PERSONAL DATA PROTECTION IN ISLAMIC FINTECH ECOSYSTEM: TOWARDS A SHARĪʿAH-GOVERNED PRIVACY FRAMEWORK

Ahmad Abubakar*, Solauddeen Jibril Sahban and Ishaq Sahban Jibreel*****

Abstract

This paper examined the ethical and legal imperatives of personal data protection within the context of Islamic fintech, proposing a Sharīʿah-governed privacy framework as a normative response to the digital challenges of the contemporary Islamic financial ecosystem. The paper was premised on the observation that, while Islamic fintech platforms have advanced in providing Sharīʿah-compliant financial products, their data governance practices often lacked a correspondingly rigorous Islamic ethical foundation. Using doctrinal analysis and conceptual clarification, the paper explored foundational Sharīʿah principles of amānah (trust), ḥuqūq al-ʿibād (rights of individuals), maṣlaḥah (public interest), and ḍarar (harm) to assert that personal data constitutes a moral and legal trust whose misuse is a violation of both divine and societal obligations. The paper identified major risks in current Islamic fintech practices, including unauthorised access, algorithmic profiling, unethical monetisation, and limited Sharīʿah oversight in digital operations. It further demonstrated that these risks could not be fully addressed by conventional data protection frameworks such as the General Data Protection Regulations and Nigerian Data Protection Regulations, as these often lacked the theological and ethical depth intrinsic to Sharīʿah. In response, the paper proposed a comprehensive Sharīʿah-compliant data governance model incorporating Digital Sharīʿah Supervisory Boards, Ethical Impact Assessments, and the application of Islamic legal maxims within platform policies. The framework also emphasized user empowerment and cross-jurisdictional harmonisation grounded in Islamic legal epistemology. This paper contributed to the development of an ethically sound, spiritually coherent, and operationally practical model of data protection. It concluded that effective personal data governance in Islamic fintech was not only a technical necessity, but a Sharīʿah obligation aimed at preserving human dignity, justice, and trust in the digital age.

Keywords: Personal Data Protection, Islamic Fintech Ecosystem, Shari‘ah-Compliance, Privacy Framework, Shari‘ah Ethical Concern

1.0 Introduction

In the era of digital transformation, financial technology (fintech) has emerged as a disruptive force redefining global financial services. With the expanding intersection between technology and Islamic finance, a new sector i.e., Islamic fintech,has taken shape, combining Sharīʿah-compliant financial innovation with digital efficiency. This sector is experiencing exponential growth, particularly in Muslim-majority countries and among ethically conscious investors.

[1] According to the Global Islamic Fintech Report 2024/25,[2] the global Islamic-fintech market was estimated at USD 161 billion in the 2023/24 cycle, representing approximately 1.4% of the total fintech market, based on transaction volumes and assets under management. The Report projects continued growth, with a forecast that the market will reach USD 306 billion by 2028 under a compound annual growth rate (CAGR) of 13.6%.[3] For 2025, the market is projected to continue its strong growth trajectory.[4] Using the compound annual growth rate (CAGR) of 13.6% provided in the Global Islamic Fintech Report 2024/25, the estimated market size for 2025 would be approximately USD 183 billion.[5] This projection is derived from the stated CAGR and the 2023/24 base figure, as the report forecasts the market to reach USD 306 billion by 2028.[6] Yet, while Islamic fintech has demonstrated potential in enhancing financial inclusion and market accessibility, it also brings forth novel legal and ethical challenges, especially in the area of personal data protection.

* Associate, Shehu Wada SAN and Co., Abuja, Nigeria ahmedbuba19@gmail.com 08146515644
** School of Postgraduate Studies, International Islamic University in Madina, sahban14@gmail.com
*** School of Postgraduate Studies, International Islamic University in Madina, jibishsah@gmail.com
[1] Global Islamic Fintech Report 2024/25, cited in 'Islamic fintech and our emerging role', *Dawn.com* (8 September 2025) https://www.dawn.com/news/1940431 accessed 27 November 2025
[2] Global Islamic Fintech Report 2024/25, *Executive Summary*, SalaamGateway (2024) https://salaamgateway.s3.us-east-2.amazonaws.com/special-coverage/islamic-fintech-2024/GIFT%202024-25%20Executive%20Summary.pdf?utm_source=chatgpt.com accessed 27 November 2025
[3] Dinar Standard and Elipses, Global Islamic Fintech Report 2024/25 (Qatar Financial Centre, 2025) https://www.qfc.qa/-/media/project/qfc/qfcwebsite/documentfiles/research/global-islamic-fintech-report-2024-25.pdf accessed 29 June 2025
[4] Ibid,
[5] ibid,
[6] ibid,

Islamic fintech platforms rely heavily on data-driven technologies including application programming interfaces (APIs), artificial intelligence (AI), cloud computing, and biometric identification to deliver services such as *robo*-advisory (*e.g., Wahed Invest*), crowdfunding (*e.g., Ethis*), and digital banking (*e.g., Insha and TakafulTech*).[7] These technologies, although efficient, introduce complex risks to consumer privacy, particularly in the absence of uniform Islamic standards governing the acquisition, use, and storage of personal data.[8]

From the perspective of Islamic jurisprudence (fiqh), personal data is not merely an economic asset but a trust (*amānah*) that must be preserved and protected. The Qurʾān commands: "O you who believe! Do not enter houses other than your own without first seeking permission"[9] and "Do not spy on one another*"[10]* which classical jurists interpreted as the foundation for the right to privacy (*khuṣūṣiyyah*). Al-Ghazālī regarded concealment of personal information as an extension of human dignity (*ʿirḍ*),[11] while Ibn Qudāmah and al-Shāṭibī linked transparency in data handling with the *maqāṣid al-Sharīʿah* (Objectives of Islamic Law), particularly the protection of life, intellect, and property.[12] Thus, the misuse or negligent management of personal data does not only raises issues of legal liability (*ḍamān*) but may also amount to moral breach of trust (*khiyānah*) in Islamic ethics.

Concurrently, secular data protection regimes such as the European General Data Protection Regulation (GDPR), Nigeria's Nigerian Data Protection Requlation, and Malaysia's Personal Data Protection Act (PDPA) have developed sophisticated rules governing consent, data minimization, and cross-border transfers. However, while these frameworks promote accountability and user rights, they often operate within a secular ethical paradigm, which may not fully align with Islamic notions of trust, divine

[7] ibid; also see Umar Munshi, 'The Rise of Islamic Fintech: Ethics, Regulation, and Innovation' *Islamic Finance News Journal* (2022) 14(3) 21–25
[8] Ibid,
[9] Qurʾān 24:27
[10] Qurʾān 49:12
[11] Al-Ghazālī, *Iḥyāʾ ʿUlūm al-Dīn* (Vol. 2, Dar al-Maʿrifah 2005) , 146–150
[12] Ibn Qudāmah, *al-Mughnī* (Vol. 4, Dar al-Fikr 1997) 142; al-Shāṭibī, *al-Muwāfaqāt fī Uṣūl al-Sharīʿah* (Vol. 2, Dar Ibn ʿAffān 1997) 305–308

accountability, and spiritual harm. This divergence invites the question: How can the principles of *Shari'ah* be operationalised in data governance structures within the Islamic fintech ecosystem? Studies on Islamic fintech address digital banking, sukuk, and contract governance,[13] while data protection research focuses on compliance and risk management.[14] However, few studies integrate *Shari'ah* principles into personal data governance, leaving a gap that this paper seeks to fill by bridging Islamic ethics and modern fintech data policies.

The paper benefits multiple stakeholders: regulators can align policies with *Shari'ah* ethics; fintech operators can design systems with ethical oversight; users and investors gain assurance that data is protected both legally and spiritually; and academics and policymakers receive a framework for further research and policy development. This paper explores the question by articulating a Sharīʿah-governed privacy framework for Islamic fintech. It bridges the gap between classical Islamic jurisprudence, contemporary data protection norms, and the practical needs of digital finance.

2.0 Conceptual Clarification of Terms

2.1 Personal Data

The term "personal data" has evolved into a central legal and technological concept in the modern digital economy. It refers to any information that relates to an identified or identifiable individual.[15] Under Article 4(1) of the General Data Protection Regulation (GDPR), personal data is defined as: "any information relating to an identified or identifiable natural person ('data subject')."[16] This includes names, email addresses, biometric identifiers, location data, financial details, and online behavioural profiles. The Nigerian Data Protection Regulation (NDPR) similarly defines personal data as data

[13] Regulation (EU) 2016/679 (GDPR) (2016); National Information Technology Development Agency, *Nigeria Data Protection Regulation* (2019)
[14] Muhammad Ayub, *Understanding Islamic Finance* (3rd edn, Wiley 2014) 145–162; Aliyu Ismail and Mohammad Hashim Kamali, 'Sharīʿah Compliance in Digital Finance' (2022) *Journal of Islamic Finance* 12(2) 34–50
[15] See Art. 1, Nigeria Data Protection Regulations
[16] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) art 4(1)

"relating to an identified or identifiable natural person," incorporating both direct and indirect identifiers.[17] While these definitions are technologically precise, they are rooted in secular legal constructs, where individual autonomy, consent, and harm are the dominant normative anchors.

From the perspective of Islamic law (Sharīʿah), however, personal data must be conceptualized within a broader spiritual and ethical framework. Islamic jurisprudence does not historically contain the term "data", yet analogical reasoning (*qiyās*) and public interest (*maṣlaḥah*) permit the extrapolation of traditional doctrines to contemporary realities. The classical Islamic legal system recognized the inviolability of private information, as part of the broader concept of *ḥuqūq al-ʿibād* (the rights of individuals) as enunciated in the relevant verses of the Book of Allah (SWT). The Qurʾān affirms that one's privacy and private matters are inviolable. For example: "Do not spy on one another"[18] prohibits invasive acquisition of information. Another verse, "Do not enter houses other than your own without seeking permission"[19] underlines the principle of consent and respect for private space.

Although the above verses reference physical spaces, contemporary Islamic scholars including Ibn ʿĀshūr and Mohammad Hashim Kamali have argued that these rulings extend to non-physical forms of privacy, such as one's thoughts, secrets, correspondences, and digital footprints.[20] In *Iḥyāʾ ʿUlūm al-Dīn*, al-Ghazālī equated unlawful exposure of someone's private affairs to theft of dignity and trust, framing information confidentiality as a matter of *amānah* (entrusted obligation).[21] Similarly, Ibn al-Qayyim regarded the concealment of private flaws and sensitive facts about others as part of the believer's moral and social duties.[22]

[17] Nigeria Data Protection Regulation (NDPR) 2019, s 1.3
[18] Qurʾān 49:12
[19] Qurʾān 24:27
[20] Ibn ʿĀshūr, *Maqāṣid al-Sharīʿah al-Islāmiyyah* (Dar al-Nafāʾis 2001) 218; Muṣṭafā Zarqāʾ, *Al-Madkhal al-Fiqhī al-ʿĀmm* (Vol. 2, Dār al-Fikr 1968) 948–950; Mohammad Hashim Kamali, *The Dignity of Man: An Islamic Perspective* (Islamic Texts Society 2002) 43–46
[21] Al-Ghazālī, *Iḥyāʾ ʿUlūm al-Dīn* (Vol. 3, Dar al-Maʿrifah 2005) 125–128
[22] Ibn al-Qayyim, *Iʿlām al-Muwaqqiʿīn* (Vol. 2, Dar Ibn al-Jawzī 2002) 142–144

Consequently, in the view of these writers, personal data within Sharīʿah may be defined as any piece of information,tangible or intangible,relating to an identifiable individual the misuse or unwarranted disclosure of which violates the trust (*amānah*), dignity (*ʿirḍ*), or security (*amn*) of the person in contravention of the principles of Sharīʿah. This definition integrates the *fiqhī* doctrines of *amānah, ḥuqūq al-ʿibād,* and *ḥifẓ al-ʿirḍ*, and goes beyond utilitarian or consent-based frameworks. It imposes on data handlers not just a contractual obligation, but a divine accountability (*taqwā*) to use or disclose information only within ethically sanctioned boundaries.

Therefore, unlike secular data definitions which rest on legal personhood and regulatory scope, the Islamic definition anchors data protection in the *maqāṣid al-Sharīʿah*, particularly the protection of *al-nafs* (life), *al-ʿaql* (intellect), *al-ʿirḍ* (honour/dignity), and *al-māl* (wealth).

2.2 Islamic Fintech: Definition, Features, and Juristic Foundations

The term "Islamic Fintech" is a fusion of two domains: Islamic finance and financial technology. Though contemporary in terminology, the underlying concepts trace their roots to centuries-old in Sharīʿah principles of commerce (*fiqh al-muʿāmalāt*) and innovation in financial instruments. However, the emerging landscape of digital Islamic financial services demands a precise and principled definition that aligns technological advancements with normative Islamic values.

Fintech is broadly defined as the use of technological innovation to enhance or automate the delivery of financial services.[23] When this innovation is embedded within Islamic finance principles, the result is termed Islamic fintech. According to the Islamic Fintech Alliance (IFA), Islamic fintech refers to technology-enabled innovation in financial services that is designed and operated in accordance with Islamic law (*Sharīʿah*), including its prohibitions on interest (*ribā*), excessive uncertainty (*gharar*), and

[23] DW Arner, *et al,* 'The Evolution of Fintech: A New Post-Crisis Paradigm?' *Georgetown Journal of International Law*(2016) 47(4) 1271–1319

investment in unlawful industries.[24] Similarly, Dinar Standard, in its 2023 Global Islamic Fintech Report, describes Islamic fintech as any digital financial solution or platform that serves Muslim consumers or institutions in a manner that is compliant with Sharīʿah rules.[25]These definitions, while operationally useful, require sharper juristic elaboration to address the normative frameworks that Islamic law imposes on financial relationships, digital contracts, and algorithmic governance.

From the Sharīʿah perspective, any financial activity whether analog or digital must comply with the five pillars of Islamic commercial law: prohibition of *ribā* (interest); avoidance of *gharar* (excessive uncertainty); exclusion of *harām* activities (alcohol, gambling, etc.); implementation of permissible contracts (e.g., *murābaḥah, mushārakah, ijārah*); and upholding of ethical values: transparency, fairness, and mutual consent.[26] Thus, in Islamic fintech, these principles are applied to digital contexts through mechanisms such as smart contracts embedded with Sharīʿah-compliant terms, AI-driven robo-advisory platforms offering only halal investment portfolios (e.g., Wahed Invest), Islamic crowdfunding platforms that fund halal enterprises based on profit-and-loss sharing (e.g., Ethis, Blossom Finance) and Blockchain-based zakāh and ṣadaqah distribution systems ensuring transparency and traceability.[27]

Sharīʿah Supervisory Boards (SSBs) are often engaged to issue *fatāwā* on digital product design, compliance standards, and the permissibility of specific financial structures used in coding contracts. However, it is worthy to note that, despite the growing use of Islamic fintech, scholars have expressed caution about two issues. Firstly, some platforms claim Sharīʿah compliance but merely replicate conventional finance structures (e.g., *murābaḥah* contracts mimicking interest-based credit) and lastly, the use of AI and big

[24] Islamic Fintech Alliance, 'What is Islamic Fintech?' https://www.islamicfintech.org accessed 25 June 2025
[25] Dinar Standard, *Global Islamic Fintech Report 2023* (DinarStandard & Elipses, 2023) 6–9
[26] Ibid,
[27] MD Bakar, *Fintech in Islamic Finance: Theory and Practice* (Amanie Media 2019) 51–75

data raises concerns about fairness, bias, and informed consent, especially in the absence of Islamic ethical oversight in algorithmic design.[28]

Thus, the conceptual scope of Islamic fintech must extend beyond financial compliance to include Sharīʿah-oriented data ethics, consumer protection, and purpose-driven innovation grounded in the *maqāṣid al-Sharīʿah*. Drawing from classical legal norms and contemporary scholarship, Islamic fintech may be defined as follows: A technology-driven financial solution or platform that operates in full conformity with the legal, ethical, and spiritual principles of Islamic law (Sharīʿah), ensuring that its instruments, processes, data practices, and market objectives reflect the prohibitions, permissions, and higher objectives (*maqāṣid*) of the Sharīʿah. This definition acknowledges not only regulatory compliance but also juristic supervision, ethical integrity, and systemic accountability i.e., attributes essential for a holistic Islamic fintech model.

2.3 Sharīʿah-Governed Privacy Framework

The notion of a "Sharīʿah-governed privacy framework" lies at the heart of reconciling Islamic jurisprudence with contemporary data protection regimes. In secular legal systems, privacy frameworks are typically structured around principles of autonomy, consent, proportionality, and harm prevention.[29] However, within Islamic law (*Sharīʿah*), the conception of privacy transcends individual autonomy to incorporate notions of divine trust (*amānah*), moral restraint, and social accountability before God (*taqwā*).[30] Therefore, any Islamic data protection regime must not only replicate regulatory safeguards but also embody the ethical-spiritual imperatives of Sharīʿah.

Legal systems such as the General Data Protection Regulation (GDPR) and the Nigerian Data Protection Regulation (NDPR) articulate privacy as a set of data subject rights: the right to access, rectification, erasure, portability, and informed consent.[31] While these

[28] Iqbal Asaria, 'Sharīʿah and Fintech Ethics: A Necessary Symbiosis' in Nabil Maghrebi and Abbas Mirakhor (eds), *Islamic Economic Institutions and the New Digital Era* (Routledge 2021) 198–210
[29] DJ Solove, 'Understanding Privacy' (Harvard University Press 2008) 84–103
[30] Ayman Shabana, 'Privacy in Islamic Legal Tradition' *Arab Law Quarterly* (2010) 27(2) 1–29
[31] GDPR art 15–21; NDPR Part II

rights protect individual liberty and data integrity, they are secular constructs, developed under philosophical assumptions rooted in Enlightenment liberalism and data utilitarianism.

In contrast, Sharīʿah's conception of privacy (*ḥuqūq al-khuṣūṣiyyah*) is rooted in: Revelation (waḥy), which identifies privacy as a divine right, Dignity (ʿirḍ), one of the maqāṣid al-Sharīʿah, and Trust (amānah), an ethical imperative in handling others' secrets and belongings. For example, the Qurʾān states: "Do not spy on one another…"[32] and "Indeed, Allah commands you to render trusts to whom they are due"[33] These verses, interpreted by scholars such as al-Qurṭubī[34] and al-Rāzī,[35] form the foundational basis for Islamic privacy obligations.

Moreover, Sharīʿah does not regard data as a neutral commodity but as a protected extension of the self i.e., analogous to wealth, blood, or honour. Mishandling personal information may be construed not merely as a civil tort but as a spiritual transgression (*ithm*) and breach of *ḥuqūq al-ʿibād*.[36] To conceptualise a Sharīʿah-compliant data governance system, the framework must rest upon five essential components:

i. *Amānah* (Trust): Data is treated as a moral trust held by a custodian, not as a commercial asset to be exploited.
ii. *Niṣf wa ʿAdl* (Fairness and Justice): Use of data must be proportionate, with equitable access and redress mechanisms.

[32] Qurʾān 49:12
[33] Qurʾān 4:58
[34] Al-Qurṭubī's tafsir, *Al-Jāmiʿ li-Aḥkām al-Qurʾān*, is primarily a jurisprudential tafsir, focusing on the legal rulings (*ahkām*) derived from the Qur'an. It systematically analyzes the verses in light of Shari'ah law, covering civil, criminal, and social obligations. Al-Qurṭubī combines linguistic analysis, explanations of variant readings, and discussions of Hadith supporting legal derivations. His work is valued for its comprehensive incorporation of fiqh perspectives, historical context, and practical guidance for jurists.
[35] Al-Rāzī's tafsir, commonly referred to as *Al-Tafsīr al-Kabīr* or *Mafātīḥ al-Ghayb*, is a comprehensive and rational tafsir. It emphasizes theological, philosophical, and exegetical reasoning, integrating logic, kalām (Islamic theology), and linguistic analysis. Al-Rāzī examines Qur'anic verses with attention to cosmology, ethics, and rational arguments, often addressing potential objections and differing scholarly opinions.
[36] Al-Qurṭubī, *Tafsīr al-Jāmiʿ li Aḥkām al-Qurʾān* (Vol. 16, Dar al-Kutub al-ʿIlmiyyah 2000) 333; Fakhr al-Dīn al-Rāzī, *Tafsīr al-Kabīr* (Vol. 29, Dar al-Fikr 1999) 249

iii. *Ḥifẓ al-ʿirḍ* (Protection of Honour): Preventing reputational harm or unlawful exposure of private details.

iv. *Maṣlaḥah* (Public Interest): Data may be used to promote public benefit, but not at the expense of individual dignity or consent.

v. *Taqwā and Iḥsān* (God-consciousness and Moral Excellence): Internal moral restraint is as vital as external legal enforcement.[37]

Thus, to these writers, a Sharīʿah-governed privacy framework may be defined as: A data protection system structured around the legal, ethical, and spiritual obligations of Islamic law, ensuring that all collection, storage, processing, and dissemination of personal data uphold the *maqāṣid al-Sharīʿah* particularly the sanctity of honour, trust, and divine accountability. This goes beyond secular legalism to integrate the spiritual dimension of privacy and lays the foundation for a comprehensive data protection regime aligned with both *Sharīʿah* compliance and technological innovation in fintech.

3.0 The Sharīʿah Foundations of Privacy and Data Protection

The legal bases of data protection in Islamic law can traced to the holy Qur'an, Sunnah as well as some doctrinal concepts which underpins data protection within the ambit of Sharīʿah law. Therefore, this subheading discusses these bases of protection in Islamic legal system.

3.1 Qurʾānic and Prophetic Foundations

Islamic law derives its primary ethical and legal authority from the Qurʾān and the Sunnah of the Prophet Muhammad (peace be upon him). Within these sources, the principle of privacy (*khuṣūṣiyyah*) is not merely a social courtesy but a divinely ordained right, interwoven with the broader Islamic concept of human dignity (*karāmah*), trust (*amānah*), and accountability (*masʾūliyyah*). These concepts underpin Islamic rulings on personal information, surveillance, consent, and disclosure.

[37] MH Kamali, *Maqāṣid al-Sharīʿah Made Simple* (International Institute of Islamic Thought 2008) 21–24

The Qurʾān clearly articulates the sanctity of private life in numerous verses. One of the most explicit is: *"*O you who believe! Do not enter houses other than your own until you have asked permission and greeted their inhabitants..."[38] This verse establishes the requirement of consent before entering a private domain. Classical exegetes such as al-Qurṭubī, al-Rāzī, and Ibn Kathīr interpreted this not only as a ruling on physical entry but also as a universal principle of informational privacy requiring permission before accessing what belongs to others.[39] Modern Islamic legal scholars argue that the verse lays the moral foundation for informed consent in data collection.[40]

Another critical verse is: *"*And do not spy on one another..."[41] The Arabic verb, *tajassasū* (translated "spy"), contained in the verse connotes deliberate attempts to uncover hidden matters.[42] Al-Ghazālī viewed this verse as a prohibition against unjustified surveillance, backbiting, and data disclosure.[43] According to Ibn ʿĀshūr, it includes all forms of unjust investigation, including modern analogues such as data mining, wiretapping, or cyber tracking, when done without necessity or public interest.[44]

In the *Sunan of Abū Dāwūd*, the Prophet said: "If a man peeps into your house without permission, and you throw a stone at him and put out his eye, you will not be blamed*."*[45] Although this ḥadīth relates to physical intrusion, the underlying ethical principle extends to unauthorized intrusion into one's informational privacy. Prophet SAW was also reported to have said ''There should be neither harm nor reciprocating harm.''[46] Scholars of *qawāʿid fiqhiyyah* (legal maxims) extrapolate from this ḥadīth the rule: "Harm must be eliminated" *(al-ḍarar yuzāl),* which is applicable to privacy breaches in the digital age.

---

[38] Qurʾān 24:27
[39] Al-Qurṭubī, *al-Jāmiʿ li Aḥkām al-Qurʾān* (Vol. 12, Dar al-Kutub al-ʿIlmiyyah 2000) 229; Fakhr al-Dīn al-Rāzī, *Tafsīr al-Kabīr* (Vol. 24, Dar al-Fikr 1999) 267; Ibn Kathīr, *Tafsīr al-Qurʾān al-ʿAẓīm* (Vol. 6, Dar Ibn Ḥazm 2000) 74
[40] MH Kamali - The Right to Life, Security, Privacy and Ownership in Islam (Islamic Texts Society, UK, 2008) 56–61
[41] Qurʾān 49:12
[42] See al-Qurtabi, n39
[43] Al-Ghazālī, *Iḥyāʾ ʿUlūm al-Dīn* Vol. 3, (Dar al-Maʿrifah 2005) 124
[44] Ibn ʿĀshūr, *Maqāṣid al-Sharīʿah al-Islāmiyyah* (Dar al-Nafāʾis 2001) 214–218
[45] Sunan Abū Dāwūd, 5153
[46] Sunan Ibn Mājah (Hadith 2340)

3.2 Doctrinal Concepts Underpinning Data Protection in Sharīʿah

The classical Islamic legal tradition developed an extensive jurisprudence (*fiqh*) of ethical responsibility, trust, harm prevention, and social justice. Notably, Islamic law does not explicitly mention "data" as a legal category. However, several core doctrines provide a strong foundation for Islamic data protection principles, especially within the fintech ecosystem. These will be discussed under this subheading.

The first concept is that of *amānah*. *Amānah* is one of the most central ethical principles in Islamic law. It refers to an entrusted obligation whose violation constitutes betrayal (*khiyānah*). The Qurʾān repeatedly invokes the concept of trust: "Indeed, Allah commands you to render trusts to whom they are due…"[47] Thus, Data collected by Islamic fintech platforms such asnames, biometrics and financial information constitutes a form of *amānah*. As such, misusing, misrepresenting, or failing to protect that data amounts to a breach of trust both legally and morally. Ibn al-Qayyim argued that every possession or secret delivered to another person is governed by the principle of *amānah*, even if not contractually formalised.[48]

The Prophet Muhammad (PBUH) further stated: *"*He who is not trustworthy has no faith*."*[49] Modern jurists such as Shaykh Wahbah al-Zuḥaylī and Taqi Usmani agree that data protection must be approached through the lens of *amānah,* making the platform operator a trustee (*amīn*) before God and society.[50]

The second concept is *Ḥuqūq al-ʿIbād* (The Rights of Human Beings). In Islamic jurisprudence, a distinction is drawn between: *Ḥuqūq Allāh* (rights of God, e.g. prayer, fasting), and *Ḥuqūq al-ʿIbād* (rights of individuals).[51] Violating the rights of humans, whether financial, reputational, or personal, has a graver implication, as violator must

[47] Qurʾān 4:58
[48] Ibn al-Qayyim, *Iʿlām al-Muwaqqiʿīn ʿan Rabb al-ʿĀlamīn* (Vol. 2, Dar Ibn al-Jawzī 2002) 108–112
[49] Musnad Aḥmad, 12512
[50] Wahbah al-Zuḥaylī, *al-Fiqh al-Islāmī wa Adillatuh* (Vol. 4, Dar al-Fikr 2006) 207–210; MT Usmani, *An Introduction to Islamic Finance* (Maktaba Ma'ariful Qur'an 2006) 183
[51] Ibid, 1

account for it on the Day of Judgment unless forgiveness is approved by the victim.[52][53] Personal data is increasingly viewed by modern scholars as falling within *ḥuqūq al-ʿibād*, meaning:

i. The data subject owns the right to their personal information.
ii. Any violation (e.g., unauthorized access, third-party sharing, profiling) may constitute a sin and legal offence.
iii. Legal remedies should ensure redress, compensation, and possibly *taʿzīr* (discretionary punishment) if public harm occurs.

This makes Sharīʿah more protective than Western legal traditions, which often reduce harm to contractual breach or statutory penalty, rather than spiritual transgression.

Additionally, the doctrine of *maṣlaḥah mursalah* refers to considerations of public interest not explicitly addressed by revelation, but consistent with *Sharīʿah* goals. Imam al-Ghazālī defined *maṣlaḥah* as: "The preservation of the ends of the *Sharīʿah*: religion, life, intellect, lineage, and property."[54] In the context of data governance, *maṣlaḥah* supports:

1. The collection and use of personal data when clearly beneficial (e.g., fraud prevention, public health, risk profiling)—provided safeguards are in place.
2. The balancing of privacy with legitimate needs, such as national security, Sharīʿah compliance verification, or financial integrity.

Yet, jurists such as al-Shāṭibī warned that *maṣlaḥah* must never override explicit prohibitions or cause greater harm.[55] Thus, using data for commercial or political purposes without consent violates the principle, even if claimed to be "beneficial."

[52] Al-Shahrastānī, *Nihāyat al-Iqdām fī ʿIlm al-Kalām* (Dar al-Maʿrifah 2002) 154
[53] This is unlike the right of Allah which can be forgiven by Allah as a result of *Istigfar*, good deeds or other reasons, not necessarily known by human being.
[54] Al-Ghazālī, *al-Mustaṣfā min ʿIlm al-Uṣūl* (Vol. 1, Dar al-Kutub al-ʿIlmiyyah 1993) 286
[55] Al-Shāṭibī, *al-Muwāfaqāt fī Uṣūl al-Sharīʿah* (Vol. 2, Dar Ibn ʿAffān 1997) 289–312

Lastly, the legal maxim "*al-ḍarar yuzāl*" (harm must be eliminated) is foundational. The Prophet (PBUH) said: "There shall be no harm nor reciprocating harm.*"*[56] In digital contexts, data breaches, identity theft, and emotional trauma are modern manifestations of *ḍarar*. Similarly, *gharar*, or excessive uncertainty, is prohibited in financial transactions.[57] Failure to disclose how user data is stored, shared, or monetized may introduce *gharar* and may make the contract or service ethically defective.

4.0 Risks of Data Misuse in Islamic Fintech Operations

The rise of Islamic fintech has introduced an innovative intersection of financial technology and Sharīʿah-compliant finance. However, with this growth comes an expanding array of data-related risks that threaten to undermine Shari'ah values particularly those of privacy (*khuṣūṣiyyah*), trust (*amānah*), and justice (*ʿadl*). This section examines key risks associated with personal data misuse in the Islamic fintech ecosystem, using both theoretical analysis and practical illustrations.

4.1 Unauthorised Access and Data Breaches

One of the most prevalent risks is unauthorised access to personal data.[58] This includes hacking, internal employee abuse, or inadequate security protocols that expose sensitive user information to third parties without consent. In a Sharīʿah context, such actions amount to clear violations of *amānah* and *ḥuqūq al-ʿibād*. The Qurʾān commands: "Do not betray the trust of Allah and the Messenger, and do not betray your mutual trusts knowingly."[59]

In fintech systems, such breaches often occur through:

i. Weak encryption protocols;
ii. Poor access control by staff;

[56] Sunan Ibn Mājah, 2340
[57] Ibn Nujaym, *al-Ashbāh wa al-Naẓāʾir* (Dar al-Kutub al-ʿIlmiyyah 1999) 85–90
[58] IFN Fintech, *Fintech and Data Privacy: A Muslim Consumer's Dilemma* (2021) https://www.ifnfintech.com accessed 25 June 2025
[59] Qurʾān 8:27

iii. Reliance on unregulated cloud services.

Thus, for instance, lack of end-to-end encryption and used third-party servers with insufficient privacy guarantees Islamic finance apps creates cyber insecurity.[60] Such practices not only breach user trust and data confidentiality, but also violate Sharīʿah requirements of *ḥifẓ al-ʿirḍ* (protection of dignity) and *ʿadālah* (justice).

4.2 Profiling and Algorithmic Bias

The use of artificial intelligence and big data in Islamic fintech enables user profiling for credit scoring, product marketing, and risk prediction. However, profiling algorithms can reinforce bias, particularly if built on discriminatory or opaque data sets. The Qurʾān explicitly warns: "Let not hatred of a people cause you to act unjustly. Be just: that is nearer to piety."[61]

Thus, unjust profiling contradicts the Islamic imperative for fairness (*ʿadl*) and non-discrimination. For example, if a platform denies a Muslim woman microfinance services due to location or ethnic background (even implicitly, through algorithmic inference), it violates the principle of universal dignity (*karāmah*) and can lead to systemic exclusion, despite operating under a Sharīʿah-compliant label. Recent studies by Dinar Standard[62] and Cambridge Islamic Finance Leadership Programme[63] highlight the risk of algorithmic injustice in Islamic robo-advisory platforms that cater to high-income earners while ignoring the *maṣlaḥah* of poorer users.

4.3 Monetisation of User Data without Consent

The commodification of user data where data is shared, sold, or monetised without informed consent is a serious Sharīʿah breach. This trend, inherited from the global tech industry, is now being replicated by some Islamic fintech startups, particularly those

[60] IFN Fintech, *Fintech and Data Privacy: A Muslim Consumer's Dilemma* (2021) https://www.ifnfintech.com accessed 25 June 2025
[61] Qurʾān 5:8
[62] Dinar Standard, *Global Islamic Fintech Report 2023* (DinarStandard & Elipses 2023) 14–18
[63] CIFLP, *Islamic Digital Ethics in Fintech* (Cambridge Islamic Finance 2022) 22–24

relying on ad-driven revenue or venture capital incentives. Sharīʿah jurists consider such practices to be a breach of:[64]

(a) Amānah, since users have not granted explicit authority;
(b) Gharar, as users are often unaware of what data is collected or how it is used;
(c) Ḍarar, as such disclosure can cause reputational or financial harm.

In classical *fiqh*, the unauthorised sale of a person's belongings, words, or likeness (e.g., a letter, testimony, or even personal secrets) was forbidden under the principle of *tasarruf fī māl al-ghayr* (unauthorised dealing in another's property).[65] By analogy (*qiyās*), user data is a non-tangible asset protected under this rule.

4.4 Weak Sharīʿah Oversight in Technical Implementation

While many fintechs maintain a Sharīʿah Advisory Board (SAB), their focus is often limited to financial instruments (e.g., *murābaḥah* or *ijārah* contracts), and not extended to data handling, algorithms, or digital infrastructure. This creates a serious compliance vacuum where:

- code is written by developers unfamiliar with Sharīʿah;
- data analytics are outsourced to secular firms; and
- privacy policies are copied from conventional apps without juristic vetting.

Such separation between Sharīʿah advisory and digital governance violates the objective (*maqṣad)* of integration, which mandates that all aspects of a business (not just its profits) must be Shari'ah-compliant.[66]

5. Towards a Sharīʿah-Governed Privacy Framework for Islamic Fintech

In light of the ethical principles, doctrinal concepts, and operational risks identified earlier, it becomes imperative to formulate a Sharīʿah-governed privacy framework that

[64] Ibid,
[65] Al-Kāsānī, *Badāʾiʿ al-Ṣanāʾiʿ fī Tartīb al-Sharāʾiʿ* (Vol. 6, Dar al-Kutub al-ʿIlmiyyah 2005) 130–132
[66] MD Bakar, *Sharīʿah Minds in Islamic Finance: An Inside Story of a Sharīʿah Scholar* (Amanie Media 2016) 201–204

guides Islamic fintech institutions in the digital age. Such a framework must combine legal enforceability, technological functionality, and theological legitimacy. Unlike secular data protection regimes that prioritize autonomy and compliance, an Islamic privacy framework must be anchored in *maqāṣid al-Sharīʿah*, particularly the protection of dignity (*ḥifẓ al-ʿirḍ*), trust (*amānah*), and public welfare (*maṣlaḥah*). The framework should contain the following key principles and structural elements orchestrated below.

5.1 Ethical Foundations of the Framework

The ethical vision of Islamic data governance should rest on the following interrelated principles:

1. *Taqwā* (God-Consciousness): All actors in the data ecosystem—developers, fintech platforms, regulators, and users—should act with awareness that Allah is watching. The Qurʾān says: *"And Allah is ever, over all things, an Observer."*[67] This transcends mere legal compliance.
2. *Amānah* (Trust): As discussed earlier, data entrusted to a platform must be treated as a moral and legal trust. Misuse constitutes betrayal (*khiyānah*).
3. *ʿAdālah* (Justice): All data practices from collection to deletion must avoid discrimination, bias, or harm.
4. Sharīʿah Integration: Privacy is not an external regulatory imposition but a core Sharīʿah requirement that should be built into the design of digital services (Sharīʿah-by-design).
5. Public Interest (*Maṣlaḥah*): Where data use benefits the public (e.g. combating fraud or zakāh distribution), it should be permissible—subject to safeguards.

[67] (Qurʾān 33:52)

5.2 Institutional Elements of a Sharīʿah-Governed Privacy Framework

To operationalize the above principles, the following components are essential:

A. Digital Sharīʿah Supervisory Boards (DSSBs)

Unlike traditional SABs which only review financial contracts, DSSBs should:

6. Audit fintech data collection and usage protocols
7. Review privacy policies from an Islamic perspective
8. Ensure compliance with *amānah*, consent, and harm principles
9. Engage in fatwā issuance regarding ethical data innovations (e.g., biometrics, blockchain IDs)

DSSBs should include Islamic legal scholars, data scientists, and cybersecurity experts working synergistically..

B. Ethical Impact Assessments (EIAs)

Before launching any data-intensive service, an Islamic Ethical Impact Assessments should be conducted, evaluating:

(i) Whether the data collected is necessary (*ḍarūrī*) or superfluous (*kāmilī*)
(ii) Whether consent is informed and freely given
(iii)Whether data retention periods are justified under *maqāṣid* principles

This concept builds upon the secular model of Data Protection Impact Assessments (DPIAs), but infuses it with Sharīʿah ethics.

C. Data Governance Policies Based on Islamic Legal Maxims

Internal platform policies should reflect major *qawāʿid fiqhiyyah* (Islamic legal maxims) after the Arabic phrase, such as:

a) *Al-ḍarar yuzāl* (Harm must be eliminated)
b) *Al-ʿādah muḥakkamah* (Custom is a basis for judgment)

c) *Al-yaqīn lā yazūlu bi al-shakk* (Certainty is not overruled by doubt)

These principles can guide decisions on data sharing, breach response, and anonymisation techniques. Thus, for instance, the practical implementation of Islamic data governance principles necessitates the adoption of robust encryption technologies and stringent access control mechanisms to mitigate harm. This is in accordance with the Sharīʿah maxim *al-ḍarar yuzāl* (harm must be eliminated). Furthermore, in accordance with the maxim of *al-ʿādah muḥakkamah* (custom is an authoritative source of law) data privacy frameworks should be harmonized with prevailing legal standards and sociocultural norms. Additionally, the establishment of clear, consistent, and transparent security protocols is imperative to ensure reliability and foster trust, in line with the legal maxim *al-yaqīn lā yazūlu bi al-shakk* (certainty is not overruled by doubt).

D. User Empowerment Tools (UETs)

Empowering users with:

- Granular consent options (per action, per dataset)
- Sharīʿah-compliant data rights portals (e.g., for data erasure, opt-outs, and rectification)
- Access to spiritual guidance on digital behaviour, such as reminders of Qurʾānic principles while navigating platforms

5.3 Comparative Advantage over Secular Frameworks

Unlike GDPR, which is often reactive and rights-based, a Sharīʿah-governed privacy framework is:

i. Proactive, emphasizing virtue (*iḥsān*) and responsibility (*masʾūliyyah*)
ii. Value-oriented, aiming at ethical excellence rather than minimal compliance
iii. Community-aware, integrating public good and theological accountability

This framework has the potential to reshape global privacy discourse by offering a spiritually enriched and socially conscious model that resonates with both Muslims and values-driven innovators.

6.0 Policy Recommendations and Best Practices

In order to ensure that Islamic fintech platforms protect personal data in accordance with Sharīʿah principles, while also complying with national and international data protection standards, a set of comprehensive policy recommendations and best practices is needed. These recommendations must integrate the ethical-legal insights from Sharīʿah jurisprudence with operational and regulatory frameworks found in the fintech industry.

The goal is to institutionalise Sharīʿah governance in data protection while enabling innovation and compliance. The following are strategic recommendations addressed to Islamic fintech firms, regulators, and Sharīʿah supervisory boards.

6.1 For Islamic Fintech Platforms

A. Establish Dedicated Sharīʿah-Compliant Data Governance Protocols

Islamic fintech companies must go beyond generic data protection statements by:

2.0 Drafting Sharīʿah-specific privacy policies, explicitly referencing Islamic legal principles (e.g., *amānah*, *ḥuqūq al-ʿibād*)

3.0 Designing internal controls to avoid unlawful data sharing, algorithmic bias, and consent violations

4.0 Aligning all third-party data processing contracts with Sharīʿah values and juristic approval

For example, a fintech startup offering *murābaḥah*-based credit must ensure that user income and expenditure data—collected during risk profiling—is not reused for unauthorised commercial gain.[68]

B. Integrate Sharīʿah Audits into Technology Development

i. Sharīʿah audit teams must include technologists and IT professionals trained in Islamic ethics.
ii. Platforms should conduct Sharīʿah-compliant DPIAs before launching any service involving personal or biometric data.
iii. *Digital ijtihād* (juristic reasoning for new technologies) should be institutionalised through joint Sharīʿah-IT task forces.

This avoids the danger of "form-over-substance" compliance, where financial products are Sharīʿah-compliant but their digital infrastructure is ethically negligent.

C. Provide Ethical User Education

a) Platforms should educate users about their Sharīʿah-based data rights and obligations.
b) Notifications should cite Qurʾānic principles when collecting sensitive data, e.g., "Your information is an *amānah* (trust) and will only be used with your consent."
c) User dashboards should include "ethical consent" settings and a record of donations (*ṣadaqah*) facilitated via data-enabled Islamic apps.

6.2 For Regulators and Policymakers

A. Formulate Islamic Data Protection Standards

International and National Islamic finance authorities (e.g., AAOIFI, IFSB, or country-specific Sharīʿah councils) should:

[68] Taqi Usmani, *An Introduction to Islamic Finance* (Maktaba Maʿariful Qur'an 2006) 190–193

a) Issue Sharīʿah-based data governance standards, integrating fiqh principles into regulatory compliance.
b) Require Islamic fintechs to conduct Ethical Impact Assessments (EIAs).
c) Provide licensing guidance for platforms using sensitive data technologies like AI, blockchain, and biometrics.

Such guidelines can complement existing laws like the NDPR in Nigeria, the GDPR in the EU, or the PDPL in Saudi Arabia, while anchoring them in the *maqāṣid* framework.[69]

B. Encourage Cross-Jurisdictional Harmonisation

Islamic fintech often operates cross-border, but inconsistent regulations on data pose a challenge. Regulators should:

a) Facilitate Sharīʿah-compliant mutual recognition agreements (MRAs) on data privacy standards
b) Promote regional sandboxes for testing Sharīʿah-governed privacy protocols (e.g., ASEAN, GCC, OIC)\

6.3 For Sharīʿah Supervisory Boards (SSBs)

A. Expand the Scope of Sharīʿah Governance

SSBs must move beyond vetting financial contracts and address:

a) Data lifecycle integrity: from collection, storage, processing, to disposal
b) Algorithms and artificial intelligence
c) Digital marketing practices and behavioural nudges
d) Biometric and location tracking ethics

They must review source codes, app permissions, and consent flows—not just *murābaḥah* clauses.

[69] Nigeria Data Protection Regulation 2019; Saudi Personal Data Protection Law 2021; European GDPR 2018

B. Issue Ethical Fatāwā on Emerging Data Use Cases

Fatāwā must address:

a) Whether facial recognition for Know Your Customer violates *ḥuqūq al-ʿibād*
b) Whether behavioural profiling in halal investment apps infringes on privacy
c) Whether cloud data storage abroad complies with *amānah* obligations

These rulings should be based on *ijtihād al-jamāʿī* (collective reasoning) involving legal, technical, and ethical specialists.

7. Conclusion

The exponential growth of Islamic fintech in recent years has raised critical ethical and legal questions concerning personal data governance. While these platforms strive to deliver Sharīʿah-compliant financial services, their handling of user data often remains under-examined. This paper addresses this gap by constructing a Sharīʿah-governed privacy framework rooted in classical jurisprudence, Qurʾānic ethics, and contemporary digital realities. Through an extensive analysis of Sharīʿah sources, it has been demonstrated that the Islamic tradition provides a robust foundation for privacy, grounded in concepts such as *amānah* (trust), *ḥuqūq al-ʿibād* (rights of individuals), *maṣlaḥah* (public interest), and the imperative to eliminate *ḍarar* (harm). These principles mandate the protection of personal data as both a moral obligation and a legal duty, transcending the proceduralism of secular data protection regimes.

The discussion of risks including unauthorised access, algorithmic bias, data monetisation, and weak Sharīʿah oversight revealed that Islamic fintech platforms are vulnerable to the same exploitative tendencies as their conventional counterparts. Yet, the ethical accountability imposed by Sharīʿah is deeper and more comprehensive, binding stakeholders not only to users and regulators, but also to God (*taqwā*) and the moral universe of Islamic law. To address these challenges, a model Sharīʿah-compliant privacy framework was proposed. This framework recommends establishing Digital Sharīʿah

Supervisory Boards, conducting Ethical Impact Assessments, embedding Islamic legal maxims into data governance policies, and educating users in ethical digital literacy. These measures would ensure that Sharīʿah compliance is not confined to the financial layer of fintech products but extends holistically to data, infrastructure, algorithms, and user experience.

Consequently, data protection in Islamic fintech is not a technical add-on but a Sharīʿah imperative. Protecting human dignity (*karāmah*), ensuring informed consent, eliminating harm, and preserving trust are essential objectives (*maqāṣid*) of Sharīʿah. As the digital economy continues to evolve, Islamic fintech must lead by example by offering a value-driven, spiritually anchored model of ethical data governance that resonates not only with Muslim consumers but with global discourses on digital justice.

The paper impacts regulators, fintech operators, and users. Regulators can align data protection laws with Shari'ah ethics, fintech developers can integrate ethical governance structures, and users gain assurance that their data is safeguarded. Stakeholders should implement Shari'ah-compliant audits, ethical training, and awareness campaigns to operationalize the framework effectively. Future studies could examine cross-jurisdictional integration of Shari'ah-compliant data governance, assess the effectiveness of Digital Shari'ah Supervisory Boards, and explore algorithmic accountability and AI ethics in Islamic fintech, contributing to a more globally relevant ethical fintech discourse.