Science, Education and Innovations in the Context of Modern Problems

Issue 2, Vol. 9, 2026

RESEARCH ARTICLE

The legal and religious basis for liability for errors resulting from the use of artificial intelligence

Ghribi Ali
Dr.
Research Center for Islamic Sciences and Civilization
Algeria
Email: a.ghribi@crsic.dz

Belhattab Benharzallah
Dr.
Amar Thelidji University of Laghouat-
Algeria
Email: b.belhattab@lagh-univ.dz

=Issue web link https://imcra-az.org/archive/392-science-education-and-innovations-in-the-context-of-modern-problems-issue-2-vol-9-2026.html

Keywords Liability, Islamic Jurisprudence, Positive Law, Artificial Intelligence

Abstract

Artificial intelligence (AI) has become a pivotal force in many vital sectors, such as education, healthcare, transportation, finance, and internet services. With the increasing prevalence of intelligent systems, numerous legal issues arise, particularly concerning liability, especially when these systems cause errors leading to significant harm. For example, when self-driving cars cause accidents, or intelligent healthcare systems misdiagnose illnesses, determining legal and Sharia-compliant liability for the resulting damages becomes challenging.

The central question of this research paper is: How can legal systems adequately address liability for errors resulting from the use of artificial intelligence? This paper primarily aims to analyze the characteristics of AI that complicate the issue of determining legal liability by examining existing legal theories and applying them to errors resulting from AI. Finally, it offers recommendations for developing legal systems to meet the challenges posed by AI.

Citation

Ghribi Al., Belhattab B. (2026). The legal and religious basis for liability for errors resulting from the use of artificial intelligence. *Science, Education and Innovations in the Context of Modern Problems*, 9(2), 1-11. https://doi.org/10.56334/sei/9.2.9

Received: 22.05.2025 | Accepted: 02.12.2025 | Published: 29.01.2026 (available online)

Introduction

The contemporary world is experiencing an unprecedented technological transformation driven by rapid advances in artificial intelligence (AI), which has become deeply embedded in everyday life across critical sectors such as healthcare, transportation, finance, education, and digital services. While these developments promise efficiency, innovation, and improved quality of life, they simultaneously raise complex legal, jurisprudential, and ethical challenges—most notably the question of liability for errors and damages resulting from the use of AI systems.

The significance of this issue stems from the distinctive nature of artificial intelligence, particularly its capacity for autonomous or semi-autonomous decision-making. This characteristic complicates the traditional attribution of responsibility and raises fundamental questions regarding liability: Should responsibility rest with the programmer, the system developer, the manufacturer, the operator, the user, or a combination of these actors? The problem is further exacerbated by the absence of comprehensive and explicit legal frameworks regulating AI-related liability, especially within Islamic jurisprudence, which necessitates innovative and principled approaches capable of ensuring justice, accountability, and the protection of individual rights (Hodge et al., 2018; OECD, 2019).

From this perspective, the present study seeks to examine the possibility of establishing liability for errors arising from the use of artificial intelligence through both Islamic jurisprudence (fiqh) and positive law. The research adopts an analytical and comparative approach, relying on the interpretation of Sharia texts, jurisprudential maxims, and legal doctrines, while also proposing practical mechanisms for their application in the AI context.

The importance of this topic can be summarized as follows:

1. Novelty of the subject: Liability for AI-generated errors remains an emerging field that has received limited scholarly attention, particularly within Islamic jurisprudence.
2. Expanding influence of artificial intelligence: The growing reliance on AI across societal domains necessitates the formulation of clear legal and ethical governance mechanisms.
3. Development of a legal and ethical framework: The study contributes to building an integrated framework that harmonizes legal responsibility with ethical accountability.
4. Enrichment of Islamic jurisprudence: The research advances contemporary Islamic jurisprudential discourse by offering a principled response to modern technological challenges grounded in the objectives of Sharia (maqāṣid al-sharīʿa).

Research Problem

The central research question guiding this study is as follows:

How can a coherent legal and Sharia-compliant foundation be established to determine liability for errors resulting from the use of artificial intelligence?

This question is of critical importance given the accelerating pace of AI development and its increasing capacity to generate significant legal, financial, and moral consequences.

Research Methodology

This research employs a comparative analytical methodology, which includes:

- Analyzing relevant Sharia texts and established jurisprudential principles related to liability and responsibility
- Examining civil and criminal liability rules in contemporary legal systems
- Comparing Islamic jurisprudence with positive law in addressing AI-related errors
- Reviewing the opinions of jurists and legal scholars concerning responsibility and accountability

Through this approach, the study aims to present an integrated vision of AI liability that bridges Islamic legal theory and modern legal frameworks, while offering practical proposals to support the development of a comprehensive ethical and legal governance system for artificial intelligence.

First Axis: Determining Liability in the Context of Artificial Intelligence in Islamic Jurisprudence

The modern technological revolution, led by artificial intelligence, has introduced transformative opportunities alongside profound legal and ethical challenges. Among the most pressing of these challenges is the determination of liability for damages caused by AI systems, particularly given their ability to act autonomously and generate outcomes that may not be directly foreseeable by human actors.

Artificial intelligence systems operate through complex algorithms and adaptive learning mechanisms that enable them to make independent decisions. This raises serious questions regarding the attribution of responsibility: whether liability should be assigned to developers, programmers, manufacturers, operators, or users. The lack of explicit legal regulations governing such scenarios further complicates this issue and underscores the need for principled solutions grounded in established normative systems (World Bank, 2020).

In this context, Islamic jurisprudence emerges as a rich and flexible normative framework capable of addressing novel challenges. Rooted in the principles of justice, equity, and public welfare, Islamic jurisprudence provides comprehensive rules for accountability and harm prevention, making it particularly relevant to contemporary technological dilemmas. The objectives of Sharia emphasize the protection of life, property, intellect, and dignity, all of which may be affected by AI-related errors (Al-Shatibi, 2003).

Islamic jurisprudence adopts an inclusive concept of responsibility that encompasses both moral accountability and legal liability, allowing it to be applied to the determination of responsibility in the development, deployment, and use of artificial intelligence technologies.

Criteria for Determining Responsibility in Islamic Jurisprudence

Islamic jurisprudence offers several foundational principles that can be employed to determine liability for AI-related errors:

1. Rules of Harm and Compensation (Ḍarar wa Ḍamān). Islamic law establishes detailed rules for addressing harm and ensuring compensation. These rules can be directly applied to damages caused by artificial intelligence systems, provided that harm and causation are established (Al-Zarqa, 1998).
2. Principle of Shared Benefit and Risk (Al-Ghunm bi-l-Ghurm). When AI systems generate economic or social benefits, those who benefit must also bear the associated risks and liabilities, particularly when harm arises from foreseeable uses.

3. Principle of Eliminating Harm (Darʾ al-Mafāsid). Islamic jurisprudence prioritizes harm prevention. Where harm occurs, it must be removed or mitigated, and affected parties must be compensated. This aligns closely with tort liability principles based on fault, damage, and causation.
4. Concept of Causation (Al-Tasabbub). Liability in Islamic jurisprudence extends beyond direct action to include indirect causation. This principle is particularly relevant in AI contexts, as developers or operators may be held liable when their actions or omissions contribute causally to harm.
5. Principle of Necessity (Al-Ḍarūra Tubīḥ al-Maḥẓūrāt). While necessity may justify the use of AI in exceptional circumstances, it does not negate responsibility. Rather, it imposes strict conditions, including proportionality, risk assessment, and harm minimization.
6. Public Interest (Al-Maṣlaḥa al-ʿĀmma). The principle of public interest enables the formulation of new legal rules to address emerging technologies, provided that they align with the objectives of Sharia and do not contradict established legal principles.

Through these criteria, Islamic jurisprudence offers a coherent and adaptable framework for assigning liability in the context of artificial intelligence while ensuring justice, accountability, and societal welfare.

Second: Applying Jurisprudential Principles to Cases of Artificial Intelligence Use

1. Artificial Intelligence in Personal Status and Financial Transactions

The majority of contemporary Muslim jurists agree on the permissibility of using modern means of communication—whether written, audio, or visual—for concluding marriage contracts, subject to procedural safeguards stipulated by the family law of each country and the fulfillment of essential contractual pillars such as offer, acceptance, witnesses, and consent (Rahmani, 2016; Bouazza, 2018; Kamarodin, 2018). However, the widespread deployment of artificial intelligence technologies necessitates a renewed jurisprudential assessment of this issue.

Artificial intelligence has introduced unprecedented challenges related to authenticity, verification, and attribution, particularly due to the ability of AI to fabricate audio recordings, images, videos, and written documents through deepfake and generative technologies. This development undermines traditional evidentiary confidence and raises serious concerns regarding accountability and proof in matters of personal status. The implications of erroneous or forged marriage contracts are far-reaching, affecting issues such as marital prohibition, alimony, inheritance, lineage, and legal rights arising from marital status.

A similar concern arises with respect to electronic divorce (ṭalāq). While most contemporary scholars recognize the validity of divorce conducted through clear audio or visual communication, disagreement persists regarding divorce effected through writing alone. In the age of artificial intelligence, this debate must be revisited, as AI-enabled forgery and impersonation significantly weaken the reliability of written declarations. Consequently, jurisprudential rulings must now account not only for the form of expression but also for the technological context, reliability of evidence, and the likelihood of manipulation (Dar al-Ifta al-Misriyyah, 2025; IslamWeb Fatwa Center, 2019).

In the field of financial transactions, including electronic commerce and digital contracting, contemporary jurists generally agree on their permissibility, provided that contractual conditions are met. Nevertheless, artificial intelligence introduces new complexities that require renewed ijtihād (juristic reasoning), particularly in relation to documentation, authentication, and liability. This includes employment contracts—referred to in Islamic jurisprudence as *ijārat al-ashkhāṣ* (hiring of persons)—where AI technologies may be used to impersonate real individuals or automate contractual execution.

For example, an individual may unknowingly contract with an AI-generated identity or interact with intelligent robotic systems that autonomously conclude contracts on behalf of companies. Given that such contracts entail financial obligations and legal consequences, determining liability for errors, deception, or unauthorized contracting becomes a critical jurisprudential issue. The application of principles such as causation (al-tasabbub) and liability for harm (ḍamān) is therefore essential in assigning responsibility to developers, operators, or beneficiaries of these systems.

2. Artificial Intelligence and Islamic Criminal Liability (Hudūd and Taʿzīr)

Islamic law aims to realize human welfare in this world and the Hereafter. Classical jurists summarized this objective in the preservation of five essential necessities: religion, life, honor, intellect, and property (*al-ḍarūriyyāt al-khams*). Islamic criminal jurisprudence developed detailed legal mechanisms to safeguard these necessities from violation. With the emergence of advanced communication technologies, contemporary scholars have already addressed certain cybercrimes and their corresponding punishments. However, the advent of artificial intelligence requires a renewed jurisprudential effort proportional to the scale and novelty of these technologies.

a. Preservation of Life (Ḥifẓ al-Nafs)

The protection of human life is a universally recognized objective of Islamic law. Any act that threatens life, directly or indirectly, is strictly prohibited. In the era of artificial intelligence, however, new threats have emerged that challenge traditional notions of control and accountability. Intelligent systems—such as self-driving vehicles, industrial robots, and AI-assisted medical devices—may commit errors that result in injury or death beyond direct human intervention.

For instance, autonomous vehicles have caused fatal traffic accidents, industrial robots have killed workers due to malfunction, and intelligent medical devices have committed surgical errors resulting in patient deaths. These incidents

raise complex jurisprudential questions regarding criminal liability: Who bears responsibility—the manufacturer, programmer, system operator, owner, or user? The issue becomes even more complex in the military domain, where autonomous weapons systems can independently select targets and deploy force without human intervention.

From a Sharia perspective, determining liability for such killings—whether intentional, quasi-intentional, or accidental—requires careful application of principles of causation, negligence, and control. Additional challenges arise regarding the applicability of qiṣāṣ (retaliation) or diyah (blood money) when harm is caused by autonomous systems, particularly when these systems are imported, externally controlled, or involve sensitive data-sharing arrangements that may threaten national security.

b. Preservation of Honor (Ḥifẓ al-ʿIrḍ)

Honor and privacy are among the most protected values in Islamic law. The misuse of artificial intelligence poses serious threats to personal dignity, family privacy, and social reputation. AI technologies enable the creation of fabricated images, videos, and audio recordings that falsely depict individuals engaging in immoral or criminal acts. Such content is often used for defamation, blackmail, and character assassination.

This reality necessitates renewed jurisprudential analysis to address several critical questions:

- Does generating AI-fabricated sexual or immoral content depicting a real individual constitute defamation (*qadhf*) or slander?
- What is the legal responsibility of those who create, disseminate, or promote such content?
- What evidentiary standards should apply to AI-generated materials in criminal cases, particularly defamation cases?

Islamic jurisprudence, which strictly prohibits spying, defamation, and violation of privacy, provides a strong ethical foundation for criminalizing such acts and imposing deterrent punishments under *taʿzīr* (discretionary penalties), adapted to the technological context.

c. Preservation of Property (Ḥifẓ al-Māl)

Property is the lifeblood of society, and Islamic law provides robust protections against its unlawful appropriation, corruption, or destruction. In the age of artificial intelligence, property faces unprecedented threats in both the digital and physical realms.

(i) The Digital Context

Cybersecurity has become a central concern in the digital age. Artificial intelligence enables criminals to conduct sophisticated cyberattacks, including identity theft, financial fraud, hacking, data manipulation, and digital extortion. AI-driven attacks exploit vulnerabilities through machine learning, making detection and prevention increasingly difficult.

From a jurisprudential perspective, several questions arise:

- What is the legal classification of social media accounts, digital wallets, and online platforms in Islamic law?
- Does attacking a personal account differ legally from attacking a commercial or institutional account in terms of liability and punishment?
- How should Islamic law assess varying degrees of harm, such as espionage, data corruption, financial extortion, or complete destruction of digital assets?

(ii) The Physical Context

Artificial intelligence also poses real-world threats to property through autonomous vehicles, robots, and intelligent systems that may damage public or private assets. Additionally, criminals have exploited AI technologies for large-scale financial fraud, particularly targeting banks. Notably, several individuals in Hong Kong were arrested for using AI-generated forged images and documents to fraudulently obtain bank loans under stolen identities (RT Arabic, 2025).

These developments raise critical jurisprudential questions:

- Who bears liability for property damage caused by autonomous systems such as self-driving cars?
- Under what conditions is the owner or operator exempt from liability?
- Can AI-enabled bank fraud be classified as theft from a secure place (*sariqa min ḥirz*) warranting fixed punishment, or does it fall under discretionary penalties?

Third: The Role of Jurisprudential Reasoning (Ijtihād) in Developing Rules Governing Responsibility in Artificial Intelligence Applications

Jurisprudential reasoning (*ijtihād*) constitutes a fundamental human intellectual capacity rooted in understanding meanings, interpreting relationships between concepts and expressions, and deriving legal rulings through recognized methodological frameworks. The process of ijtihād seeks to uncover the intent of the Lawgiver (*maqṣūd al-shārīʿ*), which may differ from purely linguistic or literal usage in legal texts. By contrast, artificial intelligence operates through algorithmic processes that rely on the statistical accumulation of data and pre-programmed linguistic patterns. As such, AI lacks the capacity to comprehend meanings, intentions, or normative values in the human sense and cannot independently perform genuine jurisprudential reasoning.

Accordingly, artificial intelligence should be viewed as a **supportive research tool**, rather than a substitute for human intellectual faculties or jurisprudential discernment. Jurisprudential reasoning remains a structured process governed by adherence to authoritative sources of law and established methodological rules. The qualified jurist (*mujtahid*) ultimately bears responsibility for issuing legal judgments based on this process. Within this framework, artificial intelligence may be employed to develop **expert systems** that assist jurists by facilitating access to sources, organizing data, and generating analytical suggestions consistent with a jurist's adopted methodology of ijtihād, without replacing human judgment (Al-Zarqa, 1998; Al-Shatibi, 2003).

It must be emphasized that ijtihād presupposes mastery of a comprehensive set of foundational sciences that shape the jurist's intellectual competence. These include Arabic linguistic sciences—both lexical and semantic—given that Islamic law is rooted in the Arabic language; the sciences of Hadith and their methodological principles; logic, insofar as it assists in evaluating evidence and constructing valid analogical reasoning; knowledge of Qur'anic verses pertaining to legal rulings and their contexts of revelation; familiarity with narrator criticism and validation (*al-jarḥ wa al-taʿdīl*); awareness of scholarly consensus (*ijmāʿ*); and the possession of sound legal intuition and judgment.

Moreover, the jurist must be capable of classifying, indexing, and verifying legal texts across primary sources such as canonical Hadith collections, Musnads, and encyclopedic jurisprudential works. He must also understand established principles of legal preference (*tarjīḥ*), including the prioritization of abrogating over abrogated texts, specific over general provisions, and restricted over unrestricted rules. These competencies remain inherently human and cannot be replicated by artificial intelligence, although AI-based expert systems can significantly facilitate access to relevant materials and analytical pathways (Kamali, 2008).

In this supportive capacity, intelligent systems may encode the governing rules of jurisprudential sciences and assist researchers in retrieving precise linguistic formulations, identifying relevant evidentiary sources, examining chains of transmission, or applying preference criteria in cases of evidentiary conflict. Such systems may operate according to the jurisprudential methodology of a particular school of law, reflecting the diversity of approaches to ijtihād within Islamic jurisprudence.

Indeed, the nature of ijtihād varies across schools of Islamic law. **Absolute ijtihād** involves the independent development of legal methodologies and rulings, while **restricted ijtihād** operates within the doctrinal framework of a specific school. Intelligent systems can support both forms, provided they are designed with appropriate epistemological boundaries and are informed by the methodological assumptions of the relevant jurisprudential tradition.

From a practical perspective, intelligent systems have considerable potential to support contemporary applications of Islamic jurisprudence, particularly in sectors undergoing rapid technological transformation. In Islamic finance, for example, the expansion of Sharia-compliant banking institutions has created an urgent demand for specialized expertise. Given the complexity of modern financial transactions, globalization, and electronic commerce, expert systems can assist practitioners by preserving accumulated jurisprudential knowledge, facilitating compliance with Sharia principles, and supporting decision-making in the absence of on-site jurists (Ayub, 2017).

Similarly, intelligent systems can be employed in the management of Sharia-compliant funds, including zakat funds, endowments (*awqāf*), funds belonging to minors, and assets of unknown ownership. These resources are often underutilized due to inadequate management structures. The development of expert systems capable of guiding investment decisions in accordance with Sharia principles could significantly enhance their socioeconomic impact.

In the judicial sphere, artificial intelligence may also play a supportive role within Sharia courts. Judicial experience accumulates over time and may diminish with generational transitions. Intelligent systems that store prior judicial decisions and jurisprudential reasoning can assist newly appointed judges by providing access to established precedents and analytical guidance, particularly in jurisdictions where similar cases recur across different countries. Importantly, such systems must remain advisory in nature and cannot replace judicial discretion or authority.

Fourth Axis: Determining Liability for Artificial Intelligence Applications in Light of Positive Law

Determining liability for damages arising from the use of artificial intelligence technologies presents a multifaceted legal challenge encompassing technical complexity, ethical considerations, and evolving legal doctrines. Under positive law, liability may be analyzed through several established frameworks.

First, **product liability principles** may be applied, whereby manufacturers and developers of AI systems are held responsible for damages caused by defects in design, programming, or production (Hodge et al., 2018). Second, **tort liability** may arise when users or operators cause harm through negligence, misuse, or failure to exercise due care in the operation of AI systems.

Third, legal scholars have proposed the application of **strict liability**, under which owners or operators of AI systems may be held liable for damages irrespective of fault. This approach is justified by the inherently risky nature of autonomous systems and their capacity for independent decision-making. However, the adaptive and self-learning characteristics of artificial intelligence may necessitate the development of new liability models that ensure fairness and proportionality (OECD, 2019).

Given the breadth of this subject, the present study focuses on **tort liability arising from the use of artificial intelligence on social media platforms**, particularly in relation to violations of users' right to privacy.

Once a user consents to the collection and processing of personal data, a contractual relationship is established between the user and the social media platform. Generally, the platform bears contractual responsibility for protecting the user's privacy. However, a critical legal question arises: may the user waive contractual liability in favor of invoking tort liability under Article 124 of the Algerian Civil Code?

Article 124 of the Algerian Civil Code provides that any person who commits a harmful act causing damage to another is obliged to provide compensation, regardless of whether a contractual relationship exists between the parties. The obligation not to cause harm constitutes a general legal duty that operates independently of contractual provisions (Algerian Civil Code, art. 124).

In this context, some legal scholars argue that tort liability forms part of public order and therefore cannot be excluded or waived. Any infringement of legally protected interests—such as the right to privacy—constitutes a violation of public order and necessitates judicial intervention to ensure fair compensation. Tort liability thus represents the general rule, while contractual liability is an exception that may be set aside at the discretion of the injured party (Badawi, 2020; Al-Tamimi, 2022).

To strengthen user protection against privacy violations by social media platforms—particularly in light of the evidentiary difficulties associated with proving contractual fault—several scholars advocate allowing users to rely on tort liability provisions. Accordingly, when a platform violates statutory obligations governing data protection and privacy, it bears tortious liability for the resulting harm and must compensate the affected user.

Establishing Tort Liability of Social Media Platforms for Violations of the Right to Privacy

Based on the foregoing analysis, this study examines the constituent elements necessary to establish **tort liability** for social media platforms when they violate users' right to privacy. These elements are addressed in accordance with general principles of civil liability and relevant legislative and jurisprudential developments.

First: The Harmful Act of the Social Media Platform

A review of legislative texts governing civil liability reveals the absence of an explicit statutory definition of a *harmful act* in cases involving digital privacy violations. Accordingly, for the purposes of this study, a harmful act may be defined as **any conduct by a social media platform that infringes upon users' personal data and causes damage to their private life**, thereby triggering civil liability.

1. Forms of Harmful Acts

The forms of harmful conduct committed by social media platforms are diverse and continuously evolving. Although it is impossible to exhaustively enumerate them, the most prevalent forms may be identified as follows:

A. Unlawful Processing of Users' Personal Data

The Algerian legislator, through **Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data**, explicitly prohibits several forms of unlawful data processing. In particular, the law provides that:

- The processing of personal data is prohibited unless the data subject gives **explicit and informed consent**.
- The processing of **sensitive data**—including data revealing racial or ethnic origin, political or philosophical opinions, religious beliefs, trade union membership, or health and genetic data—is strictly prohibited.
- The processing of **children's personal data** is prohibited without the consent of a legal guardian or authorization from a competent judge, who may grant or withdraw such authorization based on the best interests of the child (Law No. 18-07, arts. 8, 12, 18).

These provisions reflect the legislator's awareness of children's limited capacity to understand the risks associated with digital environments and the need for heightened protection of their informational rights. Some platforms have accordingly introduced mechanisms requiring parental email verification and granting guardians the right to access, modify, or delete children's data.

From this perspective, the Algerian legislator has largely succeeded in establishing a general framework for personal data protection, without distinguishing between automated and manual processing. The law applies broadly to all users of the digital space, including social media users. Given that these platforms process vast quantities of personal data on a daily basis and convert such data into economic value through predictive and descriptive analytics, **any processing contrary to statutory provisions constitutes a harmful act giving rise to tort liability** (Badawi, 2020; Al-Tamimi, 2022).

B. Unlawful Commercial Exploitation of Users' Personal Data

Social media platforms typically require users to disclose personal information to access their services. This data is often analyzed and monetized through targeted advertising, profiling, and the creation of databases reflecting users' habits and preferences. In practice, some companies establish ostensibly marketing-oriented websites whose true purpose is the illicit collection and commercial exploitation of personal data.

Judicial practice confirms the illegality of such conduct. Notably, the French Court of Cassation ruled that the sale of professional résumés to advertisers without consent constitutes an unlawful act. Similarly, the French National Commission for Information Technology and Civil Liberties (CNIL) required Facebook to provide complete user profiles and emphasized users' right to be informed about the processing of their private data (CNIL, 2016).

These practices reveal the emergence of a **data-driven economy** in which personal data has become a commodity. Although Algerian law criminalizes the commercial exploitation of personal data, it does not expressly regulate **civil compensation** for resulting harm. This legislative gap strengthens the argument for recognizing tort liability when unlawful data exploitation causes damage to users' privacy.

C. Disregard for the User's Right to Control and Delete Personal Data

While users may disclose personal data to benefit from social media services, such disclosure often results in long-term and uncontrolled circulation of their information across digital platforms. This reality has given rise to the **right to be forgotten**, which requires platforms to delete personal data after a defined retention period.

Major platforms have adopted internal retention policies: Twitter retains data for up to eighteen months; Google provides for deletion within approximately two months; and Facebook commits not to exceed a ninety-day retention period following account deletion. However, these policies remain largely discretionary and inconsistently applied.

Although the Algerian legislator did not explicitly recognize the right to be forgotten, the law implicitly refers to the principle of **data retention limitation**, requiring that personal data be preserved only for the period necessary to achieve the purpose for which it was collected (Law No. 18-07, art. 9(e)). Failure to respect this principle exposes users to risks such as discrimination, defamation, and long-term reputational harm.

Accordingly, social media platforms' failure to provide effective mechanisms for data control and deletion constitutes a harmful act that may engage their tort liability.

Second: The Harm Resulting from Privacy Violations

Harm constitutes the cornerstone of civil liability, in accordance with the principle that **"there is no liability without harm."** In the context of social media platforms, harm arises when users suffer damage as a result of violations of their right to privacy.

Harm may be **material**, such as when a platform unlawfully sells a user's personal profile to commercial entities, resulting in lost profits or financial loss. In such cases, courts assess the extent of damage by evaluating the profits unlawfully generated or the losses incurred (Al-Tamimi, 2022).

More commonly, harm is **moral**, as recognized under **Article 182 bis of the Algerian Civil Code**, which provides compensation for damage to reputation, honor, dignity, rights, or freedoms. Prolonged retention and dissemination of personal data may seriously undermine an individual's digital reputation and psychological well-being.

Legal doctrine generally agrees that **moral harm** is the most prevalent consequence of privacy violations on social media platforms, particularly for ordinary users who do not derive financial benefit from the disclosure of their private lives. Consequently, the absence of explicit legislative provisions regulating civil liability for privacy violations highlights the need for codified rules addressing both material and moral harm (Badawi, 2020).

Third: Establishing the Causal Link Between the Harmful Act and the Harm

The causal link requires a **direct relationship between the harmful act and the damage suffered**. In cases involving social media platforms, the harm must be shown to result directly from the platform's unlawful processing or misuse of personal data. In this context, courts may rely on the principle of liability for things under one's control, whereby the platform bears responsibility for the digital infrastructure and data-processing systems it operates. Where a causal link is established between the platform's conduct and the user's harm, liability arises on the basis of negligence or failure to comply with statutory obligations.

However, establishing causation in digital privacy cases remains particularly complex due to the global nature of the internet, the technical opacity of platform algorithms, and the difficulty of tracing data flows. Jurisprudence has acknowledged the limitations of traditional causation theories in addressing platform liability, as determining the precise origin of harm often requires advanced technical expertise beyond the scope of conventional legal analysis (Fathi, 2023; Cole & Kathleen, 2019).

These challenges underscore the necessity of adapting civil liability doctrines to the realities of artificial intelligence and digital platforms, either through judicial interpretation or legislative reform.

Conclusion

This study demonstrates that establishing a coherent legal and Sharia-compliant basis for liability arising from errors caused by artificial intelligence (AI) constitutes a complex and multidimensional challenge that cannot be addressed through traditional legal frameworks alone. The autonomous, adaptive, and data-driven nature of AI systems requires a rethinking of responsibility, accountability, and compensation mechanisms within both Islamic jurisprudence and positive law. From a Sharia perspective, the study confirms that Islamic jurisprudence possesses sufficient flexibility and normative depth to address emerging technological challenges. By applying the objectives of Islamic law (*maqāṣid al-sharīʿa*) and foundational jurisprudential maxims—such as *"harm must be removed"* (*al-ḍarar yuzāl*) and *"liability corresponds to benefit"* (*al-ghurm bi-l-ghunm*)—liability for AI-related errors can be allocated in a manner that ensures justice, proportionality, and the protection of fundamental human interests. These principles provide a solid ethical and legal basis for addressing harm resulting from artificial intelligence, even in the absence of explicit classical precedents.

From a legal perspective, the study highlights the limitations of existing liability doctrines when confronted with AI systems capable of learning and making decisions independently. This necessitates the development of innovative legal rules that account for the technical characteristics of AI, including shared responsibility among developers, operators, and beneficiaries. Such rules should emphasize clear attribution of liability, minimum standards of safety and reliability, effective data protection safeguards, and accessible mechanisms for compensating harm. Equally important is the

integration of ethical considerations—particularly privacy protection, fairness, transparency, and equality—into the legal regulation of AI.

The study further underscores that effective governance of artificial intelligence cannot be achieved in isolation. **Interdisciplinary cooperation** among jurists, legal scholars, technologists, ethicists, and policymakers is essential for constructing a comprehensive regulatory framework capable of ensuring the safe, responsible, and socially beneficial use of AI technologies.

Key Findings

Based on the foregoing analysis, the study reaches the following conclusions:

- There is an urgent need for a comprehensive legal and ethical framework governing artificial intelligence, incorporating clear rules of liability, transparency and accountability standards, and robust mechanisms for protecting personal data.
- International cooperation is essential to develop harmonized standards governing AI use, thereby preventing legal fragmentation and regulatory conflicts across jurisdictions.
- Continued research and development in ethical AI must be supported to enhance the safety, reliability, and social responsibility of intelligent systems.
- Public awareness and education regarding the risks and benefits of artificial intelligence are critical to enabling informed and responsible use of these technologies.

Recommendations

In light of these findings, the study proposes the following recommendations:

- States should explicitly incorporate rules governing liability for AI-related errors into their civil, commercial, and criminal legislation.
- Independent regulatory and supervisory bodies should be established to monitor AI applications, assess risks and benefits, and provide policy guidance to governments.
- Academic institutions, research centers, and technology companies should develop and adopt binding ethical standards for the responsible design and deployment of artificial intelligence.
- Effective and accessible compensation mechanisms must be established to ensure that individuals harmed by AI systems receive timely and adequate redress.

Ethical Considerations

This study is based exclusively on doctrinal legal analysis, comparative jurisprudence, and the examination of existing legal and Islamic jurisprudential sources. It does not involve human participants, personal data, clinical trials, or experimental procedures. Accordingly, formal ethical approval was not required. The research was conducted in accordance with recognized principles of academic integrity, intellectual honesty, and responsible scholarship, with full respect for legal norms, religious interpretations, and scholarly diversity.

Acknowledgements

The authors express their sincere appreciation to their respective institutions for providing an academic environment conducive to research and scholarly dialogue. They also acknowledge the contributions of scholars in the fields of law, Islamic jurisprudence, and artificial intelligence ethics whose works informed and enriched the theoretical foundations of this study.

Funding

This research did not receive any specific grant from public, commercial, or non-profit funding agencies.

Conflict of Interest

The authors declare that there are no financial, professional, or personal conflicts of interest that could have influenced the research process, analysis, or conclusions presented in this article.

References

1. Bouazza, A. (2018). The electronic marriage contract council. *Academic Journal of Legal and Political Research*, 2(3), 459–473.
2. Dar al-Ifta al-Misriyyah. (2025, March 8). *Divorce by mobile phone message* (Fatwa No. 14255). http://www.daralifta.org
3. IslamWeb Fatwa Center. (2019, April 8). *Does divorce occur via text message?* https://fatwa.islamweb.net
4. Kamarodin, M. A. (2018). Marriage contracts via the internet. *Journal of Sharia and Law*, (7), 227–252.
5. Rahmani, I. (2016). Concluding marriage contracts via modern electronic means. *Al-Shihab Journal*, (4), 81–122.
6. RT Arabic. (2025, March 23). *Hong Kong gang that defrauded banks using deepfakes busted.* https://arabic.rt.com
7. Al-Shatibi, A. I. (2003). *Al-Muwafaqat fi usul al-sharia*. Dar Ibn Affan.
8. Al-Zarqa, M. A. (1998). *Al-madkhal al-fiqhi al-'amm* (Vol. 2). Dar Al-Qalam.
9. Hodge, G. A., Greve, C., & Boardman, A. E. (2018). *International handbook on public–private partnerships*. Edward Elgar.
10. OECD. (2019). *Artificial intelligence and liability*. OECD Publishing.
11. World Bank. (2020). *Legal frameworks for artificial intelligence governance*. World Bank Group.
12. Abdullah, A. K., & Al-Sarrah, H. N. A. (2022). *Criminal protection of the right to digital oblivion: A comparative study* (1st ed.). National Library and Archives.
13. Amdah, A. (2006). *Electronic commerce from the perspective of Islamic jurisprudence* (Master's thesis). University of Batna.
14. Al-Fiqhi, F. M. A. S. (2023). *Processing personal data via websites and the contractual relationship arising therefrom: A comparative study*. Dar Misr for Publishing and Distribution.
15. Al-Hashemi, S. b. I. (2011). *Electronic commerce and its rulings in Islamic jurisprudence* (1st ed.). Dar Kunooz Ishbiliya.
16. Al-Hajjar, W. S. (2017). *The legal system of social media: A comparative legal study on privacy, personal freedom, responsibility, and jurisdiction* (1st ed.). Arab Center for Legal and Judicial Research, League of Arab States.
17. Al-Jundi, H. (1993). *Guarantees of the sanctity of private life in Islam*. Dar Al-Nahda Al-Arabiya.
18. Al-Nimr, R. M. F. (2019). Protecting the privacy of social media users under Bahraini legislation. In *Proceedings of the International Conference on Privacy in the Information Society* (Issue 26, pp. 85–102). Royal University for Women.
19. Al-Rashed, T. J. A. S. (2017). Legal protection of personal data privacy in Qatari and comparative law. *Legal and Judicial Journal*, 38–112.
20. Al-Shibl, A. A. b. I. (2012). *Electronic assault: A jurisprudential study*. Dar Kunooz Ishbiliya.
21. Al-Tamimi, S. I. K. (2022). *Civil liability for violations on social media: A comparative study* (1st ed.). Dar Misr.
22. Badawi, A. T. M. (2020). *The legal regulation of personal data processing: An applied study on visual surveillance recordings*. Dar Al-Nahda Al-Arabiya.
23. Bouazza, A. (2018). The electronic marriage contract council. *Academic Journal of Legal and Political Research*, 2(3), 459–473.
24. Brownlie, I. (1990). *Principles of public international law*. Oxford University Press.
25. Cole, C., & Kathleen, M. (2019). Social media liability exposures. *Journal of Insurance Regulation*, 38(8), 1–25. https://content.naic.org/sites/default/files/jir-za-38-08-el-social-media-liability.pdf
26. Dar al-Ifta al-Misriyyah. (2025, March 8). *Divorce by mobile phone message* (Fatwa No. 14255). http://www.daralifta.org
27. El-Danasouri, E. E. D., & El-Shawarbi, A. H. (2015). *Civil liability in light of jurisprudence and the judiciary* (Pt. 1). University Press.
28. Faleh, H. F. (2017). Compensation for civil liability arising from media damages. *Journal of Legal Sciences*, Special Issue 3(2), 231–258.
29. Hassan, K. H. A. (2020). *The right to privacy of personal data between legal protection and technical challenges: A comparative study*. Arab Book and Studies House.
30. IslamWeb Fatwa Center. (2019, April 8). *Does divorce occur via text message?* https://fatwa.islamweb.net
31. Kazem Al-Tamimi, S. I. (2022). *Civil liability for violations on social media: A comparative study* (1st ed.). Dar Misr.
32. Kamarodin, M. A. (2018). Marriage contracts via the internet. *Journal of Sharia and Law*, (7), 227–252.

33. Morsi, N. M. (2005). *Modern information technologies*. Dar Al-Jami'a Al-Jadida.
34. Rahmani, I. (2016). Concluding marriage contracts via modern electronic means. *Al-Shihab Journal*, (4), 81–122.
35. Saidi, K., & Ben Mahdi, M. (2022). Artificial intelligence as an inevitable trend in cybersecurity protection. *Journal of Human Rights Studies*, 6(1), 23–41.
36. Supreme Council of Islamic Affairs and Endowments (IACAD). (2019, April 8). *Ruling on divorce by writing*. https://services.iacad.gov.ae
37. World News (RT Arabic). (2025, March 23). Hong Kong gang that defrauded banks using deepfakes busted. https://arabic.rt.com
38. Algerian Civil Code. (1975). *Order No. 75-58 of 26 September 1975, as amended (2007)*.
39. Law No. 18-07. (2018). *Law on the protection of natural persons in the processing of personal data*.
40. Al-Shatibi, A. I. (2003). *Al-Muwafaqat fi usul al-sharia*. Dar Ibn Affan.
41. Al-Zarqa, M. A. (1998). *Al-madkhal al-fiqhi al-'amm* (Vol. 2). Dar Al-Qalam.
42. Ayub, M. (2017). *Understanding Islamic finance* (2nd ed.). Wiley.
43. Badawi, A. T. M. (2020). *The legal regulation of personal data processing*. Dar Al-Nahda Al-Arabiya.
44. Hodge, G. A., Greve, C., & Boardman, A. E. (2018). *International handbook on public–private partnerships*. Edward Elgar.
45. OECD. (2019). *Artificial intelligence and liability*. OECD Publishing.
46. Algerian Civil Code. (1975). *Order No. 75-58, as amended*.