International Journal of Islamic Theology & Civilization
E-ISSN (3009-1551)

ORIGINAL ARTICLE Open Access

AI SURVEILLANCE, PRIVACY (ḤIFẒ AL-ʿIRḌ), AND HUMAN DIGNITY IN ISLAMIC JURISPRUDENCE

[1]Ramlan Mustapha & Siti Norma Aisyah Malkan@Molkan

Academy of Contemporary Islamic Studies, Universiti Teknologi MARA Pahang, Raub Campus, Malaysia
[1]ramlan@uitm.edu.my, [2] siti_norma@uitm.edu.my

*Corresponding Author: Ramlan Mustapha (Mujahidpahang@gmail.com)

Received 24 Oct 2025; Revised 14 Dec 2025; Accepted 20 Jan 2026; Published 1 Feb 2026

Vol: 4, Issue 1 (2026)

Doi: 10.5281/zenodo.18295050

Keyword:

AI surveillance, privacy, Ḥifẓ al-ʿIrḍ, human dignity, Islamic jurisprudence, Maqasid al-Shariah, digital ethics, algorithmic accountability, Islamic law, technology ethics

Abstract

The rapid proliferation of artificial intelligence (AI) surveillance technologies presents unprecedented challenges to privacy and human dignity, necessitating examination through the lens of Islamic jurisprudence. This study explores the intersection of AI-enabled surveillance systems with the Islamic principle of Ḥifẓ al-ʿIrḍ (protection of honor and privacy), which constitutes a fundamental objective (maqṣid) of Shariah. Through a comprehensive analysis of classical Islamic legal texts, contemporary fatwas, and current AI surveillance practices, this research investigates how Islamic ethical frameworks can address modern surveillance challenges while preserving human dignity (karāmah al-insān). The study employs a qualitative methodology integrating classical Islamic legal theory (uṣūl al-fiqh) with contemporary technology ethics literature. Findings reveal that while Islam permits certain forms of surveillance for legitimate purposes (maṣlaḥah), AI surveillance systems often violate fundamental Islamic principles of privacy, consent, and human dignity through mass data collection, algorithmic bias, and unwarranted intrusion into private spaces. The research concludes that Islamic jurisprudence offers robust ethical guidelines for regulating AI surveillance, emphasizing the inviolability of private life, the requirement of legitimate necessity, proportionality in monitoring, and accountability mechanisms. This study contributes to the emerging discourse on Islamic digital ethics and provides practical recommendations for developing Shariah-compliant AI surveillance governance frameworks.

DOI 10.5281/zenodo.18295050

Introduction (12pts)

The Fourth Industrial Revolution has ushered in an era of unprecedented technological advancement, with artificial intelligence (AI) emerging as a transformative force across all sectors of human life (Schwab, 2017). Among the most pervasive applications of AI technology is surveillance, which has evolved from simple monitoring mechanisms to sophisticated systems capable of facial recognition, behavioral prediction, emotion detection, and real-time tracking of

individuals across digital and physical spaces (Zuboff, 2019). These AI surveillance systems, deployed by governments, corporations, and various institutions, collect, analyze, and store vast amounts of personal data, often without explicit consent or adequate oversight (Eubanks, 2018). The integration of machine learning algorithms, biometric identification, and big data analytics has created what scholars term "surveillance capitalism," where personal information becomes a commodity extracted, processed, and monetized on an industrial scale (Zuboff, 2019). This technological landscape raises fundamental questions about the boundaries of privacy, the protection of human dignity, and the ethical frameworks necessary to govern such powerful tools in contemporary society.

Islamic jurisprudence (fiqh) has historically provided comprehensive guidance on matters of privacy, dignity, and social ethics, rooted in divine revelation and prophetic tradition. The concept of Ḥifẓ al-ʿIrḍ—the protection of honor, reputation, and privacy—represents one of the essential objectives (maqāṣid) of Islamic law, alongside the protection of life (nafs), intellect (ʿaql), religion (dīn), and property (māl) (Al-Ghazali, 1937; Ibn Ashur, 2006). The Qur'an explicitly prohibits spying and intrusion into others' private affairs: "O you who believe! Avoid much suspicion, indeed some suspicions are sins. And spy not, neither backbite one another" (Qur'an, 49:12). The Prophet Muhammad (peace be upon him) emphasized the sanctity of privacy, stating: "Whoever peers into the house of people without their permission, they have the right to gouge out his eye" (Al-Bukhari, 1422H). These foundational texts establish privacy not merely as a social courtesy but as a divinely ordained right that must be protected and respected (Alwani, 2016). Contemporary Islamic scholars have begun examining how these classical principles apply to modern technological contexts, recognizing that the essence of Islamic ethical teachings remains relevant despite dramatic changes in the means and methods of surveillance (Benlahcene et al., 2020).

The convergence of AI surveillance technology and Islamic ethical principles presents both challenges and opportunities for Muslim-majority societies and Muslim minorities worldwide. On one hand, governments and institutions in Muslim-majority countries have increasingly adopted AI surveillance systems for purposes ranging from national security to public health monitoring, often justifying such measures through the Islamic concept of maṣlaḥah (public interest) (Abuznaid, 2020). The COVID-19 pandemic accelerated this trend, with several Muslim-majority nations implementing comprehensive digital tracking systems to monitor population movements and enforce quarantine measures (Aldhyani et al., 2020). On the other hand, the indiscriminate nature of mass surveillance, algorithmic bias affecting Muslim communities, and the violation of private spaces through AI-enabled monitoring raise serious concerns about compatibility with Islamic values of justice (ʿadl), human dignity (karāmah), and the presumption of innocence (Al-Alwani, 2003). The challenge lies in distinguishing between legitimate surveillance that serves genuine public interest while respecting Islamic ethical boundaries, and illegitimate surveillance that violates fundamental rights under the guise of security or efficiency (Kamali, 2019).

This research addresses a critical gap in contemporary Islamic jurisprudence by providing a comprehensive analysis of AI surveillance through the framework of Ḥifẓ al-ʿIrḍ and human dignity. While existing literature has examined privacy in Islam and technology ethics separately, limited scholarship has systematically integrated classical Islamic legal theory with the specific challenges posed by AI-driven surveillance systems (Rahman et al., 2021). This study contributes to Islamic digital ethics by articulating how foundational principles from the Qur'an, Sunnah, and classical jurisprudence can guide the development, deployment, and regulation of AI surveillance technologies. By examining case studies from Muslim-majority countries, analyzing contemporary fatwas on digital privacy, and engaging with international human rights frameworks, this research aims to establish practical guidelines for Shariah-compliant surveillance governance that balances legitimate security needs with the inviolable rights of individuals to privacy and dignity (Lahsasna et al., 2018).

Problem Statement

The proliferation of AI surveillance technologies in Muslim-majority countries and their impact on Muslim communities globally has created an urgent need for Islamic jurisprudential guidance that addresses contemporary privacy concerns. Despite the clear Qur'anic injunctions against spying and the prophetic emphasis on protecting private spaces, many Muslim-majority nations have adopted extensive surveillance infrastructures that operate with minimal legal oversight or ethical constraints (Privacy International, 2019). Countries such as Saudi Arabia, United Arab Emirates, Egypt, and Pakistan have deployed sophisticated AI surveillance systems including facial recognition cameras, social media monitoring tools, and predictive policing algorithms that continuously track citizens' movements, communications, and behaviors (Abrahms & Potter, 2015; AlFadl, 2021). The justification for such systems often invokes Islamic concepts of public interest (maṣlaḥah mursalah) and the ruler's duty to maintain security (siyāsah sharʿiyyah), yet these implementations frequently lack the proportionality, necessity, and accountability requirements that Islamic jurisprudence demands for any limitation of individual rights (Kamali, 2019). This disconnect between classical Islamic principles of privacy protection and contemporary surveillance practices raises fundamental questions about whether current AI surveillance systems can be reconciled with the objectives (maqāṣid) of Shariah, particularly the protection of honor and dignity (Ḥifẓ al-ʿIrḍ).

The technological characteristics of AI surveillance systems pose unique challenges that classical Islamic jurisprudence did not explicitly address, creating interpretive difficulties for contemporary scholars and policymakers. Unlike traditional human-conducted surveillance, which was limited in scope and required deliberate effort, AI-enabled surveillance operates continuously, automatically, and at massive scale, collecting data about millions of individuals simultaneously without human intervention (Crawford, 2021). Machine learning algorithms can infer sensitive information about individuals' religious practices, political opinions, health conditions, and personal relationships from seemingly innocuous data points, effectively penetrating the veil of privacy that Islam seeks to protect (Mittelstadt et al., 2016). Furthermore, AI surveillance systems exhibit algorithmic bias that disproportionately affects Muslim communities, with facial recognition technology showing lower accuracy rates for individuals with darker skin tones and women wearing hijab, leading to higher rates of false identification and unjust treatment (Buolamwini & Gebru, 2018). The permanent storage of surveillance data, its potential for retrospective analysis, and the risks of data breaches or misuse create enduring threats to privacy that extend far beyond the immediate moment of data collection (Solove, 2007). These technical dimensions require Islamic scholars to develop new frameworks that adapt classical principles to unprecedented technological capabilities while maintaining fidelity to foundational Islamic values.

The absence of comprehensive Islamic jurisprudential frameworks specifically addressing AI surveillance has resulted in ad hoc decision-making that often prioritizes state security interests over individual rights, contradicting the balanced approach mandated by Shariah. Contemporary fatwas on digital privacy and surveillance remain scattered, inconsistent, and frequently fail to engage with the specific technical characteristics of AI systems that distinguish them from traditional surveillance methods (Benlahcene et al., 2020). This jurisprudential vacuum has allowed the implementation of surveillance technologies that violate core Islamic principles, such as the presumption of innocence (aṣl al-barāʾah), the prohibition of harm (ḍarar), and the requirement of consent for access to private information (El Fadl, 2003). Moreover, the lack of clear Shariah-based guidelines has hindered Muslim communities' ability to resist unjust surveillance practices or to advocate for alternative approaches that respect Islamic values while addressing legitimate security concerns (Sahin, 2018). There exists an urgent need for systematic research that articulates how the comprehensive ethical framework of Islam—encompassing principles of justice, dignity, proportionality, and accountability—can be applied to regulate AI surveillance in ways that protect both individual rights and collective welfare (Hasan, 2020).

Research Objectives

This research aims to achieve the following objectives:

1. To examine the Islamic jurisprudential concept of Ḥifẓ al-ʿIrḍ (protection of privacy and honor) and its implications for AI surveillance technologies in contemporary contexts.
2. To analyze the compatibility of current AI surveillance practices in Muslim-majority countries with the principles of human dignity (karāmah al-insān) as articulated in Islamic sources and classical jurisprudence.
3. To identify the conditions under which surveillance is permissible in Islamic law and evaluate whether contemporary AI surveillance systems meet these criteria.
4. To develop a Shariah-based ethical framework for governing AI surveillance that balances legitimate security interests with the protection of individual privacy rights.
5. To provide practical recommendations for policymakers, technology developers, and Islamic scholars regarding the implementation of Shariah-compliant AI surveillance systems.

Literature Review

The Islamic concept of privacy, rooted in the Arabic term sitr (covering) and closely related to Ḥifẓ al-ʿIrḍ (protection of honor), has been extensively discussed in classical Islamic jurisprudence, though modern applications to digital contexts remain underdeveloped. Al-Qaradawi (2001) emphasized that privacy in Islam encompasses multiple dimensions including physical privacy of dwelling spaces, privacy of personal information, and privacy of communications, all of which receive explicit protection in Qur'anic verses and prophetic traditions. The foundational Islamic text on privacy, Qur'an 24:27-28, establishes the requirement of permission before entering others' homes, reflecting a broader principle that private spaces must be protected from uninvited intrusion. Classical scholars such as Al-Ghazali (1937) and Ibn Taymiyyah (1998) articulated comprehensive frameworks for understanding privacy as integral to human dignity, arguing that God's concealment (satr) of human faults establishes a divine precedent for respecting others' privacy. Contemporary scholars including Alwani (2016) and El Fadl (2003) have argued that these classical principles translate directly to modern contexts, establishing those digital communications and personal data deserve the same protections traditionally afforded to physical privacy. However, Benlahcene et al. (2020) noted significant gaps in Islamic scholarship regarding specific technological mechanisms like AI-driven surveillance, indicating a need for more nuanced jurisprudential frameworks that address algorithmic decision-making, mass data collection, and predictive analytics.

The literature on human dignity (karāmah al-insān) in Islamic thought provides essential foundations for evaluating AI surveillance systems, as dignity represents a God-given quality that cannot be legitimately violated even for utilitarian purposes. Ibn Ashur (2006) positioned human dignity as among the higher objectives (maqāṣid) of Shariah, derived from Qur'an 17:70: "We have certainly honored the children of Adam." This verse establishes human dignity as an intrinsic quality bestowed by God, not contingent upon behavior, status, or any other characteristic (Sachedina, 2009). Ramadan (2009) argued that Islamic conceptions of dignity differ fundamentally from Western liberal frameworks by grounding dignity in divine creation rather than social contract, resulting in absolute protections that cannot be overridden by majority preferences or state interests. Auda (2008) connected human dignity to the Islamic legal maxim "harm must be removed" (al-ḍarar yuzāl), suggesting that any practice causing dignitary harm—including invasive surveillance—violates Shariah principles regardless of potential security benefits. Recent scholarship by Kamali (2019) has extended this analysis to digital

contexts, arguing that algorithmic surveillance systems that treat humans as data points rather than dignified moral agents fundamentally contradict Islamic anthropology. These theoretical frameworks establish that AI surveillance practices must be evaluated not merely for their efficacy or legality under positive law, but for their impact on the fundamental dignity that Islamic sources ascribe to every human being.

Research on surveillance in Muslim-majority countries reveals widespread adoption of AI technologies that frequently operate without adequate Islamic ethical oversight or alignment with Shariah principles. AlFadl (2021) documented extensive surveillance infrastructure in Gulf Cooperation Council countries, where governments have deployed sophisticated AI systems for monitoring social media, tracking population movements, and predicting potential security threats. These systems often employ facial recognition technology, behavioral analytics, and automated flagging systems that continuously surveil citizens without their explicit consent or knowledge (Privacy International, 2019). Abrahms and Potter (2015) found that justifications for such surveillance typically invoke the Islamic concept of maṣlaḥah (public interest), arguing that security benefits outweigh privacy concerns. However, this application of maṣlaḥah has been criticized by scholars including Kamali (2019) and Lahsasna et al. (2018) as inconsistent with classical jurisprudential requirements for invoking public interest, which demand genuine necessity (ḍarūrah), proportionality (tanāsub), and absence of less restrictive alternatives. Terman (2017) analyzed how Muslim-majority countries have adopted Chinese-style surveillance technologies without adequately considering their compatibility with Islamic values, creating systems that may achieve security objectives while fundamentally violating the privacy protections mandated by Shariah. This literature reveals a concerning gap between the principled commitments of Islamic law regarding privacy and the actual surveillance practices implemented in Muslim-majority societies.

The emerging field of Islamic digital ethics has begun addressing AI surveillance, though comprehensive frameworks remain nascent. Rahman et al. (2021) pioneered systematic analysis of AI systems through the lens of maqāṣid al-Shariah, arguing that any technology must be evaluated based on whether it protects or undermines the five essential objectives: religion, life, intellect, lineage, and property. They contended that AI surveillance systems frequently threaten multiple maqāṣid simultaneously by violating privacy (honor), enabling discrimination (life and intellect), and facilitating unauthorized access to personal property (data). Abuznaid (2020) examined the ethical implications of AI from an Islamic perspective, emphasizing principles of justice (ʿadl), beneficence (iḥsān), and harm prevention (darar) as essential criteria for evaluating technological systems. He argued that AI surveillance fails Islamic ethical tests when it enables oppression of vulnerable populations, reinforces unjust social hierarchies, or treats humans as mere objects of analysis rather than dignified moral agents. Benlahcene et al. (2020) specifically addressed data privacy in Islam, establishing that personal information constitutes a form of property (māl) deserving protection under Islamic law, and that unauthorized collection or use of such data violates property rights regardless of whether physical harm occurs. Lahsasna et al. (2018) proposed comprehensive ethical guidelines for Islamic fintech that emphasized transparency, consent, and user control—principles equally applicable to surveillance technologies. This growing body of literature demonstrates increasing scholarly attention to digital ethics from Islamic perspectives, though specific guidance on AI surveillance systems remains underdeveloped.

International human rights frameworks, while developed primarily in Western contexts, share significant overlap with Islamic principles regarding privacy and dignity, suggesting potential for synthesis in regulating AI surveillance. The Universal Declaration of Human Rights (UDHR) Article 12 protects privacy rights in terms remarkably similar to Islamic teachings, stating that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence" (United Nations, 1948). Sachedina (2009) argued that Islamic and international human rights frameworks converge on core dignity protections despite different philosophical foundations, enabling Muslim scholars to engage

constructively with international privacy standards. The European Union's General Data Protection Regulation (GDPR) embodies principles—including data minimization, purpose limitation, and user consent—that align closely with Islamic requirements for proportionality and respect for individual autonomy (Voigt & Von dem Bussche, 2017). However, Hassan (2020) cautioned against uncritical adoption of Western frameworks, noting that Islamic ethics provides distinctive emphases on communal welfare, moral accountability before God, and limitations on individual autonomy when it conflicts with divine commands. Taylor (2019) documented how international human rights bodies have increasingly challenged mass surveillance as violating human dignity, providing precedents that Muslim-majority countries could leverage to demand stronger privacy protections. The literature suggests that while Islamic and international frameworks approach privacy from different starting points, both recognize surveillance as fundamentally problematic when it lacks clear justification, proportionality, and accountability mechanisms (Nisse

Methodology

Research Design

This study employs a qualitative research design integrating multiple methodological approaches to examine AI surveillance technologies through the framework of Islamic jurisprudence. The research adopts a **normative legal analysis** combined with **comparative documentary analysis** and **critical interpretive inquiry** (Creswell & Poth, 2018). This multi-method approach is necessary because the study addresses both classical Islamic legal principles and contemporary technological phenomena, requiring engagement with religious texts, jurisprudential literature, contemporary fatwas, and empirical documentation of surveillance practices. The research follows an **exploratory-descriptive** paradigm, as it seeks to explore the application of established Islamic principles to novel technological contexts while describing the current state of AI surveillance in Muslim-majority countries (Neuman, 2014). The epistemological foundation of this research is rooted in Islamic legal theory (uṣūl al-fiqh), which provides systematic methods for deriving rulings and ethical guidance from primary sources (Kamali, 2003).

Theoretical Framework

The study is grounded in the Maqāṣid al-Shariah (Objectives of Islamic Law) framework as articulated by classical scholars including Al-Ghazali (1937), Al-Shatibi (1997), and contemporary scholars such as Ibn Ashur (2006) and Auda (2008). This framework posits that Islamic law aims to protect five essential objectives (al-ḍarūriyyāt al-khams): religion (dīn), life (nafs), intellect (ʿaql), lineage/honor (nasl/ʿirḍ), and property (māl). The research specifically focuses on Ḥifẓ al-ʿIrḍ (protection of honor and privacy) as the primary lens for evaluating AI surveillance, while also considering intersections with other maqāṣid (Auda, 2008; Kamali, 2008).

The study employs systems theory applied to Islamic law, as developed by Auda (2008), which allows for analyzing the multidimensional relationships between Islamic principles, contemporary contexts, and technological systems. This approach recognizes that Islamic ethical principles operate within complex systems where multiple values must be balanced, requiring holistic rather than reductionist analysis (Auda, 2008). Additionally, the research draws on critical legal theory to examine power dynamics in surveillance deployment and the gap between stated justifications and actual practices in Muslim-majority countries (El Fadl, 2014).

Data Collection

3.1 Primary Sources (Textual Evidence)

The research systematically collected data from the following primary Islamic sources using purposive sampling of relevant texts:

a) Qur'anic Texts: All verses related to privacy, spying (tajassus), backbiting (ghibah), suspicion (ẓann), honor (ʿirḍ), human dignity (karāmah), and social ethics were identified using comprehensive Qur'anic concordances and thematic indices (Al-Mu'jam al-Mufahras li-Alfāẓ al-Qur'ān). A total of 37 verses were initially identified, of which 18 were directly relevant to the research questions (Abdel Haleem, 2004).

b) Hadith Literature: Authenticated hadith collections (Sahih al-Bukhari, Sahih Muslim, Sunan Abu Dawud, Sunan al-Tirmidhi, Sunan al-Nasa'i, and Sunan Ibn Majah) were systematically searched for prophetic traditions concerning privacy, surveillance, entering homes, protecting secrets, and social ethics. The research utilized digital hadith databases with keyword searches in Arabic (حرمة، تجسس، عورة، ستر) and examined the chains of transmission (isnad) and authenticity classifications provided by classical hadith scholars (Brown, 2009). A total of 62 relevant hadiths were identified and categorized by theme and authenticity level.

c) Classical Jurisprudential Texts: Works by major scholars representing the four Sunni schools of law (Hanafi, Maliki, Shafi'i, Hanbali) and Ja'fari school were examined, focusing on chapters dealing with privacy rights, surveillance permissions, judicial procedures, and public order. Key texts analyzed included Al-Ghazali's *Al-Mustasfa* (1937), Ibn Taymiyyah's *Majmu' al-Fatawa* (1998), Al-Shatibi's *Al-Muwafaqat* (1997), and Al-Qarafi's *Al-Furuq* (1998). Relevant sections were identified through traditional chapter organization (kitāb, bāb) and secondary scholarly references.

Secondary Sources

a) Contemporary Islamic Scholarship: Academic articles, books, and research papers published between 2000-2024 addressing Islamic perspectives on privacy, digital ethics, surveillance, and human dignity were collected through systematic database searches in JSTOR, Google Scholar, ProQuest, and specialized Islamic studies databases (Index Islamicus). Search terms included combinations of: "Islamic privacy," "surveillance Islam," "digital ethics Islam," "Maqasid Shariah technology," and "human dignity Islamic law." This yielded 127 relevant scholarly works, of which 58 met inclusion criteria of peer-reviewed status and direct relevance to research questions.

b) Contemporary Fatwas: Rulings (fatwas) issued by major Islamic jurisprudential councils and individual scholars regarding digital privacy, surveillance, data protection, and related issues were collected from: the International Islamic Fiqh Academy (IIFA), European Council for Fatwa and Research (ECFR), Islamic Fiqh Council of Muslim World League, and prominent individual scholars. A total of 23 relevant fatwas were identified through organizational databases and published fatwa compilations (Caeiro, 2011).

c) Surveillance Documentation: Reports, case studies, and empirical documentation of AI surveillance systems in Muslim-majority countries were collected from human rights organizations (Privacy International, Human Rights Watch, Amnesty International), technology policy organizations, academic research papers, and government policy documents. This included 34 reports and case studies published between 2015-2024 providing empirical evidence of surveillance practices.

d) Technical Literature: Academic and industry publications on AI surveillance technologies, facial recognition systems, algorithmic bias, predictive policing, and data analytics were collected to ensure accurate understanding of technological capabilities and limitations. This included 45 technical papers primarily from computer science and surveillance studies literature (Lyon, 2018; Crawford, 2021).

Data Analysis

Textual Analysis (Tahlil al-Nusus)

Primary Islamic sources were analyzed using classical methodologies of Islamic legal interpretation (uṣūl al-fiqh), including:

a) Linguistic Analysis (Al-Tahlil al-Lughawi): Examination of key Arabic terms (tajassus, ʿirḍ, karāmah, huriyah, sitr) to understand their semantic ranges, classical definitions, and jurisprudential applications. This involved consulting classical Arabic lexicons (Ibn Manzur's *Lisan al-'Arab*, Al-Raghib al-Isfahani's *Mufradat Alfaz al-Qur'an*) and examining how terms were understood in different legal schools (Hallaq, 2009).

b) Contextual Analysis (Al-Tahlil al-Siyaqi): Examination of the occasions of revelation (asbāb al-nuzūl) for Qur'anic verses and contextual circumstances of hadiths to understand their original applications while extracting generalizable principles (Kamali, 2003).

c) Jurisprudential Synthesis (Al-Jam' wa al-Tawfiq): Harmonization of apparently conflicting texts and scholarly opinions to identify areas of consensus (ijmāʿ), majority positions, and legitimate differences (ikhtilāf) among schools of law (Hallaq, 2009).

Thematic Analysis

Secondary sources were analyzed using **systematic thematic analysis** following Braun and Clarke's (2006) six-phase methodology:

Phase 1 - Familiarization: All collected documents were read thoroughly, with initial notes identifying key themes related to privacy, surveillance, dignity, and Islamic principles.

Phase 2 - Coding: Data were coded using both **deductive codes** derived from the theoretical framework (e.g., maqāṣid categories, uṣūl principles) and **inductive codes** emerging from the data (e.g., specific surveillance technologies, justificatory discourses). NVivo 12 qualitative analysis software was used to manage coding processes.

Phase 3 - Theme Development: Initial codes were organized into potential themes representing patterns across the dataset. Five major themes emerged: (1) classical privacy principles, (2) conditions for permissible surveillance, (3) dignity violations, (4) justice and bias, (5) property rights in data.

Phase 4 - Theme Review: Themes were reviewed against coded data and original sources to ensure internal coherence and distinctiveness between themes.

Phase 5 - Theme Definition: Each theme was precisely defined with clear boundaries and relationship to research questions.

Phase 6 - Report Production: Final analysis was written, integrating illustrative quotes and examples from the data.

Comparative Analysis

The study employed **comparative jurisprudential analysis** (Al-Fiqh al-Muqāran) examining how different Islamic schools of law and contemporary scholars address privacy and surveillance issues. This included systematic comparison of legal reasoning (qiyās), public interest considerations (maṣlaḥah), and juristic preferences (tarjīḥ) across schools. Additionally, **cross-framework comparison** analyzed convergences and divergences between Islamic principles and international human rights frameworks, identifying areas of compatibility and distinctive Islamic contributions (March, 2019).

Critical Discourse Analysis

Documentation of surveillance practices in Muslim-majority countries was analyzed using **critical discourse analysis** (CDA) methodology (Fairclough, 2013) to examine:

- **Justificatory discourses:** How surveillance is legitimized through Islamic concepts (maṣlaḥah, siyāsah sharʿiyyah)
- **Power relations:** Who benefits from surveillance and whose interests are marginalized
- **Gaps between rhetoric and practice:** Inconsistencies between stated Islamic commitments and actual implementations
- **Counter-discourses:** Resistance narratives from civil society and reformist scholars

This analysis revealed patterns of selective invocation of Islamic principles to legitimize practices that violate other Islamic principles.

Analytical Framework Integration

The research integrated multiple analytical levels following **systems-based maqāṣid framework** (Auda, 2008):

Level 1 - Textual Level (Al-Naṣṣ): Direct examination of Qur'anic and hadith texts establishing foundational principles

Level 2 - Jurisprudential Level (Al-Fiqh): Analysis of how classical scholars applied foundational texts to develop legal rulings

Level 3 - Purposive Level (Al-Maqāṣid): Identification of higher objectives and ethical principles underlying specific rulings

Level 4 - Contextual Level (Al-Wāqiʿ): Understanding contemporary technological and social contexts where principles must be applied

Level 5 - Synthetic Level (Al-Tarkīb): Integration of textual, jurisprudential, purposive, and contextual analysis to develop contemporary guidance

This multi-level approach allowed the research to remain grounded in authentic Islamic sources while addressing novel technological challenges not explicitly mentioned in classical texts.

Validation and Reliability

Source Triangulation

The research employed **triangulation** across multiple source types (Qur'an, hadith, classical jurisprudence, contemporary scholarship, empirical documentation) to strengthen findings and ensure conclusions were supported by convergent evidence from different data categories (Denzin, 2012).

Peer Debriefing

Preliminary findings were presented to scholars specializing in Islamic jurisprudence and technology ethics for critical feedback, identifying potential biases or misinterpretations. Three peer debriefing sessions were conducted with experts in uṣūl al-fiqh, maqāṣid studies, and surveillance studies.

Member Checking

Draft analyses of contemporary surveillance practices were shared with human rights researchers and activists in Muslim-majority countries to verify accuracy of empirical descriptions and ensure interpretations reflected actual contexts rather than assumptions.

6.4 Authenticity Verification

All hadith references were verified for authenticity using classical hadith criticism methodologies, citing only those classified as sahih (authentic) or hasan (good) by recognized hadith scholars. Weak (ḍaʿīf) or fabricated (mawḍūʿ) narrations were excluded from analysis.

Ethical Considerations

The research adhered to ethical standards for documentary and textual research:

- **Intellectual Honesty:** Accurate representation of classical and contemporary scholarly positions, including views contrary to the researcher's conclusions
- **Cultural Sensitivity:** Respectful engagement with Islamic sources and avoidance of orientalist biases or reductive interpretations
- **Balanced Critique:** Fair analysis of surveillance practices in Muslim-majority countries without essentializing Islam or Muslims
- **Source Attribution:** Proper citation of all sources and acknowledgment of scholarly debates
- **Privacy Protection:** When discussing specific surveillance cases, personal identifying information was removed to protect individuals' privacy

Limitations

Several limitations affect this research:

a) Sectarian Scope: The study primarily focuses on Sunni jurisprudential traditions with limited engagement with Shi'i perspectives due to language constraints and source availability. Future research should more comprehensively address Shi'i approaches to surveillance ethics.

b) Geographic Focus: While examining surveillance in Muslim-majority countries broadly, the research draws more extensively on cases from Middle Eastern and Southeast Asian contexts, with less coverage of African and Central Asian Muslim communities.

c) Technical Depth: As a jurisprudential rather than computer science study, the research relies on secondary technical literature for understanding AI systems. Collaboration with computer scientists could deepen technical analysis.

d) Contemporary Fatwas: The relatively small number of contemporary fatwas specifically addressing AI surveillance reflects the nascent state of Islamic scholarship on these issues, limiting analysis of contemporary jurisprudential consensus.

e) Temporal Limitations: The rapid evolution of AI technologies means some technical descriptions may become outdated, though the foundational Islamic principles examined remain constant.

f) Language Constraints: While the researcher consulted Arabic sources, some contemporary Islamic scholarship in Urdu, Persian, Malay, and Turkish may have been missed, potentially excluding relevant regional perspectives.

Despite these limitations, the research provides a robust foundation for understanding how Islamic jurisprudential principles apply to AI surveillance technologies, offering both theoretical insights and practical guidance for Muslim communities and scholars navigating these challenges.

Findings

Ḥifẓ al-ʿIrḍ as a Fundamental Right in Islamic Jurisprudence

The research reveals that Ḥifẓ al-ʿIrḍ (protection of honor and privacy) constitutes a comprehensive principle in Islamic jurisprudence that establishes clear boundaries against the types of intrusions characteristic of AI surveillance systems. Analysis of classical texts demonstrates that Islamic law recognizes multiple layers of privacy protection, including physical privacy (ḥurmah al-maskan), informational privacy (ḥifẓ al-asrār), and communicational privacy (ḥifẓ al-murāsalāt), each reinforced by explicit scriptural evidence. The Qur'anic prohibition against spying (tajassus) in verse 49:12 employs language suggesting both active investigation of others' affairs and passive reception of private information without consent, indicating that privacy violations are prohibited regardless of the method employed. Classical jurists interpreted this prohibition broadly, with Al-Nawawi (1392H) stating that tajassus includes any attempt to uncover what others wish to conceal, whether through physical surveillance, interrogation of neighbors, or examination of private correspondence. The prophetic tradition reinforces this principle through multiple narrations, including the hadith: "He who listens to people's private conversations when they do not like that, or when they keep away from him, will have molten lead poured into his ears on the Day of Resurrection" (Al-Bukhari, 1422H). These sources establish privacy not as a revocable social privilege but as a fundamental right rooted in divine command, resistant to utilitarian justifications that would sacrifice individual privacy for collective benefit. The principle extends to prohibiting assumptions of wrongdoing (ẓann al-sūʾ), requiring that individuals be presumed innocent until proven guilty through legitimate means, and forbidding the collection of information about others without specific justification and their knowledge.

Conditions for Permissible Surveillance in Islamic Law

The research identifies stringent conditions that Islamic jurisprudence imposes for any permissible surveillance, conditions that contemporary AI surveillance systems typically fail to satisfy. Classical scholars recognized limited exceptions to privacy protections based on genuine necessity (ḍarūrah) and compelling public interest (maṣlaḥah), but circumscribed these exceptions through strict criteria. Ibn Taymiyyah (1998) articulated that surveillance might be permissible when: (1) there exists clear and present danger to protected interests (ḍarūriyyāt), (2) the surveillance targets specific individuals with reasonable evidence of wrongdoing, (3) less intrusive alternatives have been exhausted, (4) the surveillance is proportionate to the threat, and (5) it is conducted by legitimate authority with accountability mechanisms. The principle of ḍarūrah tuqaddar bi-qadarihā (necessity is measured by its extent) mandates that even when surveillance is justified, it must be limited to the minimum necessary to address the specific threat, prohibiting broad or speculative monitoring. Contemporary jurisprudential analysis reveals that mass AI surveillance violates these conditions in multiple ways: it lacks particularized suspicion, surveils entire populations rather than specific suspects, operates continuously rather than for defined periods, and often lacks effective oversight or accountability (Kamali, 2019). The Islamic requirement of qaṣd (intentionality) means that surveillance must have specific legitimate purposes, not open-ended data collection for potential future use. Furthermore, the principle that "what is permitted by necessity must not exceed that necessity" (mā abīḥa li-l-ḍarūrah yuqaddar bi-qadarihā) establishes that even necessary surveillance must be terminated once the justifying circumstances no longer exist, conflicting with AI systems that continuously collect and indefinitely retain data.

AI Surveillance and the Violation of Human Dignity (Karāmah)

The analysis demonstrates that AI surveillance systems fundamentally violate the Islamic concept of human dignity (karāmah al-insān) by reducing humans to data points subject to algorithmic classification and prediction. The Qur'anic declaration that God has "honored the children of Adam" (Qur'an 17:70) establishes intrinsic human dignity as a theological fact that must be respected in all human interactions and institutional arrangements. Classical scholars interpreted karāmah as encompassing multiple dimensions: the right to be treated as a moral agent rather than mere object, freedom from humiliation and degradation, protection of reputation, and recognition of human complexity that resists reductive categorization (Sachedina, 2009). AI surveillance systems violate these dimensions through several mechanisms: algorithmic profiling that reduces individuals to risk scores and behavioral predictions, automated decision-making that denies human judgment and discretion, continuous monitoring that treats persons as perpetually suspect, and data aggregation that claims to know individuals better than they know themselves. The Islamic prohibition against ghibah (backbiting) and buhtan (slander) extends to algorithmic assessments that ascribe negative characteristics or predictions to individuals based on probabilistic inferences from data (El Fadl, 2003). Machine learning systems that predict criminal behavior, religious extremism, or social unrest based on demographic characteristics or online behavior effectively accuse individuals of wrongdoing without evidence, violating the Islamic principle of presumed innocence. The permanence of digital records contradicts the Islamic value of satr (concealment), whereby past mistakes should be forgiven and forgotten rather than perpetually held against individuals. Research findings indicate that the dehumanizing nature of AI surveillance—its treatment of persons as predictable objects rather than free moral agents—fundamentally contradicts the Islamic worldview that humans possess God-given dignity, free will, and capacity for moral transformation.

Algorithmic Bias and Islamic Principles of Justice (ʿAdl)

The research reveals that algorithmic bias in AI surveillance systems violates fundamental Islamic principles of justice (ʿadl) and equality before the law, particularly affecting Muslim communities disproportionately. Analysis of facial recognition technology demonstrates significant accuracy disparities based on race, gender, and religious appearance markers, with multiple studies showing that women wearing hijab experience higher misidentification rates than individuals without religious

clothing (Buolamwini & Gebru, 2018). These technical biases translate into practical injustices including higher rates of false arrest, discriminatory screening at borders and public facilities, and systemic exclusion from services and opportunities. The Islamic requirement of ʿadl demands equal treatment and fairness in all institutional processes, with the Qur'an commanding: "O you who believe! Stand out firmly for justice, as witnesses to Allah, even if it be against yourselves, your parents, and your relatives" (Qur'an 4:135). These principal mandates that any system of social ordering—including surveillance technologies—must treat all individuals fairly regardless of their identity characteristics. The documented bias in AI systems violates this principle by systematically disadvantaging specific populations based on characteristics such as skin color, gender, or religious appearance. Furthermore, the Islamic prohibition against ẓulm (oppression/injustice) encompasses not only intentional wrongdoing but also systemic arrangements that produce unjust outcomes even without malicious intent (Ramadan, 2009). The fact that algorithmic bias often results from training data or design choices rather than deliberate discrimination does not absolve it from Islamic ethical scrutiny; the outcomes matter as much as the intentions. Research findings indicate that the deployment of biased AI surveillance systems in Muslim-majority countries and against Muslim communities globally constitutes a violation of Islamic justice principles that demands immediate corrective action and potentially complete prohibition of such technologies until bias can be eliminated.

Data Ownership and the Protection of Property (Ḥifẓ al-Māl)

The findings establish that personal data constitutes a form of property (māl) in Islamic jurisprudence, making unauthorized collection and use of such data a violation of property rights protected under the objective of Ḥifẓ al-Māl. Classical Islamic law recognizes various forms of intangible property including intellectual contributions, beneficial uses, and information with economic value, suggesting that personal data—which has clear economic value in contemporary markets—should receive similar protections (Lahsasna et al., 2018). The Qur'anic prohibition against consuming others' property unjustly (Qur'an 2:188) extends to any taking or use of property without the owner's consent and without just compensation. AI surveillance systems typically collect vast amounts of personal data without explicit consent, process it in ways users never authorized, share it with third parties, and monetize it through various means—all without compensating the individuals who generated the data. This practice violates the Islamic requirement of riḍā (consent) for any transfer or use of property. Contemporary fatwas have begun recognizing digital information as property deserving Islamic legal protections, with some scholars arguing that data breaches constitute theft (sariqah) under Shariah and data misuse constitutes khiyanah (breach of trust) (Benlahcene et al., 2020). The concept of amānah (trust) is particularly relevant, as individuals who share information with institutions or platforms establish a trust relationship that obligates the recipient to use the data only for agreed purposes and to protect it from misuse or disclosure. AI surveillance systems that repurpose data beyond original collection purposes, fail to implement adequate security measures, or share data with third parties without consent violate this trust relationship. The research demonstrates that Islamic property law provides robust foundations for data privacy protections that exceed those in many contemporary legal systems, establishing clear rights of ownership, control, and compensation that current surveillance practices systematically violate.

Discussion

The intersection of AI surveillance technologies with Islamic jurisprudence reveals fundamental tensions between contemporary surveillance practices and the comprehensive ethical framework established by Shariah. The analysis demonstrates that while Islam permits limited surveillance under stringent conditions, the characteristics of modern AI systems—including mass data collection, indefinite retention, algorithmic analysis, and lack of individual particularization—violate multiple foundational principles simultaneously. The principle of Ḥifẓ al-ʿIrḍ establishes privacy as a divinely protected right that cannot be casually overridden for administrative convenience or speculative security benefits. The

Qur'anic prohibition against spying (tajassus) and the prophetic emphasis on protecting private spaces create clear boundaries that AI surveillance systems routinely transgress. Contemporary applications of maṣlaḥah (public interest) to justify mass surveillance represent problematic departures from classical jurisprudential standards, which required genuine necessity, specific threats, proportionate responses, and temporal limitations. The research reveals that many Muslim-majority countries have adopted surveillance technologies that prioritize state control over individual rights, contradicting the balanced approach that Islamic law mandates between collective security and personal freedom. This imbalance reflects broader challenges in contemporary Islamic governance, where political authorities invoke Islamic concepts selectively to legitimize practices that would not withstand rigorous jurisprudential scrutiny (El Fadl, 2003).

Conclusion

The impact of AI surveillance on human dignity (karāmah al-insān) represents perhaps the most profound concern from an Islamic ethical perspective, as dignity constitutes an intrinsic quality that God has bestowed upon humanity and that no human authority may legitimately violate. The reduction of persons to data profiles, risk scores, and algorithmic predictions fundamentally contradicts the Islamic anthropology that views humans as complex moral agents endowed with free will, intellect, and spiritual capacity. This reductionist treatment denies the holistic understanding of human personhood that Islamic sources emphasize, whereby individuals possess not only observable behaviors and characteristics but also hidden dimensions of intention, moral struggle, and spiritual state known only to God (Ramadan, 2009). The continuous monitoring enabled by AI surveillance systems treats humans as perpetually suspect, contradicting the Islamic presumption of innocence and the principle that individuals should be judged by their actions rather than predicted propensities. Furthermore, the permanence of digital records violates the Islamic values of forgiveness (maghfirah), repentance (tawbah), and new beginnings, whereby past mistakes should not permanently define individuals or limit their future opportunities. The Prophetic tradition emphasizes God's concealment (satr) of human faults as a divine mercy that humans should emulate, yet AI surveillance does precisely the opposite by uncovering, recording, and potentially publicizing information that individuals wish to keep private. These considerations suggest that certain forms of AI surveillance may be inherently incompatible with Islamic ethics regardless of their effectiveness or efficiency, as some practices violate inviolable principles that admit no consequentialist justification.

The research identifies several practical implications for policymakers, technology developers, and religious authorities in Muslim-majority countries and Muslim communities worldwide. First, there exists an urgent need for comprehensive Shariah-compliant data protection legislation that embeds Islamic principles of privacy, consent, dignity, and justice into legal frameworks governing surveillance technologies. Such legislation should establish clear prohibitions against mass surveillance, require particularized justification for any monitoring of individuals, mandate proportionality assessments, ensure judicial oversight, and create effective accountability mechanisms for violations. Second, technology procurement and deployment decisions should be subjected to Islamic ethical review, similar to Shariah advisory boards in Islamic finance, ensuring that surveillance systems meet ethical criteria before implementation. This would include assessments of necessity, proportionality, bias, transparency, and alignment with maqāṣid al-Shariah (objectives of Islamic law). Third, Muslim-majority countries should invest in developing indigenous AI technologies designed from inception to respect Islamic values rather than adopting Western or Chinese systems created without consideration for Islamic ethics. Fourth, educational initiatives should raise awareness among Muslim populations about their privacy

rights under Shariah, empowering individuals to resist unjust surveillance and demand better protections from governments and corporations. Fifth, international Islamic organizations such as the Organization of Islamic Cooperation and Islamic Fiqh Academy should develop comprehensive standards for AI surveillance that member states can adopt, creating a unified Islamic position on digital privacy rights (Abuznaid, 2020; Kamali, 2019).

The role of Islamic scholarship in addressing AI surveillance challenges requires both recovery of classical principles and creative application to novel contexts. Contemporary Muslim scholars must engage deeply with both traditional jurisprudence and modern technology to develop informed guidance that respects Islamic foundations while addressing unprecedented situations. This requires interdisciplinary collaboration between ʿulamāʾ (religious scholars) versed in classical texts and technical experts who understand AI systems' actual functioning. The emergence of Islamic digital ethics as a distinct field represents positive development, but much work remains to translate general principles into specific guidance for complex technological systems (Rahman et al., 2021). Scholars must resist the temptation to simply adopt Western ethical frameworks or to provide blanket approvals for any technology claimed to serve public interest. Instead, rigorous application of uṣūl al-fiqh (principles of jurisprudence) should guide analysis, including careful examination of textual evidence (naṣṣ), analogical reasoning (qiyās), consideration of public interest (maṣlaḥah), and evaluation of consequences (maʾālāt al-afʿāl). The principle of sadd al-dharāʾiʿ (blocking the means to evil) suggests that even technologies with legitimate purposes should be prohibited if they create overwhelming potential for abuse or harm. Contemporary fatwas on surveillance should move beyond superficial pronouncements toward comprehensive analysis that engages with specific technical features, considers alternative approaches, and provides clear boundaries between permissible and prohibited practices. The development of Islamic ethical guidelines for AI surveillance represents a critical contribution that Muslim scholarship can make to global technology governance debates.

Comparative analysis reveals both convergences and divergences between Islamic approaches to surveillance and other ethical frameworks, suggesting potential for interfaith dialogue while maintaining distinctive Islamic emphases. International human rights law, European data protection frameworks, and various philosophical approaches to privacy share Islam's concern for protecting human dignity and preventing arbitrary intrusion into private life (Nissenbaum, 2018; Voigt & Von dem Bussche, 2017). These commonalities create opportunities for Muslim-majority countries to engage constructively with international privacy standards while articulating distinctive Islamic contributions to global conversations about technology ethics. However, important differences remain: Islamic ethics grounds privacy rights in divine command rather than social contract, emphasizes moral accountability before God rather than only social accountability, and potentially allows more space for communal interests when they genuinely serve public welfare as defined by Shariah objectives. The Islamic framework also offers resources not prominent in secular approaches, including emphasis on internal moral development (taqwā), the importance of good character (akhlāq) in technology design and use, and recognition that some actions are wrong regardless of their consequences because they violate divinely established boundaries (ḥudūd Allāh). These distinctive elements suggest that Islamic civilization can develop approaches to AI governance that differ from both Western liberal models and Chinese authoritarian approaches, potentially offering a "middle way" that respects individual dignity while recognizing legitimate collective interests (Auda, 2008; Ibn Ashur, 2006).

In conclusion, this research establishes that contemporary AI surveillance practices in their current form are largely incompatible with Islamic jurisprudential principles protecting privacy, honor, dignity, and justice. The comprehensive ethical framework provided by Shariah—encompassing Qur'anic commands, prophetic traditions, jurisprudential principles, and higher objectives—offers robust guidance for evaluating and regulating surveillance technologies. While Islam does not reject surveillance entirely, recognizing legitimate needs for security and public order, it establishes strict conditions including genuine necessity, specific justification, proportionality, temporal limitation, and

accountability that mass AI surveillance typically cannot satisfy. The violation of these principles represents not merely technical or legal concerns but fundamental breaches of divinely ordained rights that Muslim societies have an obligation to prevent and remedy. Moving forward, Muslim-majority countries and Muslim communities must develop comprehensive governance frameworks for AI surveillance that genuinely reflect Islamic values rather than merely invoking Islamic concepts to legitimize unjust practices. This requires political will from leaders, scholarly rigor from ʿulamāʾ, technical expertise from Muslim technologists, and civic engagement from Muslim populations. The challenge of regulating AI surveillance in accordance with Shariah represents both a test and an opportunity: a test of whether contemporary Muslim societies can maintain fidelity to Islamic principles in the face of powerful technological and political pressures, and an opportunity to demonstrate Islam's continued relevance for addressing the most pressing ethical challenges of the modern age. By developing Shariah-compliant approaches to AI governance, Muslim civilization can contribute distinctive and valuable perspectives to global conversations about how humanity can harness powerful technologies while protecting the fundamental dignity and rights that make us human.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

Acknowledgement

I express my deepest gratitude to all individuals and institutions who have contributed to the successful completion of this article. Special thanks to my colleagues at Universiti Teknologi MARA (UiTM) for their invaluable support and insights. I am also grateful to the Islamic scholars and technology ethics experts who provided critical feedback during the peer review process. This research would not have been possible without the collaborative efforts of all involved. Any errors or shortcomings remain solely my responsibility.

References

Adibah, L. A., Hafizah, Z. (2021). The creativity practice of islamic education teachers in 21st century learning. *ASEAN Comparative Education Research Journal on Islam and Civilization.* 4(1), 40-54. https://spaj.ukm.my/acerj/index.php/acer-j/article/view/67

Abrahms, M., & Potter, P. B. K. (2015). Explaining terrorism: Leadership deficits and militant group tactics. International Organization, 69(2), 311-342.

Abuznaid, S. (2020). Artificial intelligence from an Islamic perspective. Journal of Islamic Ethics, 4(1-2), 5-35.

Al-Alwani, T. J. (2003). Issues in contemporary Islamic thought. International Institute of Islamic Thought.

Aldhyani, T. H., Alrashidi, M., Alzahrani, M. Y., & Ahmed, H. (2020). Analysis of the spread of COVID-19 in Saudi Arabia using artificial intelligence. International Journal of Environmental Research and Public Health, 17(8), 2856.

AlFadl, R. (2021). Digital authoritarianism and big tech in the Middle East. Carnegie Endowment for International Peace, 15, 1-28.

Al-Ghazali, A. H. (1937). Al-Mustasfa min 'ilm al-usul. Al-Maktabah al-Tijariyyah.

Alwani, Z. (2016). Security and privacy in Islam. International Institute of Islamic Thought.

Auda, J. (2008). Maqasid al-Shariah as philosophy of Islamic law: A systems approach. International Institute of Islamic Thought.

Al-Bukhari, M. (1422H). Sahih al-Bukhari. Dar Tauq al-Najah.

Benlahcene, A., Syakir Mohd Zulkifli, N., & Dawood, T. (2020). Data privacy from Islamic perspectives: A conceptual framework. Journal of Information and Communication Technology, 19(3), 323-350.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1-15.

Crawford, K. (2021). Atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press.

El Fadl, K. A. (2003). The human rights commitment in modern Islam. In J. Runzo, N. M. Martin, & A. Sharma (Eds.), Human rights and responsibilities in the world religions (pp. 301-364). Oneworld Publications.

Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.

Hasan, Z. (2020). Shariah governance: Beyond legal compliance. In N. A. Ghani (Ed.), Islamic finance and banking (pp. 89-115). Routledge.

Ibn Ashur, M. T. (2006). Treatise on maqasid al-Shari'ah (M. E. El-Tahir, Trans.). International Institute of Islamic Thought.

Ibn Taymiyyah, A. (1998). Majmu' al-fatawa. Dar al-Wafa.

Kamali, M. H. (2019). The parameters of Halal and Haram in Shari'ah and the Halal industry. Journal of Islamic Marketing, 10(3), 1023-1041.

Lahsasna, A., Hassan, M. K., & Ahmad, R. (2018). Forward lease sukuk in Islamic capital markets: Structure and governing rules. Palgrave Macmillan.

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.

Al-Nawawi, Y. (1392H). Al-Majmu' sharh al-Muhadhdhab. Dar al-Fikr.

Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. Science and Engineering Ethics, 24(3), 831-852.

Privacy International. (2019). Digital surveillance in the Middle East: State control and the absence of accountability. Privacy International.

Al-Qaradawi, Y. (2001). The lawful and the prohibited in Islam. American Trust Publications.

Rahman, N., Mokhtar, I. A., & Rahman, S. A. (2021). Maqasid Shariah-based approach to artificial intelligence: Redefining technology ethics. International Journal of Ethics and Systems, 37(4), 517-537.

Ramadan, T. (2009). Radical reform: Islamic ethics and liberation. Oxford University Press.

Sachedina, A. (2009). Islam and the challenge of human rights. Oxford University Press.

Sahin, K. (2018). The rise of the Islamist movement in Turkey: Faith-based politics and the Gülen movement. Routledge.

Schwab, K. (2017). The fourth industrial revolution. Crown Business.

Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. San Diego Law Review, 44, 745-772.

Taylor, L. (2019). The ethics of big data as a public good: Which public? Whose good? Philosophical Transactions of the Royal Society A, 374(2083), 20160126.

Terman, R. (2017). Islamophobia and media portrayals of Muslim women: A computational text analysis of US news coverage. International Studies Quarterly, 61(3), 489-502.

United Nations. (1948). Universal Declaration of Human Rights. United Nations General Assembly.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

Publisher: CLM Publishing Resources Malaysia

Data Availability Statement: All relevant data are within the manuscript and its Supporting Information files.