment of Specialized Technical Courts: Founding dedicated tribunals endowed with the authority to access proprietary data under rigorous judicial supervision, complemented by the specialized training of judges in this domain.

Granting Limited Legal Personhood: Conferring a limited legal personality upon autonomous systems—shared with the creator—to enable direct liability within the capacity for redress.

Strengthening International Cooperation: Forming a high-level international body to harmonize high-risk standards and regulate cross-border liability frameworks.

In conclusion, the judiciary remains the primary catalyst for evolving AI jurisprudence until legislation matures beyond the experimental phase into a structured system. Such a system must effectively bridge the protection of individual rights with the

freedom of technological innovation, while consistently reaffirming the injured party's right to swift and equitable redress.

Bibliography:

- ¹ - Mohammed Fadel Mahdi Al-Khafaji, *Types of Artificial Intelligence*, Al-Khawarizmi Center for Artificial Intelligence (KCAI), available at: <https://kcaiiq.org/authors-list/view?id=4>, January 7, 2026, 17:05.
- ² - Abhiuday Chandra *Liability Issues in Relation to Autonomous AI Systems*•Bucerius Law School•Germany•September 29, 2017• available at : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3052154 ,03/01/2026 at 12:15.p p 2 3.
- ³ - Maarten Herbosch,*Liability for AI Agents*,North Carolina Journal of Law & Technology, Volume 26, No. 3, Pp. 391-458 (2025),April 28, 2025, available at : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5236649 ,7/01/2026 at 14: 10 .p p 423_424.
- ⁴ - Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence Publications Office of the European Union, available at <http://data.europa.eu/eli/reg/2024/1689/oj>,5/01/2026At 22:40.
- ⁵ - Zeinab Bennour and Mokhtar Bennour,*Legal Liability for Artificial Intelligence Systems: An Analytical Reading of the European AI Act and the Prospects for its Adoption in the Arab World*. International Law Journal for Research Studies, Democratic Arab Center, Vol7, Issue 21,2026, pp 110-111.
- ⁶ - Filali Ali, *Obligations: The Act Meriting Compensation*. 3rd ed. Algeria: Mofem Publications, 2013,p. 239.
- ⁷ - Fadhli Idriss, *Al-Wajiz in the General Theory of Obligation*. Algeria: Dar Al-Kitab, 2005/2006,p 144.
- ⁸ - Abhuiday Chandra•op cit.
- ⁹ - Lakhdar Refaf and Fayrouz Maouche, 'The Specificity of Civil Liability for Damages Caused by Artificial Intelligence Systems in Algerian Law'Tobna Journal for Academic Scientific Studies, Barika University Center, Algeria, Vol. 6, Issue 1,2023, pp 572-573.
- ¹⁰ - Lakhdar Refaf and Fayrouz Maouche,op cit
- ¹¹ - Nadia Banteka,*Artificially Intelligent Persons*,lorida State University College of Law, Houston Law Review 537 (2021),available at: <https://ir.law.fsu.edu/articles/7431>.,11/01/2026,at14:33.
- Meriem Abdelwahab and Hind Labiedh•*Criminal Liability for Artificial Intelligence Crimes*. Journal of Law and Interdisciplinary Sciences, Ziane Achour University, Djelfa, Algeria, Vol. 2, Issue 2,2023,p 690.
- ¹² - Nisrine mechta. *Criminal Liability for Artificial Intelligence Crimes in Algerian Legislation*. Journal of Legal and Economic Studies, Barika University Center, Algeria, Vol 8, Issue 2,2025, p. 529.
- ¹³ - Fahad Saeed Al-Dhahouri and Mustafa Salem Al-Nujaifi,*Administrative Liability for the Use of Artificial Intelligence Based on Fault*,t University of Shariqah Journal for Humanities and Social Sciences, Vol 21, Issue 1,2024• p317.
- ¹⁴ - Maarten Herbosch,op cit.
- ¹⁵ - *Artificial Intelligence and Civil Liability*,European Parliament,op cit.
- ¹⁶ - *Efforts against discrimination and bias in automated systems*.federal trade commission :

https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf, 15/01/2016 at 17:22, p3.

¹⁷ - Oecd, AI principles report February 2026, <https://www.oecd.org/en/topics/ai-principles.html> 01/03/2026 at 14:27.

¹⁸ - Oecd, AI principles report, op, p8 p9

¹⁹ - Jenna Burrell, *How the machine 'thinks': Understanding opacity In machine learning algorithms*, <https://doi.org/10.1177/2053951715622512>, 17/01/2026 at 16:45.

²⁰ - Henrique Sousa Antun, *Civil Liability Applicable to Artificial intelligence: A Preliminary Critique of the European Parliament Resolution of 2020*, https://scholar.google.com/scholar?q=Artificial+Intelligence+and+Civil+Liability+European+Parliament+2020#d=gs_qabs&t=1774624587928&u=%23p%3DzULZfrIEjJ2026/01/15, at 13:00, P15-18.

²¹ - Chandra Abhuiday, op cit.

²² - Maarten Herbosch, op cit.

²³ - (EU AI Act, 2024), op cit.

²⁴ - Maarten Herbosch, op cit, pp415. 416.

²⁵ - Abhuiday Chandra, op cit, P 8.

²⁶ - EU AI Act, 2024, op cit.

²⁷ - Nadia Banteka op cit, p535 and seq.

²⁸ - Lamia Hamzaoui, *Artificial Intelligence as a Model for Contemporary Challenges to Tortious Liability*. *Algerian Journal of Law and Justice*, Vol. 10, Issue 1, 2024 p148.

²⁹ - Maarten Herbosch, op cit, p410 and seq.

³⁰ - Oecd, AI principles report February 2026, op cit.

³¹ - Abhuiday Chandra, op cit.