



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

Ethical and Legal Frameworks for AI in Muslim Communities: A Technical Survey of Privacy Constraints and Civil Liability Challenges

Mazhar al-Din Nezampour, (Afghanistan)¹, Dr. Seyed Zuhair Al-Mesilini (Tunisia)²

¹Ph.D. Candidate in Private Law, Al-Mustafa International University – Golestan, Iran. Email: 11515534@gmail.com

²Scientific Department of Islamic Theology, Golestan Representative Office, Al-Mustafa International University, Tunisia.

Orcid: <https://orcid.org/0009-0008-1335-7267>, E-mail: zohir_mesilini@miu.ac.ir

Abstract

The rapid advancement of artificial intelligence technologies, while offering transformative benefits across diverse domains, has concurrently generated serious and emerging privacy challenges. These challenges acquire particular salience in Muslim communities, where religious values deeply inform expectations regarding personal dignity, data protection, and moral accountability. These communities face the complex task of reconciling the technical requirements and global governance norms of AI with foundational Islamic precepts—particularly the prohibition of unlawful surveillance, the sanctity of private life, and the ethical duty to prevent harm. The primary research question investigates the distinctive privacy-related challenges arising from AI deployment within this cultural-religious context, and explores the feasibility of designing an accountable framework integrating civil liability and Islamic ethics. Employing a descriptive-analytical methodology with an interdisciplinary approach, the study draws upon primary Islamic sources—including the Qur'an, the Sunnah, and jurisprudential texts—alongside contemporary academic literature on AI governance and algorithmic accountability. Findings reveal that privacy challenges in AI are intrinsically three-dimensional—technical, legal, and socio-cultural—with regulatory gaps significantly exacerbating associated risks. Moreover, established Islamic legal maxims such as *Lā Ḍarar* (no harm), *Ḥurmah al-Tajassus* (prohibition of spying), and *Ḍamān al-Itlāf* (liability for damages) offer substantial normative potential for articulating the civil liability of developers, governments, and end-users. The study ultimately proposes a dual-level framework that concurrently strengthens legal redress mechanisms and establishes independent ethical oversight institutions, thereby laying the groundwork for responsible, value-aligned AI that respects Islamic ethical traditions while addressing contemporary technological imperatives.

Keywords: Artificial Intelligence, Privacy, Islamic Ethics, Civil Liability, Contemporary Jurisprudence, Technology Governance.

Introduction

The contemporary world is witnessing the emergence of the "Fourth Industrial Revolution," at the heart of which lie artificial intelligence and machine learning technologies. These systems, with their capacity for exponential data processing, behavioral prediction, and relative autonomy in decision-making, are fundamentally transforming domains ranging from healthcare and finance to security and governance. However, the driving engine of this transformation is the consumption of vast quantities of personal data, often collected without informed consent, full awareness, or effective user control. This has given rise to the phenomenon of "privacy commodification" and has established "surveillance capitalism" as the dominant economic model of the digital age. In Muslim communities, these developments unfold at a complex intersection. On the one hand, these societies seek to benefit from the developmental and welfare advantages of AI; on the other hand, they remain committed to an Islamic value system that regards privacy (*ḥurmah al-tajassus*) not merely as a contractual right, but as a divine-human entitlement (*ḥaqq Allāh wa ḥaqq al-nās*) rooted in human dignity (*karāmah al-insān*) and divine trusteeship (*istikhlāf*). Modern concepts such as "data ownership," "informed consent," and "algorithmic accountability" require reinterpretation and adaptation within the framework of foundational jurisprudential concepts such as "property" (*māl*), "faith" (*īmān*), "honor" (*ʿird*), "liability" (*ḍamān*), and the preservation of life, intellect, lineage, faith, and property as the objectives of Sharia (*maqāsid al-sharīʿah*). The research problem of the present study is to examine these tensions and to assess the feasibility of offering indigenous solutions. The central research question is: "Given the specific challenges that AI poses to privacy within the cultural-religious context of Muslim communities, how can a comprehensive framework for prevention, regulation, and compensation be designed by drawing

upon the system of civil liability and Islamic ethics?" The primary objective of this article is to provide a systematic interdisciplinary analysis that links three distinct discourses: the technical-legal discourse of AI, the discourse of Islamic jurisprudence and *maqāṣid al-sharī'ah*, and the discourse of applied moral philosophy. The secondary objectives are as follows:

1. To identify and qualitatively categorize privacy challenges arising from AI, with attention to the specific characteristics of Muslim communities.
2. To extract and elucidate the theoretical foundations of privacy and liability from authentic Islamic sources (the Qur'an, Sunnah, reason, and consensus) and applicable jurisprudential rules.
3. To analyze the allocation of civil liability among three key actors (developers, operators, and regulators) in light of rules such as *ḍamān* (liability), *tasbīb* (causation), and *lā ḍarar* (no harm).
4. To design a dual-level governance framework (a legal-hardware level and an ethical-institutional software level) for managing the ethical risks of AI.

The necessity of this research is three-dimensional:

- **Theoretical:** Filling the gap in deep interdisciplinary studies that engage Islamic jurisprudence and ethics in dialogue with the advanced literature on AI ethics. Most existing studies are either overly general or merely translate Western principles without contextual adaptation.
- **Legal-Policy:** Offering practical recommendations for legislators in Islamic countries to formulate comprehensive data protection and AI governance laws that are both technically effective and compliant with Sharia standards.
- **Socio-Cultural:** Contributing to the building of public trust and enhancing digital-ethical literacy in society, so that Muslim citizens neither passively submit to technology nor entirely reject it out of fear.

This research employs a descriptive-analytical method with an interdisciplinary approach. Data collection is library-documentary, and qualitative content analysis of texts has been utilized to extract foundational principles. The theoretical framework is a hybrid model combining the theory of *maqāṣid al-sharī'ah* (al-Ghazālī, al-Shāṭibī) and the information ethics framework (Floridi).

1. AI Challenges to Privacy in Muslim Communities

Privacy in the age of artificial intelligence is no longer merely synonymous with "seclusion in the home," but has instead evolved into the concept of "control over the flow of personal information" and "immunity from unfair judgment and manipulation" (Mittelstadt, Brent et al., "The Ethics of Algorithms: Mapping the Debate," *Big Data & Society*, 2016, p. 5). This conceptual transformation carries specific obstacles and complexities within Muslim communities.

1.1. Technical and Infrastructural Challenges: From Big Data to Smart Cities

Mass Data Collection: Many deep learning algorithms require vast and often sensitive datasets—including biometric images, health records, and financial transactions. In the absence of robust legal frameworks, such data can be collected through seemingly benign applications without the genuine consent of Muslim users. The challenge becomes particularly acute when this data contains information pertaining to religious beliefs, participation in religious ceremonies, or activities related to veiling (*ḥijāb*), which may become accessible to non-Muslim entities or secular governments.

Pervasive Digital Surveillance: Technologies such as facial recognition, intelligent audio monitoring, and geolocation tracking enable unprecedented levels of surveillance. In developing smart cities across the Middle East, these technologies can be deployed for social control purposes—a practice that stands in direct contradiction to the Islamic concept of "security in privacy" (*al-amn fī al-ḥurmah*). Islamic jurisprudence explicitly prohibits entering another's home without permission. Does "digital entry" into individuals' locational and behavioral data without explicit and informed consent constitute a modern manifestation of the same prohibited spying (*tajassus*)? (Muṣṭafavī, Sayyid Muḥammad Kāẓim, *Privacy in Imami Jurisprudence and Iranian Law*, Dādgostar Publishing, 2021, p. 125).

Algorithmic Bias and Systematic Discrimination: Algorithms may amplify existing biases against particular groups—such as ethnic or religious minorities, or women in certain contexts—based on historical data. This can result in their exclusion from financial services (e.g., in AI-driven Islamic banking), employment opportunities, or accuracy in AI-based judicial systems. Such outcomes conflict with the Qur'anic principle of "Be just" (*i'dilū*) and the jurisprudential rule of *naḥy al-sabīl* (the negation of non-believers' dominance over believers).

1.2. Legal and Institutional Challenges: Gaps and Conflicts

Lack of Comprehensive Legal Frameworks: Many Islamic countries lack dedicated, modern "personal data protection" laws comparable to Europe's GDPR. Existing legislation, such as cybercrime laws in some jurisdictions, remains predominantly penal and reactive, lacking preventive mechanisms, transparency provisions, and effective civil redress (Wachter, Sandra & Mittelstadt, Brent, *AI Ethics: A Textbook*, MIT Press, 2021, p. 178).

Ambiguity in Civil Liability: When an AI system deployed on a digital health platform, through misdiagnosis, leads to the disclosure of a user's confidential medical condition, who bears liability for compensation? Is it the algorithm developer, the platform-operating company, or the government regulatory body? Traditional civil liability laws (grounded in the fault of a natural person) prove inadequate in addressing "distributed responsibility" within complex AI systems (ʿĀbidī, M. & Nowrūzī, F., "A Jurisprudential Analysis of Civil Liability Arising from AI Algorithm Errors," *Journal of Islamic Law and Jurisprudence Studies*, 2021, p. 80). AI, by contrast (as discussed in the functionalist and behaviorist account offered by Alawijeh and Al-Mesilini (2025)) simulates or reproduces certain cognitive functions without possessing intentionality or intrinsic semantic experience (Alawijeh, M. 'A., S. Z. Al-Mesilini. 2025).

Conflict Between Data Sovereignty and Transnational Islamic Values: Muslim users' data may be stored on servers of multinational corporations located outside Islamic jurisdiction. This phenomenon raises significant jurisprudential questions regarding the preservation of the sanctity of data concerning Muslim beliefs in non-Muslim hands, and the possibility of Sharia oversight over how such data is utilized.

1.3. Socio-Cultural and Normative Challenges

Lack of Digital-Ethical Literacy: In many Muslim societies, a profound digital divide persists. Users may be unaware of the extent and implications of their data collection, and their "consent" often remains formal and uninformed. This contradicts the Islamic condition of "knowledge and intellect" (*ʿilm wa ʿaql*) for the validity of transactions.

Tension Between Tradition and Modernity: Cultural-religious resistance may arise against certain forms of surveillance or data collection (e.g., the use of cameras in private spaces). Conversely, pressure to modernize may lead to the uncritical adoption of surveillance technologies. Finding a pathway that simultaneously supports digital "enjoining good and forbidding evil" (*al-amr bil-maʿrūf wal-nahy ʿan al-munkar*) while respecting "personal privacy" demands considerable jurisprudential nuance.

The Trust Deficit: Historical distrust of governmental institutions or foreign corporations can impede the adoption of AI-based systems, even when technically beneficial. Building trust requires radical transparency and robust ethical guarantees.

2. Jurisprudential and Ethical Foundations for Privacy and Liability in the Digital Age

Islam possesses the capacity to address these challenges not only by offering general principles but by providing a coherent legal-ethical system. This system rests upon several pillars:

2.1. The Concept of Privacy (al-ḥurmah al-khāṣṣah) in Islamic Texts

The Holy Qurʾān: Numerous verses explicitly emphasize privacy. Verse 12 of Sūrat al-Ḥujurāt—"O you who have believed, avoid much assumption; indeed, some assumption is sin. And do not spy (*lā tajassasū*)..."—not only prohibits spying but situates it in the context of negative suspicion, subtly indicating the cognitive roots of privacy violation. Verses 27-28 of Sūrat al-Nūr, concerning seeking permission before entering homes, delineate physical privacy as a concrete example of a broader privacy framework.

Prophetic Sunnah: Numerous authentic ḥadīth affirm the inviolability of the home's privacy, including the following: "Verily, the home of a person has sanctity" (*inna li-bayt al-rajul ḥurmah*) (narrated by Saḥīḥ Muslim, Book of Etiquette, Chapter on the Prohibition of Looking into Another's Home, Ḥadīth No. 2156). Another well-known ḥadīth similarly emphasizes this principle, narrated by Abū Hurayrah (may Allah be pleased with him), that the Prophet (peace be upon him) said: "Whoever looks into the home of a people without their permission has made it lawful for them to put out his eye" (narrated by Saḥīḥ al-Bukhārī, Book of Seeking Permission, Chapter on the One Who Looks into the Home of a People, Ḥadīth No. 6902). While the wording appears severe, it demonstrates the gravity with which this right is regarded in the Islamic worldview. These rulings can be extended to "digital space" as an extension of personal privacy.

2.1. Maqāṣid al-Sharīʿah (Objectives of Sharia)

The preservation of *ʿird* (honor, reputation) and *māl* (property) is recognized as one of the five essential necessities (*ḍarūriyyāt*) of Islamic law. In the digital age, "personal data" and "digital reputation" constitute salient manifestations of *ʿird* and *māl*. Accordingly, their protection is not a secondary matter but a religious obligation (*wājib sharʿī*) (Bakar, M. A., & Zeki, A. M., "Islamic Perspective on Data Privacy: An Analysis of Maqasid al-Shariah," *International Journal of Islamic Thought*, 2020, p. 50).

2.2. Key Jurisprudential Rules for Determining Liability

The Rule of Lā Ḍarar wa Lā Ḍirār (No Harm and No Reciprocating Harm): This foundational rule prohibits any harmful act—whether material or immaterial. The deployment of a system that infringes upon individuals' privacy constitutes a clear instance of "harm" (*ḍarar*). Pursuant to this rule, *al-ḍararu yuzāl* (harm must be eliminated)—whether through system cessation or through compensation for damages.

The Rule of Ḍamān (Liability): This general rule constitutes the foundation of civil liability in Islamic jurisprudence. Relevant applications include:

- **Ḍamān al-Itlāf (Liability for Loss/Destruction):** *Man atlaḡa māla ḡhayrihi faḡhuwa ḡḡāmin* (Whoever destroys the property of another is liable). If an AI system leads to the disclosure, corruption, or unlawful manipulation of personal data—which is considered "property" (*māl*)—the responsible party is obligated to compensate.

- **Ḍamān al-Yad (Liability of Possession/Control):** *‘Alā al-yadi mā akḡadḡat ḡattā tu‘addiyahu* (The hand is responsible for what it has taken until it returns it). Any party (or institution) that exercises control over users' data—whether as a trustee or otherwise—is liable for its preservation and integrity.

- **Ḍamān al-Tasbīb (Liability for Causation):** *Kullu mā aṡāba al-muslima faḡhuwa ‘alā al-fā‘ili in kāna muta‘ammidan wa ‘alā al-musabbibi in kāna ḡhayra muta‘ammid* (Whatever befalls a Muslim is upon the direct doer if intentional, and upon the one who caused it if unintentional). If a developer or operator creates the conditions for harm (i.e., privacy violation) to occur, even without direct intent, they are liable.

The Rule of Aṡālat al-ṡiḡḡah and Isālat al-Dḡimmah (Presumption of Validity and Presumption of Innocence): The default principle is the exculpation of individuals from obligation and the validity of their actions. This rule does not place the burden of proof upon the claimant (the user). Rather, given technical complexity, it can be interpreted as shifting the burden of proof—concerning safety and privacy compliance—onto the AI system provider (the principle of precaution / *al-iḡṡiyāt*).

2.3. Islamic Ethical Principles Governing Technology: From Theory to Practice

Beyond legal rules, Islam offers a rich ethical framework capable of shaping the culture of AI development and deployment:

The Principle of Trusteeship (al-Istikḡlāf): Humanity is God's vicegerent (*kḡalīfat Allāḡ*) on earth, and all resources—including data and technology—are a trust (*amānah*) in human hands. This perspective rejects exploitative approaches to user data (Ramadan, Tariq, *The Quest for Meaning*, Penguin, 2017, p. 156).

The Principle of Intention (al-Niyyah): Technology must be employed in the service of public welfare (*maṡlaḡah ‘āmmah*) and proximity to God, not for domination, exploitation, or the propagation of corruption (*fasād*).

The Principle of Transparency and Prohibition of Deception (al-Naḡy ‘an al-ḡḡishsh): Concealment regarding algorithmic functioning and data usage constitutes deception (*ḡḡishsh*) and fraud (*kḡidā*). Transparency (*al-shaḡāfiyyah*) is an ethical virtue and a condition for the validity of a transaction—in this context, the data transaction.

The Principle of Justice (al-‘Adālah): AI systems must be just and must not engender unjust discrimination. This justice must be observed both in outcomes and in the processes of model design and training (Larijani, L. C. & Rezaei, M., "A Framework for Ethical AI Based on Islamic Principles," *AI & Ethics*, 2022, p. 350).

3. Analysis of Civil Liability and a Proposed Islamic Governance Framework

3.1. Distribution of Civil Liability Based on Jurisprudential Rules

By applying the rules outlined in the preceding section, a liability matrix can be designed as follows:

Actor	Basis/Jurisprudential Rule	Nature of Liability	Concrete Example
Developer / Researcher	<i>Ḍamān al-Tasbīb</i> (liability for causation) and <i>Ḍamān al-‘Ayb</i> (liability for defect)	Liability for defects in design, use of incorrect or illegitimate data for training, and failure to provide adequate warnings regarding system limitations. If the algorithm is inherently discriminatory or privacy-invasive, the developer, as the primary cause (<i>musabbib</i>), bears liability.	Design of a facial recognition algorithm that, due to a biased training dataset, systematically fails to accurately identify veiled women (<i>ḡijāb-wearing women</i>).
Operator (Company / Government)	<i>Ḍamān al-Yad</i> (liability of possession/control) and the Rule of <i>Lā Ḍarar</i> (no harm)	Liability as the owner/possessor (<i>mutasarrif</i>) of the system. Obligated to conduct continuous	A smart transportation company that uses passengers'

		monitoring, implement updates to remedy harms, obtain informed consent, ensure transparent disclosure, and provide compensation in the event of an incident. Ultimate liability rests with the operator.	geolocation data for secondary purposes, leading to the disclosure of an individual's private schedule.
Government Regulatory Body	<i>Hifẓ al-Niẓām</i> (preservation of public order) as a governmental obligation, and <i>al-Amr bil-Ma'rūf wal-Nahy 'an al-Munkar</i> (enjoining good and forbidding evil)	Responsibility for regulation, oversight, and judicial action. Duty-bound to enact transparent laws, issue operating licenses, investigate violations, and impose discretionary punishments (<i>ta'zīr</i>) on offenders. Responsible for the protection of public interest (<i>maṣlaḥah 'āmmah</i>).	Failure to enact a comprehensive data protection law, or failure to take enforcement action against a company that repeatedly suffers data breaches.

3.2. The Proposed Dual-Level Governance Framework

Building upon the liability matrix and the ethical-jurisprudential foundations established earlier, this study proposes a dual-level governance framework for managing the ethical and privacy risks of AI in Muslim societies:

Level One: The Legal-Hardware Level (Enforceable Legal Mechanisms)

This level comprises binding legal instruments and institutional structures designed to establish clear rules, allocate responsibilities, and provide remedies:

- 1. Comprehensive Data Protection Legislation:** Enactment of national laws specifically addressing personal data protection in AI contexts, drawing inspiration from international frameworks (e.g., GDPR) while remaining fully compliant with Sharia principles. Such laws should explicitly recognize personal data as a form of *māl* (property) and digital reputation as a form of *irḍ* (honor), thereby triggering the full protective apparatus of Islamic law.
- 2. AI Licensing and Registration Regime:** Mandatory registration and licensing of high-risk AI systems (particularly those involving biometric identification, health diagnostics, and predictive policing) with a designated national authority. Licensing should require algorithmic impact assessments, privacy audits, and demonstration of Sharia compliance.
- 3. Clear Liability Allocation Rules:** Statutory codification of the liability matrix outlined above, specifying the respective responsibilities of developers, operators, and regulators. This should include:
 - Presumption of operator liability in case of harm.
 - Joint and several liability provisions where both developer and operator are at fault.
 - Explicit recognition of *tasbīb* (causation) as a basis for developer liability.
- 4. Effective Redress and Compensation Mechanisms:** Establishment of accessible dispute resolution mechanisms, including specialized AI ethics tribunals. Compensation should cover both material and immaterial harm (e.g., reputational damage, emotional distress), consistent with the rule *al-ḍararu yuzāl* (harm must be eliminated).
- 5. Data Sovereignty and Cross-Border Transfer Rules:** Regulations ensuring that data pertaining to Muslim citizens, particularly sensitive data concerning religious beliefs and practices, is stored and processed under Islamic jurisdiction. Transfers to non-Islamic jurisdictions should be strictly conditioned on adequate protection standards.

Level Two: The Ethical-Institutional Software Level (Normative and Institutional Oversight)

This level comprises non-binding but normatively powerful institutions and practices designed to embed Islamic ethical values into the AI ecosystem:

- 1. National AI Ethics Council:** Establishment of an independent council composed of scholars of Islamic jurisprudence (*fuqahā'*), AI engineers, legal experts, and civil society representatives. The Council's functions should include:
 - Issuing *fatwās* and ethical guidelines on emerging AI applications.
 - Reviewing and certifying AI systems as Sharia-compliant.

- Advising the government on AI policy and legislation.
- Raising public awareness and digital-ethical literacy.
- 2. **Corporate Ethics and Compliance Programs:** Mandating that AI-operating companies establish internal ethics committees and compliance units responsible for:
 - Conducting regular privacy and ethics audits.
 - Implementing privacy-by-design principles.
 - Ensuring algorithmic transparency and explainability.
 - Providing clear, accessible information to users about data practices.
- 3. **Public Awareness and Education:** Development of national educational programs to enhance digital-ethical literacy among citizens. Such programs should explain both the technical realities of AI and the Islamic ethical principles governing data privacy and accountability, enabling Muslim users to make informed choices.
- 4. **Independent Ethical Certification and Auditing:** Creation of a voluntary or mandatory certification system for AI systems that comply with Islamic ethical standards. Independent third-party auditors should assess algorithmic fairness, privacy protection, and transparency.
- 5. **Community Engagement and Participatory Governance:** Establishment of mechanisms for public consultation and stakeholder engagement, ensuring that affected communities have a voice in AI governance decisions. This aligns with the Islamic principle of *shūrā* (consultation).

3.3. Integrative Summary: The Interplay of Law and Ethics

The proposed framework operates on the premise that **law and ethics are not substitutes but complements**. The legal-hardware level provides the enforceable backbone—clear rules, binding obligations, and remedies for violations. The ethical-software level provides the normative soul—cultivating a culture of responsibility, trust, and moral self-regulation. In Islamic tradition, this duality resonates with the distinction between *fiqh* (jurisprudence) and *taqwā* (God-consciousness). While *fiqh* provides the external rules that govern conduct, *taqwā* cultivates the internal moral compass that motivates compliance beyond fear of punishment.

For Muslim societies, this integrated approach offers a pathway to AI governance that is simultaneously:

- **Legally robust:** Through binding laws, clear liability, and effective remedies.
- **Ethically grounded:** Through deep engagement with Islamic moral traditions.
- **Culturally authentic:** Through indigenous frameworks rather than uncritical imports.
- **Technically viable:** Through alignment with international best practices while adapting to local values.

3.2. Dual-Level Governance Framework: Integrating Legal Enforcement and Ethical Institutions

To operationalize the aforementioned foundations, a hybrid framework is proposed that leverages both external incentives (law and sanctions) and internal motivations (ethics and peer oversight).

Level One: Legal-Judicial Framework (The Governance Hardware)

Enactment of a Comprehensive "Personal Data Protection and AI Ethics Law": This law should be grounded in *maqāṣid al-sharī'ah* and include the following provisions:

1. A clear definition of "personal data" and "sensitive data" (including religious and biometric data).
2. A requirement for "explicit, informed, and specific consent" for data collection and processing.
3. Granting users the rights of access, rectification, erasure (the "right to be forgotten"), and data portability.
4. Mandating explainability and transparency for high-risk AI systems.
5. Establishing joint and multi-layered liability (Developer, Deployer) with ultimate liability resting with the operator.
6. Provision of mechanisms for swift, effective, and fair compensation, including compensation for non-material damage.
7. Establishment of a "National Data Protection Authority" with strong supervisory and discretionary punitive (*ta'zīrī*) powers.

Level Two: Ethical Oversight Institutions (The Governance Software)

Establishment of "Supreme Councils for AI Ethics and Emerging Technologies": These councils, at the national or regional level, will be supra-governmental, independent, and interdisciplinary bodies.

Composition of Members: Jurists (*fuqahā'*) well-versed in contemporary issues (*masā'il mustaḥdathah*), AI and cybersecurity specialists, legal experts, moral philosophers, and civil society representatives.

Key Functions:

1. **Pre-Market Ethical Impact Assessment:** Evaluating high-risk AI systems (in judicial, health, and security domains) for compliance with Islamic principles and issuing "Sharia and Ethical Compliance Certificates."
2. **Drafting and Publishing Specialized Ethical Charters:** For various sectors (e.g., AI in Islamic banking, education, etc.).

3. **Adjudicating Ethical Complaints:** Establishing rapid, non-judicial proceedings for resolving disputes related to ethical violations.

4. **Cultural Development and Education:** Enhancing digital-ethical literacy in society and among developers. *Jurisprudential Basis:* This institution can be justified based on the institution of *ḥisbah* in Islamic civilization, which was entrusted with enjoining good and forbidding evil in public affairs and supervising trades and professions. Additionally, the theory of *wilāyat al-faqīh* (within the Shiite jurisprudential framework) or *wilāyat al-amr* (within Sunni jurisprudence) can be utilized to legitimize governmental oversight over critical public matters such as vital technologies (Khamene'i, Seyyed Ali, *Jurisprudence and Governance in the Age of Information Technology*, Research Institute for Islamic Culture and Thought, 2019, p. 234). This body would serve as the specialized arm of the *walī al-amr* (the guardian/authority) in this domain.

Conclusion

This study has demonstrated that the privacy challenge in the age of artificial intelligence for Muslim communities constitutes a complex polygon comprising technical, legal, and cultural-religious dimensions. Effective engagement with this challenge is neither possible through the outright rejection of technology nor through uncritical submission to Western models; rather, it is attainable through a creative and context-sensitive reinterpretation of Islamic sources. Jurisprudential rules such as *lā ḍarar* (no harm), *ḍamān* (liability), and *tasbīb* (causation) possess considerable capacity for establishing an efficient and equitable civil liability system in the digital space. However, law alone is insufficient. Islamic ethics—with its emphasis on trusteeship (*amānah*), justice (*ʿadālah*), transparency (*shafāfiyyah*), and good intention (*niyyah*)—must constitute the animating spirit governing the entire AI lifecycle.

The proposed dual-level governance framework—combining robust law with dynamic ethical institutions—can offer an indigenous model that simultaneously defends individual rights, encourages responsible innovation, and secures public trust. This framework views AI as a "means" that must be employed in pursuit of the *maqāṣid al-sharīʿah* (the preservation of religion, life, intellect, lineage, and property).

Research Limitations

1. Due to its theoretical-analytical nature, this study has not relied upon field research or surveys of elites or users in specific countries.
2. The diversity of Islamic schools of thought and jurisprudential interpretations may give rise to differing opinions regarding the application of specific rules (e.g., the extent of government liability), necessitating separate comparative studies.
3. The exceptionally rapid pace of technological evolution may render some concrete examples obsolete in the medium term.

Recommendations for Future Research and Practical Action

Future Research:

1. Conducting in-depth case studies in specific domains, such as civil liability in Islamic financial platforms (FinTech) or the ethics of facial recognition deployment in sacred places.
2. Comparative research on AI governance frameworks across different Islamic countries (e.g., UAE, Malaysia, Iran, Saudi Arabia).
3. Exploring the feasibility of drafting an "International Islamic AI Ethics Document" with the participation of scientific-religious institutions from across the Muslim world.
4. Studying jurisprudential approaches to the intellectual property of data and AI-generated outputs.

Immediate Practical Actions:

1. **For Governmental Bodies:** Initiating the process of drafting a comprehensive data protection law by forming a committee comprising jurists (*fuqahāʾ*), legal experts, and technology specialists.
2. **For Academic and Religious Institutions:** Incorporating courses entitled "Jurisprudence of Data" (*Fiqh al-Muṭayyāt*) or "Technology Ethics" into advanced jurisprudential seminars (*durus al-khārij*) and relevant university curricula.
3. **For Technology Companies:** Establishing internal ethics committees and conducting "Sharia Impact Assessments" on new products.
4. **For Civil Society and Media:** Launching awareness campaigns regarding digital rights in light of Islamic teachings.

Ultimately, the proper engagement with artificial intelligence requires a collective, courageous, and forward-looking *ijtihād* (independent legal reasoning) capable of bridging the timeless wisdom of religion with the

changing realities of the world. This path, though challenging, is an inescapable necessity for preserving identity, justice, and human dignity in Muslim societies in the digital age.

References

The Holy Qur'an

1. 'Ābidī, M., & Nowrūzī, F. (2021). "A Jurisprudential Analysis of Civil Liability Arising from AI Algorithm Errors." *Quarterly Journal of Islamic Law and Jurisprudence Studies*, 13(28), 75-102. [In Persian].
2. Al-Atawneh, M. (2020). *Islamic Law and the Challenges of Modernity*. Abingdon: Routledge.
3. Alawijeh, M. 'A., S. Z. Al-Mesilini. 2025. "A Comparative Study of Artificial and Natural Intelligence from Ibn Sina's Perspective". *Journal of Ecohumanism*, Vol. 4, No. 1, 2879. Available at: <https://doi.org/10.62754/joe.v4i1.6082>.
4. Al-Bukhārī, Muḥammad ibn Ismā'īl. (n.d.). *Al-Jāmi' al-Ṣaḥīḥ* (Vol. 8). Beirut: Dār Ṭawq al-Najāh. [1422 AH].
5. Bakar, M. A., & Zeki, A. M. (2020). "Islamic Perspective on Data Privacy: An Analysis of Maqasid al-Shariah." *International Journal of Islamic Thought*, 17(1), 45-58.
6. Bakar, O. (2017). *The History and Philosophy of Islamic Science*. Cambridge: Islamic Texts Society.
7. Bujnūrdī, S. M. ibn Ḥ. Mūsavī. (2022). *Jurisprudential Rules* (Vol. 2). Tehran: 'Urūj Institute. [In Persian].
8. Floridi, L. (2013). *The Ethics of Information*. Oxford: Oxford University Press.
9. Jobin, A., Ienca, M., & Vayena, E. (2019). "The Global Landscape of AI Ethics Guidelines." *Nature Machine Intelligence*, 1(9), 389-399.
10. Khamene'i, S. A. (2019). *Jurisprudence and Governance in the Age of Information Technology*. Tehran: Research Institute for Islamic Culture and Thought. [In Persian].
11. Larijani, L. C., & Rezaei, M. (2022). "A Framework for Ethical AI Based on Islamic Principles: Justice, Trusteeship, and Benevolence." *AI & Ethics*, 2(3), 345-360.
12. Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). "The Ethics of Algorithms: Mapping the Debate." *Big Data & Society*, 3(2), 1-21.
13. Mohamed, M., et al. (2021). "Artificial Intelligence, Ethics, and the Islamic Moral Economy: A Framework for Evaluation." *Journal of Islamic Accounting and Business Research*, 12(5), 631-648.
14. Muslim ibn al-Ḥajjāj al-Naysābūrī. (n.d.). *Al-Jāmi' al-Ṣaḥīḥ* (Vol. 3). Beirut: Dār Iḥyā' al-Turāth al-'Arabī. [n.d.].
15. Muṣṭafavī, S. M. K. (2021). *Privacy in Imami Jurisprudence and Iranian Law*. Tehran: Dādgostar Publishing. [In Persian].
16. Raḥmatullāhī, Ḥ. (2020). "Information Privacy in the Age of Big Data from the Perspective of Jurisprudence and Law." *Journal of Justice Legal Studies*, 84(105), 153-180. [In Persian].
17. Ramadan, T. (2017). *The Quest for Meaning: Developing a Philosophy of Pluralism*. London: Penguin Books.
18. Wachter, S., & Mittelstadt, B. (2021). *AI Ethics: A Textbook*. Cambridge: MIT Press.