

ARTICLE



REVISTA
COLETA CIENTÍFICA

Civil Liability for Damages Arising from Artificial Intelligence and Digital Tools: A Comparative Analytical Study in Light of European Legislative Developments and the Position of Algerian Civil Law

Responsabilidade Civil por Danos Decorrentes da Inteligência Artificial e dos Instrumentos Digitais: Estudo Analítico Comparado à Luz dos Desenvolvimentos Legislativos Europeus e da Posição do Direito Civil Argelino

Djouabi fella¹

<https://orcid.org/0009-0001-5143-1068>

Phd, Faculty of Law, University of Algiers 01, Algeria.

E-mail: f.djouabi@univ-alger.dz

Publication information

ARK: [24285/RCC.v10i20.281](https://nbn-resolving.org/urn:nbn:br:coleta-2026-10-20-281)

ISSN: 2763-6496

Keywords:

Black Box.
Defective Products.
Legal Presumptions.
AI Act.
Algorithmic Bias.
Product Liability Directive.

Palavras-chave:

Caixa-preta.
Produtos defeituosos.
Presunções legais.
Regulamento de Inteligência Artificial (AI Act).
Viés algorítmico.
Diretiva de Responsabilidade por Produtos

Abstract

This article examines the question of civil liability for damages caused by artificial intelligence systems and digital tools through a comparative analytical study encompassing contemporary European legislative developments and the Algerian civil law framework. The study reveals a structural deficiency inherent in the classical rules of civil liability—whether in the provisions governing the custodian's liability for things or in product liability regimes—when confronted with the adaptive characteristics and operational autonomy that define intelligent systems. This deficiency generates acute evidentiary dilemmas, particularly in light of the "black box" phenomenon, thereby placing victims' rights at serious risk of irremediable loss. By contrast, European legislation—embodied in the Artificial Intelligence Act of 2024 and the updated Product Liability Directive (EU) 2024/2853—adopts a flexible strict liability regime that reconfigures the boundaries of proof through legal presumptions and broadens the scope of compensable damages. Algerian legislation, conversely, remains anchored in concise traditional provisions that neither accommodate the dynamics of algorithmic code nor recognize the causal presumptions necessary to protect injured parties, thereby necessitating comprehensive and systematic legislative reform.

¹ PhD in Faculty of Law, University of Algiers 01, Algiers, Algeria (2016); a Master's degree in law from Faculty of Law, University of Algiers 01, Algiers, Algeria (2012). a PhD in Law from Faculty of Law, University of Algiers 01, Algiers, Algeria (2020).

Resumo

O presente artigo examina a problemática da responsabilidade civil por danos causados por sistemas de inteligência artificial e instrumentos digitais, mediante um estudo analítico comparado que abrange os desenvolvimentos legislativos europeus contemporâneos e o quadro normativo do direito civil argelino. O estudo revela uma deficiência estrutural inerente às regras clássicas da responsabilidade civil—tanto nas disposições que regem a responsabilidade do guardião da coisa quanto nos regimes de responsabilidade pelo fato do produto—quando confrontadas com as características adaptativas e a autonomia operacional que definem os sistemas inteligentes. Essa deficiência gera dilemas probatórios agudos, particularmente à luz do fenômeno da "caixa-preta" (*black box*), colocando os direitos das vítimas em sério risco de perda irremediável. Em contrapartida, a legislação europeia—consubstanciada no Regulamento de Inteligência Artificial de 2024 e na Diretiva atualizada relativa à Responsabilidade por Produtos Defeituosos (UE) 2024/2853—adota um regime de responsabilidade objetiva flexível que reconfigura os limites da prova por meio de presunções legais e amplia o âmbito dos danos indenizáveis. A legislação argelina, por seu turno, permanece ancorada em disposições tradicionais concisas que nem acomodam a dinâmica do código algorítmico nem reconhecem as presunções causais necessárias à proteção das partes lesadas, impondo-se, assim, uma reforma legislativa abrangente e sistemática.

I. Introduction

Artificial intelligence, as one of the most transformative technological revolutions of the contemporary era, represents a scientifically complex paradigm that fundamentally challenges the conceptual and structural foundations of private law. Since the French legislature established the general theory of civil liability in the Napoleonic Code of 1804, the assumption underlying tortious liability has remained intimately linked to human volition—or, at most, to animals and things subject to human control. When, however, an autonomous machine adopts a harmful decision untethered to any conscious human will, and when neither its creators nor its operators can adequately explain the reasoning pathway that produced that decision, the traditional architecture of liability collapses under the weight of unprecedented complexity.

The technological transition from linearly programmed software with predefined commands to machine learning systems and deep neural networks did not constitute a mere technical advancement; rather, it effected a fundamental transformation in the very nature of agency itself. These systems autonomously develop the parameters governing their decisions on the basis of training data and interaction outputs, and they produce material acts with legal consequences in the absence of any contemporaneous human direction. This reality renders the classical theory of personal fault structurally incapable of providing an adequate legal basis for accountability, while simultaneously complicating the identification of the effective custodian and the establishment of the causal nexus.

This problematic acquires heightened significance in light of the accelerating pace of European legislative reform. The European Union has moved swiftly to address regulatory lacunae through a comprehensive legislative package, prominently including Regulation (EU) 2024/1689 on Artificial Intelligence (hereinafter the AI Act) and the updated Product Liability Directive (EU) 2024/2853. Against this backdrop, the Algerian legal framework appears to confront an increasingly pronounced gap between its existing civil law provisions and the successive demands of the digital age.

The central research question animating this article is as follows: Do the general rules of civil liability under Algerian law—and under comparative law more broadly—possess the normative capacity to accommodate the damages produced by artificial

intelligence systems and to provide just and adequate redress? And what legislative reforms are necessary to bridge this gap?

This article employs a comparative analytical methodology that integrates a critical reading of Algerian, French, and European legislative texts with an examination of specialized legal scholarship and an analysis of newly enacted legislative instruments, with a view to presenting a comprehensive vision for necessary legal reform.

II. Conceptual Framework and Structural Challenges Posed by Artificial Intelligence to Civil Liability Rules

1. The Legal Nature of Artificial Intelligence Systems: The Debate over Classification and the Dilemma of Legal Identity

Contemporary artificial intelligence systems are distinguished by a set of technical characteristics that place them outside the ambit of traditional legal definitions. They are not merely passive instruments that translate human commands into mechanical execution; rather, they function as operational agents possessing a degree of decisional autonomy determined by the complexity of their algorithmic architecture and the depth of their training data (Goodfellow, Bengio, & Courville, 2016, pp. 1–10). This reality has generated an intense doctrinal dispute over the appropriate legal classification of these entities.

The first approach—represented by the European Parliament's resolution of 2017—advocated exploring the possibility of conferring a novel form of "electronic legal personality" (*personnalité juridique électronique*) upon autonomous artificial intelligence systems, reasoning that the independence of their decision-making necessitates their direct accountability and the attribution to them of a distinct legal patrimony (European Parliament, 2017). This proposal, however, has attracted vigorous scholarly criticism. Critics contend that recognition of such legal personality could effectively shield developers and manufacturers from comprehensive accountability and would establish a liability model that serves the interests of the technology industry at the expense of victims of digital harm (Delvaux, 2017). Notably, a group of leading artificial intelligence researchers and ethicists submitted an open letter to the European Commission in 2018 warning against the premature attribution of legal personality to artificial intelligence systems, emphasizing that such a step would obscure, rather than clarify, the human chains of responsibility (Floridi et al., 2018, p. 690).

The second approach, which predominates in comparative legal scholarship, insists upon treating artificial intelligence as a "thing" or digital "product," while seeking to reformulate objective liability frameworks in a manner suited to the unique characteristics of such entities (Borghetti, 2019, p. 4). This approach appears more consonant with the legislative logic of risk distribution and the preservation of human accountability chains, without recourse to the creation of a fictional legal persona for the machine.

2. The "Black Box" Problem and the Collapse of Traditional Liability Elements

The deepest legal problem is manifest in the "black box" phenomenon (*l'effet boîte noire*), which legal and computer science scholars have described as the most formidable challenge confronting the civil liability system in the digital age. This phenomenon denotes the practical impossibility of accessing the internal algorithmic pathway that produced a harmful decision—a challenge that persists even for the system's own developers (Pasquale, 2015, p. 8). Deep learning algorithms operate through layers of neural networks that transform raw data into decision outputs in a manner that is nearly impossible to fully trace or explain.

This programmatic opacity casts its shadow directly upon three foundational elements of liability law: the element of fault, the element of damage insofar as its attribution is concerned, and most critically, the causal relationship. The injured party cannot establish whether the harm resulted from an original design defect in the system, from training data contaminated by societal biases, or from an adaptive behavior autonomously developed by the machine during its operational phase (Mittelstadt, Allo, Taddeo, Wachter, & Floridi, 2016, pp. 1–8). This produces a severe functional dysfunction in the mechanism of reparation that imperils the fundamental purpose of civil liability law.

The European Union Agency for Fundamental Rights (FRA) issued a report in 2020 documenting cases in which predictive policing systems produced discriminatory outputs that their developers could not retrospectively explain—a striking illustration of how the black box effect translates from a theoretical concern into a concrete juridical obstacle (FRA, 2020). This reality underscores the urgent need for legislative responses that do not merely shift the burden of proof incrementally but fundamentally reconceive the evidentiary architecture of digital liability.

III. Classification of Damages Arising from Artificial Intelligence and Analysis of Their Typology

1. Traditional Harms in the Digital Context

Some artificial intelligence-related harms do not depart from the familiar categories of physical, material, and moral damage; however, the particularities of the digital context reshape their characteristics and complicate their attribution. Physical injuries caused by accidents involving autonomous vehicles or deviations by surgical robots are recognizable in their consequences, yet they resist traditional analysis with respect to the attribution of fault (Vladeck, 2014, p. 118). Similarly, material harms resulting from erroneous algorithmic decisions in the management of electrical grids or industrial production lines conform to recognizable damage typologies in their final effects while presenting novel difficulties of causal attribution. Moral damages—such as those suffered by a patient incorrectly informed of a terminal diagnosis by a malfunctioning intelligent diagnostic application—are distinctive in that they flow from an "automated recommendation" rather than a "direct human act," which complicates the question of accountability in ways that classical doctrine does not adequately address.

2. Novel Harms: Products of the Digital Environment

The artificial intelligence environment has produced novel categories of harm that transcend, by their nature and scope, the bounds of traditional damage typologies.

Data Damage and Digital Asset Corruption: Harm is no longer confined to breaches of data confidentiality but extends to the destruction of digital informational assets themselves. The corruption of personal files stored in cloud systems or the erasure of educational and professional records caused by algorithmic malfunction has come to be recognized in modern legislation as an autonomous compensable harm, independent of any requirement of tangible physical damage (Directive (EU) 2024/2853, Recital 34). This represents a paradigmatic shift in the conception of legally cognizable injury, moving beyond the material world to encompass the integrity of the digital patrimony of individuals.

Algorithmic Bias and Automated Discrimination: When intelligent systems extract patterns from historical data embedded with societal biases—whether racial, gender-based, or socioeconomic—they reproduce those biases in decisions concerning employment, credit allocation, and criminal risk assessment. The COMPAS algorithm, deployed in certain American courts, provides a stark illustration of this phenomenon. Empirical studies demonstrated that this algorithm exhibited a systematic bias against individuals of African descent in assessments of recidivism risk (Angwin, Larson, Mattu, & Kirchner, 2016). Such algorithmic decisions cause profound harm to the rights and fundamental freedoms of individuals in the absence of any tangible material damage amenable to valuation under conventional standards (Barocas & Selbst, 2016, pp. 671–732). The legal challenge lies in conceptualizing discriminatory algorithmic outputs as actionable wrongs and in identifying the appropriate defendants—whether the system's developer, its deploying institution, or both—within existing liability frameworks.

Deepfakes and Synthetic Generated Content: Generative artificial intelligence has enabled the production of synthetic audio-visual and textual content of a high degree of persuasiveness, giving rise to identity theft, reputational harm, and facilitation of financial fraud. The accountability question is further complicated by the multiplicity of parties involved: the developer of the generative system, the provider of the underlying cloud infrastructure, and the end-user who formulated the prompting instruction. Responsibility is distributed among these parties in a manner that renders precise legal attribution highly problematic (Chesney & Citron, 2019, pp. 1753–1820). Some European jurisdictions have begun to address deepfake-related harms through amendments to existing defamation and data protection frameworks, but a comprehensive liability regime for generative artificial intelligence outputs remains absent.

Harms Caused by Autonomous Physical Systems: This category encompasses damages produced by unmanned aerial vehicles, autonomous vehicles, and field robotics. It presents a unique juridical problem when such systems encounter a critical situation in which competing interests are in conflict—the classic "trolley problem" scenario—and adopt a preferential decision based on pre-programmed optimization parameters. In such cases, the concept of fault attributable to a human custodian is deprived of any practical content, since no human actor exercised real-time directional control over the system's choice.

IV. Evaluation of Classical Civil Liability Rules in the Face of Artificial Intelligence Damages

1. Custodial Liability for Things: The Limits of Traditional Doctrine

French civil law—and Algerian civil law in its wake—grounded the custodian's liability for things upon an assumption of objective responsibility linked to effective control. Article 138 of the Algerian Civil Code provides that whoever assumes custody of a thing—in terms of its use, management, and supervision—shall be liable for damage caused by that thing (Algerian Civil Code, Article 138; French Civil Code, Article 1242). This rule has historically accommodated a broad range of materially dangerous objects, from motor vehicles to industrial installations.

The application of this rule to artificial intelligence systems, however, reveals fundamental structural difficulties.

The Problem of Fragmented and Dispersed Custody: French and Algerian jurisprudence distinguishes between "custody of structure" (*garde de la structure*) and "custody of behavior" (*garde du comportement*) (Carbonnier, 2000, p. 397). In the context of artificial intelligence systems, custody is distributed in a complex and non-linear manner: the user of an autonomous vehicle holds physical custody, while programmatic custody—that is, the authority to update and algorithmically modify the system—remains with the manufacturing company, which is capable of altering the system's behavior remotely through cloud updates without the user's knowledge or consent. This distinction places the injured party in the difficult position of determining which party constitutes the legally responsible custodian.

The Absence of Effective Control over the Intelligent Object: Custody presupposes genuine directive authority over the behavior of the thing. The user of an artificial intelligence system, however, exercises no control whatsoever over its internal processing; the system operates according to the self-learning parameters it has independently developed. Professor Borghetti has observed that the traditional custodial liability system has fulfilled its historical function but is no longer adequate for the complexities of the digital environment, calling for a reorientation of accountability toward a specialized product liability regime with a restructured conception of defect that encompasses unsafe software (Borghetti, 2019, p. 11).

The Temporal Dimension of Custody: A further complication arises from the fact that artificial intelligence systems continue to evolve after their initial deployment. A manufacturer who relinquishes physical custody of an autonomous vehicle while retaining the capacity to modify its decision-making algorithms through remote updates occupies an anomalous position that existing custodial frameworks are ill-equipped to capture. The question of who bears custodial responsibility for a system whose behavioral parameters are continuously modified by a party remote from the site of harm has no satisfactory answer under classical doctrine.

2. Product Liability for Defective Products: Between Legal Text and Digital Reality

The European Directive 85/374/EEC—reflected in Article 140 bis of the Algerian Civil Code as amended in 2005—established a system of strict product liability independent of any requirement of fault, requiring the injured party to demonstrate only the existence of a defect, the occurrence of damage, and the causal link between them. The application of this framework to digital tools, however, encounters three structural obstacles.

The Problem of Classifying Software as a "Product": Scholarly debate has long persisted over whether immaterial software falls within the category of "movable material products" subject to product liability provisions. The updated European Directive of 2024 has resolved this debate by expressly including software, yet the Algerian legislative text contains no equivalent definition, leaving the field open to divergent judicial interpretations (Jourdain, 2003, p. 52). This lacuna is not merely technical; it has substantive consequences for the availability of strict liability to persons harmed by stand-alone software systems and cloud-based artificial intelligence services.

The Difficulty of Defining "Defect" in Adaptive Algorithms: Defect has traditionally been defined as the failure of a product to provide the safety that persons are entitled to expect. Continuous learning systems, however, autonomously modify their operational rules after market introduction, on the basis of data acquired through ongoing interaction with their operational environment. This makes it difficult to distinguish between an "original defect" in the programming at the time of commercialization and an "adaptive behavior" subsequently generated through self-learning (G'sell, 2020, p. 23). More precisely, when an algorithm causes harm on the basis of its analysis of contaminated training data, the "defect" does not reside in the original code but in the input data or in the underlying algorithmic architecture itself—a distinction that existing product liability frameworks are not equipped to draw.

Reliance on the Development Risks Defence: Comparative law provisions—including Article 140 bis of the Algerian Civil Code—permit a manufacturer to escape liability if it establishes that the state of scientific and technical knowledge at the time the product was put into circulation was not sufficient to enable the defect to be discovered. This defence affords artificial intelligence companies broad immunity, since the behaviors of deep learning systems cannot be fully predicted even by their own developers (Calo, 2015, p. 531), effectively depriving injured parties of compensation on the ground that the defect was scientifically unknowable at the time of release.

3. The Crisis of Proof and the Opacity of Causation

The crisis of proof represents the most decisive factor bearing upon the effectiveness of legal protection for persons harmed by artificial intelligence systems. Whereas general rules require proof of a direct causal link between fault and damage, the black box phenomenon systematically deprives injured parties of the evidentiary tools necessary to discharge this burden. The complexity is compounded by the fragmentation of digital value chains among the original programmer, the data provider, the hardware manufacturer, the cloud service provider, and the end-user, which disperses accountability and renders the identification of the direct cause of any particular malfunction extremely difficult (Hildebrandt, 2015, p. 200).

The asymmetry of information between plaintiffs and defendants in artificial intelligence litigation is qualitatively different from that encountered in conventional product liability cases. Whereas a claimant harmed by a defective pharmaceutical product may face difficulties in establishing causation, the relevant technical information is at least theoretically comprehensible and communicable. In artificial intelligence cases, even the defendant may lack the technical capacity to explain the system's decision-making process, creating an informational vacuum that cannot be filled through conventional disclosure mechanisms.

V. Contemporary European Legislative Frameworks for Regulating Artificial Intelligence Damages

1. The AI Act: Regulation (EU) 2024/1689

The European Artificial Intelligence Act, enacted in 2024, constitutes the first comprehensive international legislative framework for the regulation of artificial intelligence, adopting a risk-based approach organized across four graduated levels (Regulation (EU) 2024/1689, Article 6).

The first level—unacceptable risk—imposes an absolute prohibition on systems used for behavioral social scoring and unauthorized psychological manipulation. The second level—high risk—imposes stringent requirements regarding data quality and technical documentation upon providers of systems deployed in critical infrastructure, medical diagnosis, employment, judicial proceedings, and security management, coupled with a mandatory requirement of effective human oversight (human-in-the-loop). The third level—transparency risk—requires generative artificial intelligence systems to explicitly inform individuals of the existence of automated processing. Systems presenting minimal risk are subject to voluntary codes of conduct.

The significance of this Regulation for civil liability law lies in its establishment of a presumptive standard of regulatory fault: failure by a developer or operator to comply with the prescribed safety requirements constitutes a legal breach that facilitates the injured party's demonstration of liability without requiring penetration of the black box. This provides the injured party with a substantive legal anchor upon which to rely before the courts, rather than being consigned to the labyrinth of technical proof (Floridi et al., 2018, pp. 690–691). The Regulation thus serves a dual function: it directly governs market conduct, and it indirectly restructures the evidentiary landscape of private litigation by establishing a publicly verifiable compliance record against which claims of liability can be assessed.

2. The Updated Product Liability Directive: Directive (EU) 2024/2853

This Directive, enacted in October 2024—which repealed Directive 85/374/EEC and entered into force in December 2024, with Member States granted until December 2026 to transpose it into national law—represents a qualitative transformation in the rules governing liability for digital products (Directive (EU) 2024/2853, Article 5).

Expansion of the Concept of "Product": The Directive expressly includes all categories of software—including embedded and autonomous artificial intelligence systems and cloud computing applications—within the definition of a product subject to liability. It also broadens the category of persons qualifying as "producer" to encompass

system providers, update developers, importers, and digital platforms, thereby ensuring the presence of a financially solvent party within the Union against whom claims can be brought (Directive (EU) 2024/2853, Article 7).

Expansion of Compensable Damages: The Directive transcends traditional categories of physical and material harm, recognizing compensation for serious damage affecting medically recognized psychological health (*dommages psychologiques reconnus médicalement*), and for the destruction or corruption of data not used for professional or commercial purposes (*destruction ou altération de données non utilisées à des fins professionnelles ou commerciales*) (Directive (EU) 2024/2853, Article 4). This expansion reflects a legislative recognition that the harms most commonly produced by artificial intelligence systems—discrimination, psychological distress, and digital asset loss—have not been adequately addressed by existing liability frameworks calibrated to physical injury.

Redistribution of the Burden of Proof and the Establishment of Legal Presumptions: This is perhaps the most significant innovation of the Directive from the perspective of victim protection. The Directive establishes two rebuttable legal presumptions: a presumption of defect, which arises when the defendant fails to disclose the technical evidence requested by the court or when regulatory non-compliance is established; and a presumption of causation, which arises automatically once defect is established and the damage is of a type consistent with the nature of that defect (Directive (EU) 2024/2853, Article 10). These two presumptions constitute a practical legislative mechanism for circumventing the obstacle of the black box and for securing just redress for victims of artificial intelligence systems.

3. The General Data Protection Regulation: GDPR (EU) 2016/679

The General Data Protection Regulation performs a preventive function against unjust algorithmic exploitation. Article 22 confers upon individuals the right not to be subject to decisions based solely on automated processing—including profiling—when such decisions produce legal effects or similarly significantly affect them (Regulation (EU) 2016/679, Article 22). Article 82, moreover, establishes a system of strict liability that obliges data controllers and processors to compensate any person who suffers material or non-material damage as a result of a processing operation that infringes the Regulation's provisions, unless they can demonstrate that they were in no way responsible for the event giving rise to the damage (Regulation (EU) 2016/679, Article 82). This regime intersects with civil liability law by achieving a shift in the burden of proof in favor of the injured party, without requiring that party to produce comprehensive technical evidence of the algorithmic failure.

4. The Proposed AI Liability Directive (2022)

Although the proposed AI Liability Directive has not yet been enacted in its final form, the European Commission's 2022 proposal contains promising mechanisms that complement the existing legislative framework. Most notably, the proposal provides for facilitated access to evidence and technical information concerning high-risk artificial intelligence systems, and introduces a presumption of causation in cases of regulatory non-compliance. The Commission's explanatory memorandum indicates that the object of

the proposal is to bridge the gap between the general rules of non-contractual liability and the specific characteristics of artificial intelligence systems (European Commission, 2022, p. 3). The relationship between this proposed Directive and the AI Act is intended to be complementary: the AI Act establishes safety requirements, while the proposed Directive provides the civil liability consequences of their breach, creating a coherent regulatory ecosystem rather than isolated legislative interventions.

VI. Critical Assessment of Algerian Legislation and Prospects for Reform

1. Analytical Reading of the Applicable Algerian Legal Provisions

Algerian law relies upon three provisions of the Civil Code in addressing damages arising from artificial intelligence.

Article 124 of the Algerian Civil Code provides that "any act whatsoever committed by a person through his fault that causes damage to another obliges the person responsible for its occurrence to provide compensation" (Law No. 75-58, as amended). This provision presupposes the existence of a personal human fault predicated upon conscious awareness—an element that is absent in the autonomous decisions adopted by independent machine learning systems in the absence of any deliberate operational deviation on the part of the user or developer. This renders the application of Article 124 truncated in the majority of artificial intelligence damage scenarios.

Article 138 of the Algerian Civil Code imposes liability upon whoever assumes custody of a thing. Algerian courts—like their counterparts in other civil law jurisdictions—have historically interpreted the concept of "thing" as referring to tangible movable and immovable property (Supreme Court of Algeria, Decision No. 171942, 1999). This interpretive tradition has the consequence of excluding algorithms and cloud networks from the provision's scope of application. Furthermore, assigning custody to the physical user ignores that user's complete lack of effective authority over the cognitive processes of the intelligent system.

Article 140 bis of the Algerian Civil Code, introduced by the 2005 amendment, established strict liability for producers. The provision is, however, marked by a degree of brevity that renders it inadequate to the demands of the digital environment: it omits any definition of software and digital systems as products; it establishes no legal presumptions to facilitate proof; and it makes no provision for the problem of defects in adaptive algorithms. This structural deficiency leaves the injured party in an unequal contest with manufacturers and developers who possess exclusive access to the technical information necessary to establish or refute liability.

2. Supporting Special Legislation and Its Practical Limitations

Law No. 18-07 on the Protection of Personal Data represents a notable reform initiative in prohibiting the unlawful processing of personal data and regulating the rights of access, rectification, and erasure. It concentrates primarily, however, on administrative sanctions and criminal penalties without formulating precise civil law provisions establishing criteria for the quantification of compensation for moral and discriminatory damages caused by algorithmic processing and automated profiling operations (Law No. 18-07, Articles 62–68). The gap between the regulatory prohibition of unlawful data processing and the effective civil remedy for its victims remains, accordingly, substantial.

Law No. 09-03 on Consumer Protection and the Suppression of Fraud imposes upon market operators an obligation to ensure the safety of products and services. This law may be invoked when artificial intelligence systems are embedded in physical goods such as medical devices or intelligent vehicles. It falls short, however, of encompassing stand-alone software and cloud-based services delivered directly to users without a tangible material substrate, thereby narrowing its scope of application precisely in relation to the most significant scenarios of novel digital harm (Law No. 09-03, Article 6).

3. A Legislative Reform Roadmap for Algeria

In light of the structural deficiencies identified and drawing systematic inspiration from the European experience, the following comprehensive reform agenda can be outlined.

First—Amendment of Article 140 bis: The definition of "product" should be expressly expanded to encompass software and artificial intelligence systems of all types—embedded, cloud-based, and autonomous—accompanied by a definition of "defect" in adaptive systems that distinguishes between an original programming defect and a subsequent adaptive behavior generated through self-learning. The scope of the development risks defence should be narrowed in high-risk sectors such as healthcare, autonomous transportation, and critical infrastructure.

Second—Introduction of Facilitative Evidentiary Presumptions: The reform should expressly establish a presumption of defect when the defendant fails to disclose the technical evidence requested by the court, and a presumption of causation when the damage is, by its nature, consistent with the established defect. These presumptions—as demonstrated by the European Directive of 2024—need not take the form of irrebuttable conclusions; they can be framed as shifting the burden of production to the defendant while preserving the court's ultimate evaluative function.

Third—Expansion of Compensable Damages: The reform should expressly recognize compensation for the corruption and destruction of non-professional digital data, for psychologically documented harm attributable to artificial intelligence decisions, and for discriminatory harm resulting from algorithmic bias. The recognition of these categories would bring Algerian law into alignment with evolving international standards and would ensure that the most common and serious harms produced by artificial intelligence systems are not excluded from the scope of tortious recovery.

Fourth—Compulsory Insurance and a Guarantee Fund: The complexities of attribution in artificial intelligence damage cases—as Madame G'sell has observed (2020, pp. 28–30)—necessitate the introduction of a compulsory liability insurance regime binding upon operators and developers, complemented by a state-administered guarantee fund covering cases of insolvency and multi-party harm. This approach anchors compensation in the insurability of risk rather than in the futile search for a specifically identified personal fault.

Fifth—Enactment of a Dedicated Artificial Intelligence Statute: The most effective legislative response would be the enactment of a dedicated Algerian statute on artificial intelligence that draws upon the European AI Act's risk-based classification methodology, enshrines the principle of continuous human oversight over automated decisions in sensitive sectors, designates competent regulatory authorities, and

establishes mechanisms for prior technical audit of high-risk systems. Such a statute would provide a coherent and internally consistent normative framework, rather than relying upon the incremental adaptation of civilian liability rules that were not designed with algorithmic agency in mind. Algeria's constitutional commitment to the protection of fundamental rights, elaborated in the 2020 constitutional amendments, provides a normative foundation for such a statute insofar as it reinforces the state's obligation to protect citizens from novel technological harms.

VII. Conclusion

This study demonstrates that artificial intelligence systems have effected a fundamental transformation in the concept of harmful conduct and have exposed the deep structural limitations of classical civil liability theories designed for a tangible, mechanical world. The programmatic autonomy of these systems, their self-learning algorithms, and the black box phenomenon have collectively dismantled the traditional elements of custody and fault, and have rendered the establishment of causal relationships a formidable obstacle that threatens to consign the rights of injured parties to effective nullity.

Against the relative inertia of the Algerian legislative framework, European legislation has demonstrated a promising adaptive capacity through a comprehensive package of laws enacted in 2024. These instruments adopt a flexible strict liability regime that classifies software as a product, facilitates proof through legal presumptions of causation and defect, broadens the range of compensable damages to include digital data and medically documented psychological harm, and distributes accountability across the full spectrum of actors in digital value chains.

The Algerian legislature can no longer postpone a comprehensive and systematic legislative reform that reconstitutes product liability rules to reflect the digital environment, establishes presumptions to facilitate proof, mandates compulsory insurance against artificial intelligence risks, and aspires to the enactment of a dedicated artificial intelligence statute. This statute must balance the encouragement of digital transformation with the protection of citizens' fundamental rights and freedoms.

The delay of this reform does not signify a mere regulatory gap. It signifies a failure to fulfill the foundational human purpose of civil liability law: to make whole those who have been harmed, and to restore the equilibrium of rights that tortious conduct has disturbed. In an era in which decisions affecting employment, creditworthiness, criminal justice, and medical care are increasingly delegated to algorithmic systems, the capacity of the law to provide effective redress for algorithmic harm is not a technical question of secondary importance—it is a matter of fundamental justice.

References

I. Legislative Instruments and Legal Texts

- Algeria, Law No. 75-58 of 26 September 1975, comprising the Civil Code, *Official Gazette*, as amended by Law No. 05-10 of 20 June 2005.
- Algeria, Law No. 09-03 of 25 February 2009 on Consumer Protection and the Suppression of Fraud, *Official Gazette*, No. 15.
- Algeria, Law No. 18-07 of 10 June 2018 on the Protection of Natural Persons in the Processing of Personal Data, *Official Gazette*, No. 34.
- France, *Code civil*, Article 1242, consolidated version of 1 January 2023, Légifrance.
- Council of the European Union. (1985). *Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products*. Official Journal of the European Communities, L 210, 29–33.
- European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1–88.
- European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union, L 2024/1689.
- European Parliament & Council of the European Union. (2024). *Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC*. Official Journal of the European Union, L 2024/2853.

II. Arabic Legal Scholarship

- Belhadj, A. (2010). *Al-Wajīz fī sharḥ al-qānūn al-madani al-jazā'iri: al-naẓariyya al-‘amma lil-iltizām fī al-qānūn al-madani al-jazā'iri* [Concise Commentary on the Algerian Civil Code: The General Theory of Obligations in Algerian Civil Law] (3rd ed.). Office of University Publications.
- Si Youcef, Z. H. (2014). *Al-mas’ūliyya al-madaniyya lil-muntij wifqan lil-qānūn al-jazā'iri wal-muqārin* [Civil Liability of the Producer under Algerian and Comparative Law]. Dar Houma.
- Al-Sanhuri, A. R. (1998). *Al-Wasīṭ fī sharḥ al-qānūn al-madani: naẓariyyat al-iltizām bi-wajh ‘amm, maṣādir al-iltizām* [The Intermediate Commentary on Civil Law: The General Theory of Obligation, Sources of Obligation] (Vol. 1). Halabi Legal Publications.

III. Western Legal Scholarship

- Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks. *ProPublica*. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732. <https://doi.org/10.15779/Z38BG31>
- Borghetti, J.-S. (2019). La responsabilité du fait des produits défectueux à l'épreuve du numérique. *Revue des contrats*, (3), 1–15.
- Calo, R. (2015). Robotics and the lessons of cyberlaw. *California Law Review*, 103(3), 513–563. <https://doi.org/10.15779/Z38BC8>
- Carbonnier, J. (2000). *Droit civil: Les obligations* (Vol. 4, 22nd ed.). Presses Universitaires de France.
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820. <https://doi.org/10.15779/Z38RV0D15>
- Delvaux, M. (2017). *Report with recommendations to the Commission on Civil Law Rules on Robotics* (A8-0005/2017). European Parliament, Committee on Legal Affairs.
- European Agency for Fundamental Rights (FRA). (2020). *Facial recognition technology: Fundamental rights considerations in the context of law enforcement*. Publications Office of the European Union.
- European Commission. (2022). *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)* (COM/2022/496 final). Publications Office of the European Union.
- European Parliament. (2017). European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). *Official Journal of the European Union*, C 252, 239–257.
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
- G'sell, F. (2020). Intelligence artificielle et responsabilité civile: Enjeux et perspectives. *Recueil Dalloz*, (1), 20–32.
- Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Edward Elgar Publishing.
- Jourdain, P. (2003). *Les principes de la responsabilité civile* (6th ed.). Dalloz.
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. <https://doi.org/10.1177/2053951716679679>
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Vladeck, D. C. (2014). Machines without principals: Liability rules and artificial intelligence. *Washington Law Review*, 89(1), 117–150.

IV. Algerian Legal Periodical Literature

- Ben Awda, M. (2021). Khuṣūṣiyyat al-mas'ūliyya al-madaniyya 'an aḍrār anzimat al-dhakā' al-ṣīnā'ī fī al-qānūn al-jazā'irī [The particularities of civil liability for



damages of artificial intelligence systems under Algerian law]. *Majallat al-Ḥuqūq wal-‘Ulūm al-Siyāsiyya*, University of Abbès Laghrour Khenchela, 8(2), 112–130.

Lareid, M. A., & Hammadi, Z. (2022). Niẓām al-mas’ūliyya al-madaniyya ‘an aḍrār al-dhakā’ al-ṣīnā’ī fī al-qānūn al-jazā’irī [The civil liability regime for artificial intelligence damages under Algerian law]. *Majallat al-Ḥuqūq*, University of Abderrahmane Mira Bejaia, 15(1), 45–68.

V. Judicial Decisions

Supreme Court of Algeria, Civil Chamber, Decision No. 171942, 15 December 1999.

Cour de cassation française, Chambre civile 2, arrêt n° 72-12.764 du 15 juin 1972 (Dalloz 1973, p. 285, note Larroumet).

Cour de cassation française, Chambre civile 1, arrêt n° 97-20.429 du 3 mars 1998 (Bull. civ. I, n° 95, p. 64).