Contemporary Fiqh Studies
Vol. 1, No. 1, 2026, pp. 179–198
https://doi.org/10.66277/cfs.v1i2.416

Elkuator Research & Publication
E-ISSN: 3163-9364
https://e-journal.elkuator.com

Digital Privacy and Personal Data Protection: A Contemporary Maqasid Perspective on Informational Dignity

Bagas Lukito,[1] Sutrisno Hadi,[1] and Ikhwan Fikri[1]

[1]Department of Comparative Islamic Jurisprudence, UIN Raden Fatah, Palembang, Indonesia
Corresponding author bagaslukito23@gmail.com

Abstract

Digital privacy represents a contemporary issue within Islamic jurisprudence, necessitating renewed legal reasoning grounded in the objectives of Sharia. This study examines the relationship between digital privacy under Indonesian Law No. 27 of 2022 on Personal Data Protection (UU PDP) and the Islamic legal principle of *ḥifẓ al-'irḍ*, traditionally associated with the protection of honor and reputation. Employing a qualitative juridical approach, the study utilizes comparative doctrinal and conceptual analysis within a maqasid-based framework. A structured comparative analysis is applied to identify convergences and divergences between the two frameworks regarding consent, restrictions on information access and use, accountability, harm prevention, normative authority, and enforcement. The findings reveal substantial functional convergence in their protective objectives, particularly regarding consent, limitations on information access, custodial responsibility, and harm prevention, while demonstrating differences in their normative foundations and enforcement mechanisms. Building on this comparison, the study proposes "informational dignity" as a contemporary interpretive category developed through a maqasid-based reconstruction of *ḥifẓ al-'irḍ*. This category extends the protection of human honor to digital contexts. The study contends that this reconstruction offers an Islamic normative foundation for addressing emerging challenges in digital privacy, including algorithmic profiling and AI-driven data inference.

Keywords
digital privacy; personal data protection; maqasid sharia; informational dignity; Islamic jurisprudence

Article History
Received:
3 July 2026
Revised:
17 October 2026
Accepted:
21 October 2026

Introduction

The transition to a data-driven global economy has made personal information one of the most valuable—and simultaneously one of the most vulnerable—assets of the twenty-first century. Across jurisdictions, the exponential growth of e-commerce, social media, and cloud computing has been accompanied by an equally exponential rise in data breaches, identity theft, and unauthorized surveillance. This surge has prompted more than one hundred countries to adopt comprehensive data protection legislation, modeled to varying degrees on the European Union's General Data Protection Regulation (GDPR).[1] For contemporary fiqh, this transformation is not

[1] Graham Greenleaf, "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills," *UNSW Law & Justice Research Series* 48, no. 181 (2023): 1-6; Sinta Dewi Rosadi et al., "Indonesia's Personal Data Protection Bill, 2020: Does It Meet the Needs of the New Digital Economy?," *International Review of Law, Computers & Technology* 37, no. 1 (2023): 78–90.

© The Author(s) 2026. Published by Elkuator Research & Publication. This is an open access article licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted reuse, reproduction, and distribution in any medium, provided the original work is properly cited.

merely a regulatory phenomenon but a juristic one: digital data did not exist as an object of legal reasoning for classical jurists, and its unauthorized collection, storage, and disclosure therefore constitute a *nāzilah*—a new occurrence for which no explicit textual ruling exists and which demands fresh ijtihad grounded in the maqasid sharia rather than in the literal texts alone.[2] Treating digital privacy as fiqh *al-nawāzil*, rather than as a subject external to Islamic law awaiting comparison with statute, reframes the present inquiry: the question is not only how Indonesian positive law regulates personal data, but also how contemporary fiqh reasoning itself must evolve to address it.

Within the Muslim world, this juristic tension is further complicated by a distinctive normative challenge: states that identify constitutionally or culturally as Islamic must reconcile an imported, secular regulatory framework with an indigenous fiqh tradition. This tradition has historically addressed privacy, honor, and the protection of personal secrets through doctrines such as *tajassus* (spying or snooping), *ghībah* (backbiting), and *amānah* (trustworthiness), rather than through statutory law.[3] A growing body of contemporary fiqh scholarship has begun to engage this challenge directly, applying maqasid reasoning to issues of cyber privacy and AI-driven surveillance. Scholars argue that digital ethics cannot be adequately addressed by analogical reasoning (*qiyās*) based solely on classical cases but require a systemic, maqasid-based reconstruction capable of generating genuinely new applications.[4] In Indonesia, this tension became tangible following a series of large-scale data breaches affecting the Election Commission (KPU), the social security agency (BPJS Kesehatan), and major e-commerce platforms. These incidents exposed the personal records of tens of millions of citizens and accelerated the legislature's adoption of Law No. 27 of 2022 on Personal Data Protection (UU PDP), a statute framed in the idiom of administrative law and individual consent rather than the vocabulary of Islamic legal ethics.[5]

Against this background, the study is guided by three research questions. First, how does Law No. 27 of 2022 structure the rights of data subjects and the obligations of data controllers, and on what normative premises does this structure rest? Second, how does the classical principle of *ḥifẓ al-ʿirḍ*, understood within the framework of maqasid sharia, address the protection of personal secrets, reputation, and private space, and to what extent can this principle be extended to digital information? Third, what does the comparison between these two frameworks reveal about the capacity of contemporary fiqh to generate a determinate, operative framework for informational dignity, rather than merely providing a retrospective moral

[2] Sherin Kunhibava et al., "Selected Issues in the Use of RegTech in the Islamic and Conventional Financial Markets," *Journal of Islamic Accounting and Business Research* 15, no. 5 (2024): 746–61.
[3] Zlatan Morić et al., "Protection of Personal Data in the Context of E-Commerce," *Journal of Cybersecurity and Privacy* 4, no. 3 (2024): 731–61.
[4] Misbahun Nidhom and Ali Murtadho, "Does Islam Protect Digital Privacy? An Islamic Studies Approach to Personal Data Protection," *Al-Afham: Journal of Islamic Studies* 2, no. 2 (2025): 107–28; Moufid El-Khoury and Saleh Albarashdi, "Navigating the Privacy Landscape of Healthcare-Driven AI in the Middle East: Case Studies from Oman, Qatar, and Saudi Arabia," *Social Sciences and Humanities Open* 11 (2025): 1–10..
[5] Eryna Syahadatina Badar et al., "Personal Data Protection Policy in Law Number 27 of 2022 in the Perspective of Positive Law and Islamic Law," *Hukum Islam* 23, no. 1 (2023): 61–74.

endorsement of positive law? These questions place the study at the intersection of statutory analysis and the reconstruction of legal doctrine, explaining why the analysis proceeds through a structured comparative framework rather than a single analogy to a classical case. Scholarly, it provides an Indonesia-specific, doctrinal-level account that the existing literature lacks and demonstrates how maqasid reasoning can function as a generative method for contemporary fiqh. Practically, it offers religious scholars, fatwa institutions, educators, and regulators a shared vocabulary through which the protection of personal data can be explained to a Muslim-majority public as a matter of both legal compliance and moral responsibility. This article's primary contribution is both conceptual and comparative. It argues that while UU PDP and *ḥifẓ al-ʿirḍ* substantially converge at the level of operative norms—such as consent, purpose limitation, data minimization, and accountability—they diverge in their legitimating foundations and enforcement logic. This divergence allows *ḥifẓ al-ʿirḍ* to be reinterpreted as a contemporary maqasid framework for informational dignity.

Previous Studies

Scholarship on personal data protection has largely developed along four intersecting lines of inquiry. The first strand offers doctrinal, positive law analyses of Law No. 27 of 2022, examining its consent mechanisms, data subject rights, and administrative criminal sanctions primarily as a self-contained regulatory system.[6] These studies provide a solid technical account of the statute but generally set aside questions regarding its ethical or religious foundations. A second strand situates the UU PDP comparatively against the GDPR and neighboring jurisdictions, demonstrating that Indonesia's dual administrative-criminal enforcement model approximates the European civil law tradition, though it still lags in institutional independence.[7] This comparative literature is analytically valuable for benchmarking procedural robustness; however, it treats data protection as a purely secular-administrative construct, leaving the normative question of why personal data warrants protection largely unexplored. A third, more recent strand engages Islamic legal sources directly, arguing that data protection can be grounded in maqasid concepts such as *ḥifẓ al-khuṣūṣiyyah* (protection of privacy) or *sadd al-dharīʿah* (blocking the means to harm).[8] These contributions effectively demonstrate that Islamic ethics is not silent

[6] Rosadi et al., "Indonesia's Personal Data Protection Bill, 2020: Does It Meet the Needs of the New Digital Economy?"; Rina Shahriyani Shahrullah, Jinny Park, and Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment," *Hasanuddin Law Review* 10, no. 1 (2024): 1–20; Valerie Angel Simbolon and Vishnu Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and the European Union General Data Protection Regulation," *Publik: Jurnal Ilmu Administrasi* 11, no. 2 (2022): 178–90..

[7] Damian Eke and Bernd Stahl, "Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies.," *DISO* 3, no. 11 (2024): 1–23; Simbolon and Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and the European Union General Data Protection Regulation."

[8] Kukuh Pandu Wicaksana, Tahegga Primananda Alfath, and Heru Kuswanto, "Personal Data Protection in the Digital Era: A Maqasid Al-Shariah Perspective on Contemporary Legal Challenges," *Mizan: Journal of Islamic Law* 14, no. 1 (2026): 114–22; Utomo Setyo, "Personal Data Protection Through Law Number 27 Of 2022: Challenges of Cybercrime in The Era of Globalization and Digital," *Pena Justisia Media Komunikasi dan Kajian Hukum* 23, no. 3 (2024): 2967–75..

on privacy, drawing on Quranic prohibitions of *tajassus* (spying) and *ghībah* (backbiting), as well as the doctrine of *amānah* (trust). A fourth, emerging strand compares maqasid-based reasoning with AI governance and data regulation in Gulf jurisdictions, including Oman, Qatar, Saudi Arabia, and the UAE.[9] This literature offers a useful conceptual vocabulary for interpreting positive statutes as partial codifications of Islamic ethical principles, but its empirical focus on Gulf regulatory and technological contexts limits its direct applicability to Indonesia's distinct constitutional and socio-legal architecture.

However, these works tend to remain at the level of general ethical reflection, invoking maqasid as a broad legitimating framework rather than systematically mapping its specific doctrinal content, principle by principle, against the determinate provisions of a single statute such as the UU PDP. Two gaps emerge from these scholarly debates. First, no existing study systematically maps the specific normative framework of the UU PDP—its consent requirements, purpose limitation principle, custodial accountability duties, and sanctions regime—against the precise doctrinal content of *ḥifẓ al-ʿirḍ* as elaborated in classical and contemporary fiqh, rather than against maqasid al-sharia in the abstract. Second, the literature rarely examines the philosophical divergence between a rights-based, state-enforced regulatory model and a duty-based, divinely anchored ethical model, nor its implications for compliance culture in Muslim-majority societies. By constructing a structured comparative framework between UU PDP and *ḥifẓ al-ʿirḍ* across four categories—consent, scope, accountability, and enforcement—this study addresses both gaps, offering a granular doctrinal comparison that moves beyond the general ethical reflections of prior scholarship and beyond the Gulf-centric focus of comparative regulatory technology literature.

Beyond mere classification, a critical examination of the third and fourth strands reveals a significant limitation for a journal dedicated to contemporary fiqh: much of this scholarship treats maqasid sharia as a legitimizing vocabulary applied retrospectively to existing statutory provisions, rather than as a generative methodology for producing new fiqh rulings on genuinely novel digital phenomena—such as cyber *tajassus*, algorithmic profiling, cross-border data transfers, and AI-driven inference of private attributes from ostensibly anonymized data.[10] When contemporary fiqh scholarship does engage these phenomena directly, it tends to do so at the level of broad ethical principles rather than through detailed, provision-by-provision doctrinal reconstruction that would enable *ḥifẓ al-ʿirḍ* to function as an operative, rather than merely rhetorical, framework for digital governance. This juristic development—shifting from ethical reflection to doctrinal reconstruction—is the focus of the present study.

[9] Ezieddin Elmahjub, "Artificial Intelligence (AI) in Islamic Ethics: Towards Pluralist Ethical Benchmarking for AI," *Philosophy & Technology* 36, no. 4 (2023): 1–24; Amani Aloufi et al, "Legal Gaps, Islamic Ethics, and Digital Trust: Building a Regulatory Framework for Saudi E-Commerce Under Vision 2030," *Journal of Cultural Analysis and Social Change* 10, no. 4 (2025): 3860–80.
[10] Fatima Ali et al., "Islamic Ethics and AI: An Evaluation of Existing Approaches to AI Using Trusteeship Ethics.," *Philosophy & Technology* 38, no. 120 (2025): 1–34.

Research Methodology

Research Design

This study employs a qualitative normative legal approach,[11] using maqasid-based comparative doctrinal analysis within the Indonesian context. In this design, comparison and conceptual analysis serve not as separate methodologies but as complementary analytical techniques. Comparison examines the relationship between the UU PDP and *ḥifẓ al-ʿirḍ*, while conceptual analysis facilitates the reconstruction of categories, such as informational dignity, that are not explicitly articulated in either source. This approach is appropriate because the object of inquiry—the relationship between a positive statute and an Islamic legal doctrine—is conceptual and textual rather than behavioral, and therefore does not require field-based data collection.[12] The comparative method was chosen because it allows the two legal systems, Indonesian positive law and Islamic law, to be analyzed on equal doctrinal footing without privileging one framework as the interpretive standard for the other.[13]

Data Sources

The research was conducted over approximately five months, from February to June 2026, as desk-based library research at the Faculty of Sharia, Universitas Islam Negeri Raden Fatah, Palembang, Indonesia. Data for this study were drawn from both primary and secondary sources. Primary sources included the text of Law No. 27 of 2022 on Personal Data Protection; the 1945 Constitution of the Republic of Indonesia, particularly Article 28G, which guarantees the right to protection of the person, family, honor, dignity, and property; the Qur'an, notably Al-Hujurat 49:12 and Al-Nur 24:27–28; and classical works of usul fiqh and maqasid sharia. Secondary sources comprised thirty peer-reviewed journal articles, book chapters, and conference papers addressing personal data protection, digital privacy, and Islamic legal theory across Indonesia, the Gulf states, and the broader Muslim world.[14] Secondary sources were selected based on their relevance to personal data protection and Islamic ethics, publication in peer-reviewed outlets or recognized conference proceedings, and analytical relevance to the UU PDP and *ḥifẓ al-ʿirḍ*. Sources treating data protection solely as a technical or commercial matter, without legal or normative argumentation, were excluded from the analysis.

Data Analysis

The data were analyzed using qualitative document analysis combined with a comparative conceptual technique. The analysis began with an internal doctrinal

[11] Tunggul Ansari Setia Negara, "Normative Legal Research in Indonesia: Its Origin and Approaches," *Audito Comparative Law Journal* 4, no. 1 (2023): 1–9.
[12] Yati Nurhayati, Ifrani Ifrani, and M Yasir Said, "Metodologi Normatif dan Empiris dalam Perspektif Ilmu Hukum," *Jurnal Penegakan Hukum Indonesia* 2, no. 1 (2021): 1–20.
[13] Compare with Muannif Ridwan et al., "Approaches in Legal Research: An Introduction about Study Analysis of Western Law and Islamic Law," in *Proceedings of the Borneo International Conference on Education and Social Sciences* (European Alliance for Innovation, 2022).
[14] Nidhom and Murtadho, "Does Islam Protect Digital Privacy? An Islamic Studies Approach to Personal Data Protection."

reconstruction of each legal order, mapping the principles, rights, and obligations articulated in the UU PDP, and separately mapping the textual and juristic content of *ḥifẓ al-'ird* as a component of the *ḍarūriyyāt* (essential objectives) within maqasid al-shariah, following Auda's systems approach. This approach treats the maqasid not as a fixed classical list but as a dynamic framework capable of accommodating contemporary categories such as digital data.[15] The two reconstructions were then compared using a structured comparative framework organized around four analytical categories: consent, scope and purpose, accountability, and enforcement, to identify points of convergence and divergence. This interpretive procedure enables the study to move beyond descriptive juxtaposition toward an argument about the normative relationship between the two frameworks, while maintaining transparency and replicability for subsequent scholarly evaluation.[16]

Analytical Framework

The analytical framework guiding this study is based on two interrelated commitments. The first is the classical conception of maqasid sharia, which defines the objectives that provide Shariah with its rational coherence. These objectives are traditionally organized into a hierarchy of necessities (*ḍarūriyyāt*), needs (*ḥājiyyāt*), and refinements (*taḥsīniyyāt*). Within the doctrinal literature, the preservation of honor has been regarded either as a component of the preservation of lineage or as an independent objective; this study adopts the latter position for analytical purposes.[17] The second commitment is Jasser Auda's maqasid systems approach. Viewed through this approach, *ḥifẓ al-'irḍ* is not a static element in a closed list but rather a node within an open, self-renewing system capable of recognizing new forms of harm, with unauthorized data processing serving as a prominent example.[18] The concept of fiqh *al-nawāzil* provides the juristic framework for this theoretical perspective. *Nawāzil* are newly emerging cases that early jurists did not address, and their resolution has traditionally required a combination of textual evidence, analogy, public interest (*maṣlaḥah*), and the prevention of harmful means (*sadd al-dharī'ah*). Digital privacy fits precisely into this category because the subject of regulation—data that can be copied, aggregated, and inferred at scale—has no equivalent in Islamic classical jurisprudential manuals. These methods are applied collectively (*ijtihād jamā'ī*) by qualified scholars when the issue is of general concern.[19]

[15] Wicaksana, Alfath, and Kuswanto, "Personal Data Protection in the Digital Era: A Maqasid Al-Shariah Perspective on Contemporary Legal Challenges."
[16] Muhammad Ahmad Wathoni, "Sociocultural Dynamics of Islamic Legal Reform Across Muslim-Majority Countries: A Comparative Perspective," *Diktum: Jurnal Syariah dan Hukum* 23, no. 2 (2025): 214–31.
[17] Umami and Ghofur, "Human Rights in Maqāṣid Al-Sharī'ah Al-'Āmmah: A Perspective of Ibn 'Āshūr."
[18] Refer to Jasser Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach* (London: The International Institute of Islamic Thought, 2028).
[19] Kunhibava et al., "Selected Issues in the Use of RegTech in the Islamic and Conventional Financial Markets."

Research Approach

The study's fiqh methodology is specifically grounded in maqasid-based reasoning rather than classical usul fiqh derivation from textual sources alone. Since digital data protection is a *nāzilah* without direct textual precedent, the study does not proceed through *qiyās* to identify a single classical case. Instead, it adopts Jasser Auda's systems approach to maqasid sharia, which views the objectives of Sharia as a dynamic, cognitive system capable of generating new applications—such as *ḥifẓ al-ʿirḍ* understood as informational dignity—rather than as a fixed classical list. Accordingly, *ḥifẓ al-ʿirḍ* is treated in this study not merely as an interpretive lens external to the primary sources but as the operative doctrinal category through which the Quranic prohibitions of *tajassus* and *ghībah*, along with the doctrine of *amānah*, are systematized into a coherent framework comparable, provision by provision, with the UU PDP. Two limitations of the methodology should be acknowledged. First, because the study is doctrinal, it does not assess how data controllers, regulators, or religious communities actually behave; thus, its claims about the potential of *ḥifẓ al-ʿirḍ* to reinforce compliance are normative propositions rather than empirical findings.[20] Second, the comparison addresses fiqh at the level of a general maqasid-based framework and does not attempt a madhhab-by-madhhab survey of every ruling on privacy.

Analytical Procedures

The comparative procedure consisted of four steps. First, the provisions and principles of the UU PDP were extracted and classified under four analytical categories. Second, the textual bases and juristic elaborations of *ḥifẓ al-ʿirḍ* were collected from Quranic verses, Prophetic traditions, and secondary fiqh literature, then classified under the same categories. Third, each pair of entries was compared to determine whether it exhibited functional equivalence, partial overlap, or divergence in its legitimating foundation. Fourth, the resulting pattern of convergences and divergences was interpreted using Auda's systems approach to establish whether *ḥifẓ al-ʿirḍ* could be reconstructed as an operative framework. To enhance the credibility of the analysis, claims about the statute were directly tied to its text, claims about fiqh were linked to identifiable textual or scholarly sources, and the interpretive connections between the two were explicitly stated rather than implied.

Results

Following a comparative synthesis, the study's findings highlight two main aspects. The first finding demonstrates the normative framework of Law No. 27 of 2022, identifying the principles, rights, obligations, and sanctions through which the statute translates the constitutional guarantee of personal dignity into regulatory practice. The second finding reconstructs the doctrinal content of *ḥifẓ al-ʿirḍ* as a

[20] See Negara, "Normative Legal Research in Indonesia: Its Origin and Approaches"; Nurhayati, Ifrani, and Said, "Metodologi Normatif dan Empiris dalam Perspektif Ilmu Hukum."

contemporary maqasid-based framework for personal data privacy through the notion of informational dignity, tracing its textual foundations, supporting maxims, and its extension to digital information. Each finding was derived from the primary and secondary sources described in the preceding section and organized under the same analytical categories to facilitate subsequent comparison. The findings are presented in this order because the UU PDP provides clearer legal provisions that serve as a basis for interpreting the broader principles of *ḥifẓ al-ʿirḍ*. Table 1 summarizes the comparison between the two, followed by a discussion of how they differ and complement each other in understanding privacy, its protection, and the responsibilities involved.

The Normative Architecture of Personal Data Protection

Law No. 27 of 2022 represents Indonesia's first comprehensive, sector-neutral personal data protection statute, replacing a fragmented regime previously scattered across sectoral regulations on electronic information, health, and banking. The statute is anchored in the constitutional guarantee of Article 28G of the 1945 Indonesian Constitution, which recognizes the right of every person to protection of the self, family, honor, dignity, and property.[21] The UU PDP operationalizes this constitutional guarantee through a set of processing principles—lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability—that closely mirror the structure of the GDPR, though adapted to Indonesia's administrative law tradition.[22] Personal data controllers and processors are obligated to obtain explicit consent from data subjects prior to collection and processing, except in narrowly defined circumstances such as the fulfillment of contractual or legal obligations. Beyond the processing principles, UU PDP grants data subjects a set of enforceable rights, including the right to obtain clear information about the identity of the data controller, the legal basis for processing, and the purposes of personal data collection and processing; the right to complete, update, or correct inaccurate personal data; the right to access and obtain a copy of their personal data; and the right to request the termination of processing, deletion, or destruction of personal data, subject to statutory exceptions.[23]

Institutionally, the law establishes a supervisory body responsible for overseeing compliance. It also distinguishes between administrative sanctions, ranging from written warnings to temporary suspension of processing activities and administrative fines, and criminal sanctions for the unlawful acquisition, disclosure, or falsification of personal data. These criminal penalties include several years of imprisonment and substantial fines for corporate offenders.[24] Comparative studies suggest that this dual administrative and criminal enforcement framework places Indonesia closer to the European civil law model than to the more litigation-driven and sector-specific approach of the United States, although Indonesia continues to lag behind the

[21] Republik Indonesia, "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945" (1945). Art. 28G.
[22] Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi" (Jakarta: Sekretariat Negara Republik Indonesia, 2022), 4-6.
[23] Republik Indonesia., "Undang-Undang Nomor 27 Tahun 2022," 16.
[24] Republik Indonesia., "Undang-Undang Nomor 27 Tahun 2022," 57–65.

GDPR in terms of institutional independence and cross-border enforcement capacity.[25] The rationale behind this legislative framework is best understood as a response to two converging pressures: domestic pressure arising from repeated high-profile data breaches that have eroded public trust in digital platforms, and external pressure stemming from the GDPR's extraterritorial reach and the requirements of cross-border data flow agreements. Together, these pressures made the enactment of a dedicated data protection law increasingly necessary for Indonesia's continued integration into the global digital economy.[26]

Two additional features of the statute warrant emphasis because they shape the comparison that follows. The first is its distinction between general and specific personal data. The latter category encompasses information such as health data, biometric and genetic data, criminal records, children's data, and personal financial data. This classification reflects the legislature's recognition that certain types of information pose a greater risk of serious harm if exposed and therefore warrant a higher level of protection.[27] The second feature is the statute's enumeration of lawful bases for processing personal data. Explicit consent is one such basis, alongside the performance of a contract, compliance with a legal obligation, the protection of vital interests, the performance of a public interest task, and the pursuit of legitimate interests. Thus, although consent remains central to data protection, it is not the sole legal basis for lawful processing.[28]

Regarding data controller obligations, the statute requires controllers to demonstrate the lawfulness of their processing activities, maintain the security and confidentiality of the personal data they hold, prevent unauthorized access, and notify both data subjects and the supervisory authority in writing of any failure to protect personal data within three times twenty-four hours. Controllers that process specific personal data or engage in large-scale monitoring of data subjects are also required to appoint a data protection officer.[29] These obligations are particularly significant to the present study because they demonstrate that the statute does not rely on consent as its sole safeguard. Rather, it establishes an ongoing duty of care for entities entrusted with personal data. As the second finding demonstrates, this obligation resonates with the fiduciary logic of *amānah*.

The statute also regulates the transfer of personal data beyond Indonesian jurisdiction, permitting such transfers only when the recipient jurisdiction provides an equivalent or higher level of protection or, in the absence of such protection, when adequate and binding safeguards are in place or the data subject has given consent. It also provides for a supervisory institution accountable to the President, while leaving the details of its institutional form, powers, and independence to subsequent regulations.[30] Taken together, these provisions establish a framework

[25] Simbolon and Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and the European Union General Data Protection Regulation."
[26] Shahrullah, Park, and Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment."
[27] Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022," Art. 4.
[28] Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022," Art. 20.
[29] Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022," Arts. 46 and 53.
[30] Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022," Arts. 56 and 58–61.

characterized by detailed procedural requirements and a graduated approach to data protection risks, although its institutional enforcement mechanisms are still evolving. Comparative research on data protection in emerging digital economies further suggests that jurisdictions adopting GDPR-influenced frameworks tend to prioritize procedural compliance, consent documentation, data protection impact assessments, and breach notification over substantive ethical inquiry into the underlying reasons for protecting personal data.[31] This normative gap—the absence of an explicit account of why personal data warrants protection beyond its instrumental economic value—creates the analytical space for engaging with the Islamic legal principle of *ḥifẓ al-ʿirḍ*, which is examined in the following section.

From Ḥifz al-ʿIrḍ to Informational Dignity

Classical maqasid theory identifies five essential objectives (*al-ḍarūriyyāt al-khams*) that the Sharia seeks to preserve: religion (*ḥifẓ al-dīn*), life (*ḥifẓ al-nafs*), intellect (*ḥifẓ al-ʿaql*), lineage (*ḥifẓ al-nasl*), and property (*ḥifẓ al-māl*). A substantial body of classical and contemporary jurisprudence recognizes the preservation of honor (*ḥifẓ al-ʿirḍ*) either as an integral dimension of the preservation of lineage or as an independent sixth objective. This position rests on the understanding that an individual's reputation, privacy, and social standing are essential to human dignity, just as life and property are, and that their violation through slander, exposure, or unauthorized disclosure constitutes harm that Islamic law is obligated to prevent.[32] Jasser Auda's systems-based reconstruction of maqasid theory further supports this expansive understanding. He argues that the classical objectives should not be treated as a fixed and closed list but rather as a dynamic system capable of generating new applications in response to contemporary circumstances, including the protection of information and personal data against threats that were unknown to classical jurists.[33]

The textual foundations of *ḥifẓ al-ʿirḍ* are derived primarily from the Qur'an and Hadith. Al-Hujurat 49:12 instructs believers to avoid excessive suspicion and prohibits *tajassus* (spying or intrusive surveillance) and *ghībah* (backbiting or disclosing information about someone that they would not wish to have revealed). The verse further likens backbiting to consuming the flesh of one's deceased sibling, underscoring the gravity of violating another person's dignity and privacy.[34] Al-Nur 24:27–28 further requires individuals to seek permission and offer greetings before entering another person's dwelling. Classical exegetes and contemporary scholars have interpreted this requirement as an early juridical articulation of controlled access to private spaces, a principle that bears a structural resemblance to the requirement of consent in modern data protection law.[35] Building on these textual foundations, contemporary scholarship extends the prohibitions of *tajassus* and

[31] Morić et al., "Protection of Personal Data in the Context of E-Commerce."
[32] Ulul Umami and Abdul Ghofur, "Human Rights in Maqāṣid Al-Sharī'ah Al-'Āmmah: A Perspective of Ibn 'Āshūr," *Al-Ahkam* 32, no. 1 (2022): 91–108.
[33] Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law*, 12.
[34] Al-Hujurat 49:12.
[35] Al-Nur 24:27–28.

ghībah to the digital domain. From this perspective, the unauthorized collection, storage, or disclosure of personal data may constitute a digital form of *tajassus*, while its subsequent dissemination may constitute a digital form of *ghībah*. Both practices are prohibited regardless of the medium through which they occur.[36]

Two additional doctrinal elements further strengthen this framework. The first is *amānah* (trust), which establishes that any party entrusted with another person's property, secrets, or information assumes an ethical and legal obligation to safeguard it and may be held accountable for its loss or misuse. Several scholars have extended this principle by analogy to the relationship between data controllers and data subjects, conceptualizing cloud-stored personal data as an object of *wadīʿah* (safekeeping) rather than as property over which the platform exercises unconditional ownership. The second is the legal maxim *lā ḍarar wa lā ḍirār* (there shall be neither harm nor the reciprocation of harm), which underpins the broader Islamic prohibition against causing material, reputational, or psychological injury to others. Contemporary jurists invoke this maxim to argue that data breaches, algorithmic profiling, and non-consensual data monetization may constitute legally relevant forms of harm under Islamic legal reasoning, even in the absence of specific textual rulings addressing digital technologies.[37] Comparative scholarship on AI governance and data protection in the Gulf states further suggests that existing statutory frameworks are increasingly interpreted by local jurists through the lens of *ḥifẓ al-ʿirḍ*, rather than being treated solely as autonomous secular innovations.[38]

The Prophetic tradition reinforces the Quranic foundations of *ḥifẓ al-ʿirḍ* and provides the concept of *ʿirḍ* with its juristic contours. In his sermon during the Farewell Pilgrimage, the Prophet declared the blood, property, and honor (*aʿrāḍ*) of Muslims to be inviolable, thereby placing the protection of honor on the same normative level as the protection of life and property.[39] Classical lexicographers and jurists generally understand *ʿirḍ* as the dimension of a person's identity that is subject to praise or blame, encompassing reputation, social standing, and personal dignity that individuals seek to preserve against disparagement. This broad understanding helps explain why the subsequent jurisprudence concerning *ghībah* (backbiting), *qadhf* (false accusation of adultery), and *sitr* (concealing another person's faults) can be understood within a shared normative objective. The Prophetic tradition stating that whoever conceals the faults of a Muslim will have their own faults concealed by God further reinforces this understanding. It presents discretion in handling another person's private affairs as a positive moral obligation rather than merely an injunction to refrain from wrongdoing.[40]

---

[36]Nidhom and Murtadho, "Does Islam Protect Digital Privacy? An Islamic Studies Approach to Personal Data Protection."

[37] Elmahjub, "Artificial Intelligence (AI) in Islamic Ethics: Towards Pluralist Ethical Benchmarking for AI."

[38] Radwan Eskhita and Evert Stamhuis, "The Influence of the Brussels Effect on the Interpretation of Data Protection Laws in the Gulf," *Global Journal of Comparative Law* 13, no. 2 (2024): 261–78.

[39] The narration of the farewell pilgrimage sermon on the inviolability of blood, property, and honor is recorded in the collections of al-Bukhari and Muslim.

[40] The narration on concealing the faults of a Muslim is recorded in the collections of Muslim and al-Bukhari.

Two further juristic developments are relevant to extending this framework to the digital domain. First, the doctrine of *isti'dhān* (seeking permission) is not limited to entering private dwellings. The Prophetic explanation that the requirement of seeking permission was established to protect against intrusion through the gaze (*al-baṣar*) indicates that the underlying rationale is to safeguard matters that individuals are entitled to keep beyond the sight and knowledge of others. Accordingly, the scope of this principle should be understood in light of its underlying purpose rather than restricted to the physical boundaries of a home.[41] From this perspective, accessing an individual's private informational space, including personal accounts, digital devices, or databases containing personal records, without authorization may fall within the scope of the prohibition, even when no physical boundary is crossed. Second, Islamic jurists have long distinguished between the prohibited exposure of another person's faults and disclosure justified by a legitimate interest. Recognized grounds for such disclosure include lodging a complaint before a judge or competent authority, warning a prospective party to a transaction about a fraudulent individual, and consulting someone capable of addressing or remedying a particular harm. This distinction offers a useful conceptual parallel to modern data protection law, in which the general prohibition on processing personal data is qualified by lawful bases and specific exceptions relating to public interest, legal obligations, and the protection of human dignities.

The findings also differ from a strand of Islamic scholarship that grounds data protection in maqasid concepts at a general level.[42] While these studies establish that Islamic ethics is not silent on privacy, the present study offers a more determinate mapping and, more importantly, advances a methodological claim: when understood as an open system, the maqasid generate new categories rather than merely ratifying existing ones. Informational dignity is proposed as one such category. It does not replace *ḥifẓ al-'irḍ* but rather specifies its application in contexts where harm arises from the aggregation, inference, and circulation of information. This specification enables contemporary fiqh to address phenomena such as algorithmic profiling, which fall beyond the scope of both classical legal manuals and existing legislation. In this respect, the study also converges with scholarship on Islamic ethics and artificial intelligence, which calls for ethical benchmarks grounded in the Islamic tradition rather than imported wholesale from external frameworks.[43]

Table 1 provides a structured comparison of the two normative frameworks across seven dimensions: sources of authority, grounds for access, limitations on data collection, custodial responsibilities, harm prevention, enforcement mechanisms, and scope of protection. These dimensions offer a more detailed analytical basis for examining four overarching categories: consent, scope and purpose, accountability, and enforcement. The comparative analysis is designed to identify not only areas of

[41] The narration on the purpose of seeking permission (*isti'dhān*) is recorded in the collections of al-Bukhari and Muslim works.
[42] Nidhom and Murtadho, "Does Islam Protect Digital Privacy? An Islamic Studies Approach to Personal Data Protection."
[43] Elmahjub, "Artificial Intelligence (AI) in Islamic Ethics: Towards Pluralist Ethical Benchmarking for AI"; Ali et al., "Islamic Ethics and AI: An Evaluation of Existing Approaches to AI Using Trusteeship Ethics."

convergence and divergence but also the distinct normative rationales underpinning each framework. The Indonesian Personal Data Protection Law (UU PDP) provides the statutory basis for the entries in the left-hand column, whereas the right-hand column draws on the Qur'an, Prophetic traditions, and juristic interpretations examined in the preceding discussion. Each dimension thus brings a statutory provision into dialogue with an Islamic legal principle that serves a comparable protective function. Through this comparison, the study demonstrates how the protection of informational dignity can be articulated within a contemporary maqasid framework.

Table 1. Comparative Analysis of UU PDP No. 27/2022 and Informational Dignity

Aspect	UU PDP No. 27/2022	Informational Dignity
Source of authority	State legislation grounded in constitutional guarantees, particularly Article 28G of the 1945 Constitution	Divine authority grounded in the Qur'an, Hadith, and the maqasid sharia
Basis for access	Consent of the data subject, alongside other lawful bases for processing	Permission (*isti'dhān*) before entering private spaces or accessing protected information
Restraint on collection	Purpose limitation and data minimization	Prohibition of *tajassus* (spying or intrusive surveillance) and unjustified intrusion into private affairs
Custodial duty	Accountability of data controllers and processors, including obligations to maintain data security and confidentiality	*Amānah* (trust) and the duty of safekeeping, informed by the principles of *wadī'ah*
Harm rationale	Personal data breaches and unlawful processing that may trigger administrative or criminal liability	The legal maxim *lā ḍarar wa lā ḍirār* (there shall be neither harm nor the reciprocation of harm)
Enforcement	Supervisory oversight, administrative sanctions, and criminal penalties	Individual *taqwā* (God-consciousness), communal *al-amr bi al-ma'rūf wa al-nahy 'an al-munkar* (enjoining good and forbidding wrong), and divine accountability
Scope	Personal data processed electronically or through non-electronic systems that form part of, or are intended to form part of, a structured filing system	The protection of a person's honor, reputation, privacy, and information that they are entitled to keep from unauthorized exposure, in both digital and non-digital contexts

Source: Authors' elaboration, 2026.

The comparative findings suggest that the relationship between the two normative frameworks extends beyond the functional parallels identified across the seven analytical dimensions. The UU PDP establishes the legal and procedural requirements for protecting personal data through consent, purpose limitation,

custodial responsibilities, and sanctions. However, although its normative foundation includes constitutional guarantees of dignity and the protection of individual rights, the statute primarily specifies the legal conditions and mechanisms of data protection rather than developing a broader ethical account of why informational interests warrant protection.

The Islamic normative framework, by contrast, provides a substantive ethical and juridical rationale through the principle of *ḥifẓ al-ʿirḍ*, situating the protection of personal information within the broader objectives of preserving human honor and dignity and preventing harm. The points of convergence identified in the comparative analysis—particularly those concerning access, collection, custodial responsibility, and harm prevention—therefore indicate that the procedural safeguards established by the UU PDP can be interpreted as institutional and legal expressions of the protective objectives associated with *ḥifẓ al-ʿirḍ*. Conversely, the differences concerning normative authority, enforcement, and scope reveal areas in which the maqasid-based perspective can broaden the statute's interpretive and ethical foundations. This complementary relationship provides the basis for developing informational dignity as a contemporary interpretive category that connects the procedural requirements of positive law with the substantive ethical objectives of Islamic jurisprudence.

Discussion

The findings demonstrate that the UU PDP and *ḥifẓ al-ʿirḍ* exhibit a remarkable degree of structural convergence at the level of operative norms, despite originating from entirely distinct sources of authority. The most evident point of convergence concerns consent: the UU PDP's requirement of explicit, informed consent prior to the collection and processing of personal data closely parallels the Quranic mandate in Al-Nur 24:27–28, which requires permission before entering another's private space. Both frameworks treat unauthorized access to private matters as presumptively wrongful, subject to narrowly defined exceptions.[44] A second point of convergence involves purpose limitation and data minimization: the UU PDP's prohibition on processing data beyond its stated purpose functions, in effect, as a positive-law analogue to the Quranic prohibition on *tajassus*. Both restrict the collection of information to what is necessary and legitimate, rather than permitting open-ended surveillance.[45] A third point of convergence concerns accountability. The UU PDP imposes on data controllers an affirmative duty to implement technical and organizational safeguards and holds them liable for breaches resulting from negligence. This closely aligns with the fiqh concept of *amānah*, which imposes fiduciary liability on any custodian of another's property or secret.[46] Finally, both frameworks recognize a harm-based rationale for regulation: the UU PDP's criminal provisions against unlawful disclosure of personal data causing loss to the data

[44] Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022," Art. 20–22.
[45] Nidhom and Murtadho, "Does Islam Protect Digital Privacy? An Islamic Studies Approach to Personal Data Protection."
[46] Koko Komaruddin et al., "Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications," *West Science Law and Human.* 1, no. 4 (2023): 166–72.

subject echo the maxim *lā ḍarar wa lā ḍirār*, which prohibits the infliction of harm regardless of whether that harm is codified in a specific ruling.[47]

Taken together, these convergences suggest that the UU PDP, whether or not its drafters intended it, substantially reproduces the operative content of *ḥifẓ al-ʿirḍ* in a secular administrative form. This finding aligns with recent comparative scholarship on Gulf jurisdictions, where positive data protection statutes are increasingly interpreted by local scholars as functional extensions of maqasid-based privacy doctrine.[48] Despite this significant normative overlap, the two frameworks diverge sharply in their legitimating foundations and enforcement logic. The UU PDP is anthropocentric and procedural: its authority derives from state sovereignty and constitutional delegation; violations are adjudicated by an administrative oversight body and, in aggravated cases, by criminal courts; and its remedies are limited to fines, imprisonment, and administrative sanctions calculated in monetary and custodial terms.[49] In contrast, *ḥifẓ al-ʿirḍ* is theocentric and moral: its authority derives from divine command; violations entail accountability before God in addition to any worldly consequences; and its enforcement relies substantially on individual conscience (*taqwā*) and communal moral suasion (*al-amr bi al-maʿrūf wa al-nahy ʿan munkar*) rather than on a centralized regulatory institution.[50]

This divergence has three practical implications. First, the scope of protection differs: the UU PDP applies exclusively to personal data that is structured, recorded, or processed electronically or otherwise systematically, whereas *ḥifẓ al-ʿirḍ* extends to any disclosure or exposure of what a person wishes to keep concealed, whether transmitted through digital data, spoken rumor, or written text, making its scope considerably broader than that of any single statute.[51] Second, the remedial logic differs: UU PDP's administrative fines and criminal penalties are calibrated to deter and compensate, while Islamic legal doctrine on *ghībah* and slander (*qadhf*) contemplates both worldly sanctions and an obligation of repentance and, where applicable, restitution of honor, reflecting a restorative rather than purely punitive orientation.[52] Third, the institutional capacities differ: UU PDP relies on state oversight, which still faces resource and independence challenges, while ḥifẓ al-ʿirḍ depends on individual and community moral responsibility, which religious and social institutions in Muslim-majority societies such as Indonesia can help strengthen.[53]

---

[47] Miftahudin Azmi, "Protection of Human Rights Victims of Sexual Violence through Maqâsid Al-Sharî'ah: A Case in Batu City Indonesia," *Jurnal HAM* 13, no. 3 (2022): 613–30.
[48] Laroussi Chemlali, Abdesselam Salmi, and Leila Benseddik, "A Reflection on the UAE's New Data Protection Law: A Comparative Approach with GDPR," *Journal of Data Protection & Privacy* 6, no. 1 (2023): 24–36.
[49] Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022," Art. 65–67.
[50] Mohamed Salem Abou El Farag and Tarek Rashed, "The Impact of Maqasid Al Shariah (Objectives of Islamic Shariah) to Obtain Legal Protection of Humans: A Comparative and Analytical Study of the Qatari Laws," *Journal of Law and Sustainable Development* 11, no. 9 (2023): 1–26.
[51] Wahbah Al-Zuhaili, *al-Fiqh al-Islāmī wa Adillatuh* 8, 127.
[52] Nidhom and Murtadho, "Does Islam Protect Digital Privacy? An Islamic Studies Approach to Personal Data Protection."
[53] Badar, "Personal Data Protection Policy in Law Number 27 of 2022 in the Perspective of Positive Law and Islamic Law."

The complementarity proposed here should not be interpreted as an argument for subordinating the statute to religious doctrine or for incorporating religious sanctions into a law that applies to all citizens regardless of faith. UU PDP is a general law whose authority is grounded in the constitutional order, and its protections extend equally to Muslims and non-Muslims. The role attributed to *ḥifẓ al-ʿirḍ* is therefore explanatory and motivational rather than coercive; it offers Muslim communities and the institutions that guide them a theological framework in which the requirements of the statute can be understood as consistent with, and in part mandated by, their own tradition. This distinction preserves the pluralistic character of Indonesia's legal system while allowing religious ethics to contribute to a culture of compliance. It parallels the way comparative scholarship on the Gulf describes positive statutes as being interpreted by local jurists as partial codifications of Islamic ethical principles rather than as replacements for them.[54] The same caution applies to the scope of fiqh itself, since the plurality of juristic opinions on questions of privacy means that the framework proposed here is best understood as a shared set of objectives and criteria within which differing rulings may be reasoned, rather than as a single codified rule.[55]

The comparative analysis presented above has three implications for digital governance in Indonesia. First, because the UU PDP and *ḥifẓ al-ʿirḍ* substantially converge at the level of operative norms, socialization efforts aimed at improving public compliance with the UU PDP can legitimately draw on Islamic religious vocabulary. This approach frames data protection not merely as a bureaucratic obligation but as an extension of long-established religious duties and ethical principles, including the prohibition of *ghībah* and *tajassus* and the obligation of *amānah*. Comparative scholarship on Gulf jurisdictions suggests that such religious framing can strengthen voluntary compliance among Muslim-majority populations.[56] Second, because *ḥifẓ al-ʿirḍ*'s scope extends beyond structured electronic data to any wrongful exposure of what a person wishes to keep concealed, it offers a normative resource for addressing forms of privacy violation that fall outside the UU PDP's statutory definitions. These include informal rumor spreading, unauthorized disclosure of health or family information within community settings, and reputational harm inflicted through means that do not qualify as "personal data processing" in the technical sense of the statute. Religious and educational institutions, rather than the state data protection authority, are best positioned to address this residual category of harm.[57] Third, the divergence in enforcement logic suggests that state regulation and religious ethics are complementary rather than

[54] Eskhita and Stamhuis, "The Influence of the Brussels Effect on the Interpretation of Data Protection Laws in the Gulf"; Chemlali, Salmi, and Benseddik, "A Reflection on the UAE's New Data Protection Law: A Comparative Approach with GDPR."
[55] See Wathoni, "Sociocultural Dynamics of Islamic Legal Reform Across Muslim-Majority Countries: A Comparative Perspective."
[56] Ahmad Faiqun Nawwar Rofiq et al., "Online Data Privacy Ethical Guidelines Based on Islamic Perspectives," *International Journal on Islamic Applications in Computer Science and Technology* 13, no. 2 (2025): 1–7.
[57] Munifah and Mufrod Teguh Mulyo, "Personal Data Hacking: A Critical Analysis of Islamic Criminal Law and Islamic Jurisprudence," *Ulul Albab: Jurnal Studi dan Penelitian Hukum Islam* 8, no. 2 (2025): 179–97.

substitutable. The UU PDP provides the coercive, institutional mechanisms—such as an oversight body, sanctions, and a formal complaints process—that Islamic ethics alone cannot offer, while *ḥifẓ al-ʿirḍ* supplies the internalized moral motivation that pure legal compliance, absent genuine conviction, tends to lack. Therefore, integrating both approaches, rather than substituting one for the other, is the most promising pathway toward cultivating a data protection culture that is simultaneously legally robust and ethically grounded in Indonesia's Muslim-majority context.[58]

These three implications indicate that the contribution of this comparative reading extends beyond merely demonstrating compatibility between UU PDP and *ḥifẓ al-ʿirḍ*. For contemporary fiqh, the more significant outcome is that *ḥifẓ al-ʿirḍ* can be reconstructed as an operative category of informational dignity, capable of guiding future ijtihad on digital phenomena, cyber *tajassus*, algorithmic profiling, and AI-driven data inference—areas that neither classical fiqh nor Indonesia's current positive law address in definitive terms. Doctrinal studies of UU PDP have generally described the statute without exploring what normative resources a religious tradition could contribute to its interpretation, while comparative studies have benchmarked it against the GDPR and neighboring regimes without engaging Islamic legal theory.[59] This analysis reveals a shared blind spot in both bodies of work: they treat the justification for data protection as either settled by constitutional or regulatory text or as external to law. By reading the statute through *ḥifẓ al-ʿirḍ*, the study demonstrates that the justification can be articulated in terms internal to a living legal tradition, and that doing so changes how certain statutory features are understood. For example, consent appears not merely as an administrative precondition but as the modern form of a permission-based ethic of access, and the security duty of the controller appears not merely as regulatory diligence but as an application of the fiduciary responsibility inherent in trust.

Conclusion

This study demonstrates that the relationship between Indonesia's Personal Data Protection Law (UU PDP) and the maqasid principle of *ḥifẓ al-ʿirḍ* extends beyond normative convergence to reveal the need for a broader juristic reconstruction of personal data protection grounded in the concept of informational dignity. Although both frameworks converge on fundamental principles such as consent, purpose limitation, and accountability, their normative foundations remain philosophically distinct. This distinction does not imply that one framework should replace or take precedence over the other. Rather, it reveals the complementary yet irreducible dimensions of legal and moral responsibility in protecting personal data. The study therefore proposes informational dignity as a contemporary specification of *ḥifẓ al-ʿirḍ*, extending its normative relevance to the conditions of the digital age. As a new

[58] Resty Regina Putri, "Perlindungan Data Pribadi Dan Etika Privasi Digital Dalam Perspektif Islam," *Qolamuna: Keislaman, Pendidikan, Literasi dan Humaniora* 3, no. 1 (2026): 175–80.
[59] Rosadi et al., "Indonesia's Personal Data Protection Bill, 2020: Does It Meet the Needs of the New Digital Economy?"; Simbolon and Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and the European Union General Data Protection Regulation."

juristic category, it provides a conceptual foundation for future ijtihad on emerging challenges, including cyber-*tajassus*, algorithmic profiling, and AI-driven inference, which remain insufficiently addressed by both classical fiqh and existing positive law. In this way, the study contributes to the development of contemporary fiqh by demonstrating how the maqasid sharia, understood as an open and dynamic normative framework, can generate new categories of legal and ethical reasoning in response to technological transformations.

Several limitations qualify these findings and suggest directions for future research. First, the study adopts a doctrinal approach and does not empirically assess whether religious framing strengthens compliance with UU PDP. The proposition that *ḥifẓ al-ʿirḍ* can encourage voluntary compliance therefore requires testing through surveys, fieldwork, or evaluations of religious literacy programs on data protection. Second, the institutional framework for implementing UU PDP, particularly its supervisory and enforcement mechanisms, remains under development. Its enforcement capacity should therefore be reassessed as implementing regulations and enforcement practices evolve. Third, the study approaches fiqh through the maqasid sharia framework. Further research could explore how different Islamic legal schools address issues such as data monetization, digital platform liability, and consent under conditions of informational asymmetry. It could also examine the role of institutional ijtihad, particularly fatwa institutions and Indonesian Islamic legal deliberation forums (*baḥth al-masāʾil*), in formulating contextually relevant responses. Fourth, the comparison with Gulf jurisdictions relies primarily on secondary literature. Direct analysis of their legal frameworks and interpretive practices would provide a stronger basis for comparison with Indonesia's mixed legal order. Addressing these limitations would advance the proposed framework beyond conceptual reconstruction toward an empirically tested and institutionally grounded contribution to contemporary fiqh.

Acknowledgments

The authors would like to express their sincere gratitude to the faculty members and academic staff of the Faculty of Sharia and Law, UIN Raden Fatah Palembang, Indonesia, for their invaluable support and contributions to the academic work underlying this study.

Disclosure Statement

The authors declare no conflict of interest and confirm that no external party was involved in any way that could compromise the objectivity of this research.

Ethical Approval

Ethical approval was not required for this study because it was based exclusively on doctrinal legal analysis of legislation, Islamic legal sources, and published academic literature.

Financial Support

The authors confirm that this research was conducted without financial support from any public, commercial, or non-profit funding organizations.

References

Ali, Fatima, Karim Bouzoubaa, Frank Gelli, Boumediene Hamzi, and Suhair Khan. "Islamic Ethics and AI: An Evaluation of Existing Approaches to AI Using Trusteeship Ethics." *Philosophy & Technology* 38, no. 120 (2025): 1–34. https://doi.org/10.1007/s13347-025-00922-4.

Aloufi, Abdulrahman, Muhammad Akbar Khan, Muhammad Akbar Khan, and Bilal Hussain. "Legal Gaps, Islamic Ethics, and Digital Trust: Building a Regulatory Framework for Saudi E-Commerce Under Vision 2030." *Journal of Cultural Analysis and Social Change* 10, no. 4 (2025): 3860–80. https://doi.org/10.64753/jcasc.v10i4.3678.

Al-Zuhaili, Wahbah. *Al-Fiqh al-Islāmī wa Adillatuh*. n.d.

Auda, Jasser. *Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach*. London: The International Institute of Islamic Thought, 2008.

Azmi, Miftahudin. "Protection of Human Rights Victims of Sexual Violence through Maqâsid Al-Sharî'ah: A Case in Batu City Indonesia." *Jurnal HAM* 13, no. 3 (2022): 613–30. https://doi.org/10.30641/ham.2022.13.613-630.

Badar, Eryna Syahadatina, Ahmad Fauzi, and Ahya Jazuli. "Personal Data Protection Policy in Law Number 27 of 2022 in the Perspective of Positive Law and Islamic Law." *Hukum Islam* 23, no. 1 (2023): 61–74. https://doi.org/10.24014/jhi.v23i1.20465.

Chemlali, Laroussi, Abdesselam Salmi, and Leila Benseddik. "A Reflection on the UAE's New Data Protection Law: A Comparative Approach with GDPR." *Journal of Data Protection & Privacy* 6, no. 1 (2023): 24–36. https://doi.org/10.69554/opeg2767.

Eke, Damian and Bernd Stahl. "Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies." *DISO* 3, no. 11 (2024): 1–23. https://doi.org/10.1007/s44206-024-00101-6.

El Farag, Mohamed Salem Abou, and Tarek Rashed. "The Impact of Maqasid Al Shariah (Objectives of Islamic Shariah) to Obtain Legal Protection of Humans: A Comparative and Analytical Study of the Qatari Laws." *Journal of Law and Sustainable Development* 11, no. 9 (2023): 1–26. https://doi.org/10.55908/sdgs.v11i9.983.

El-Khoury, Moufid, and Saleh Albarashdi. "Navigating the Privacy Landscape of Healthcare-Driven AI in the Middle East: Case Studies from Oman, Qatar, and Saudi Arabia." *Social Sciences and Humanities Open* 11 (2025): 1–10. https://doi.org/10.1016/j.ssaho.2025.101492.

Elmahjub, Ezieddin. "Artificial Intelligence (AI) in Islamic Ethics: Towards Pluralist Ethical Benchmarking for AI." *Philosophy & Technology* 36, no. 4 (2023): 1–24. https://doi.org/10.1007/s13347-023-00668-x.

Eskhita, Radwan, and Evert Stamhuis. "The Influence of the Brussels Effect on the Interpretation of Data Protection Laws in the Gulf." *Global Journal of Comparative Law* 13, no. 2 (2024): 261–78. https://doi.org/10.1163/2211906x-13020007.

Greenleaf, Graham. "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills." *UNSW Law & Justice Research Series* 48, no. 181 (2023): 1-6. http://dx.doi.org/10.2139/ssrn.4426146.

Indonesia, Republik. "Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." Jakarta: Sekretariat Negara Republik Indonesia, 2022.

Indonesia, Republik. "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945."

Komaruddin, Koko, Andrew Shandy Utama, Eko Sudarmanto, and Sugiono Sugiono. "Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications." *West Science Law and Human* 1, no. 4 (2023): 166–72. https://doi.org/10.58812/wslhr.v1i04.323.

Kunhibava, Sherin, Aishath Muneeza, Zakariya Mustapha, Mohammad Ershadul Karim, Auwal Adam Sa'ad. "Selected Issues in the Use of RegTech in the Islamic and Conventional Financial Markets." *Journal of Islamic Accounting and Business Research* 15, no. 5 (2024): 746–61. https://doi.org/10.1108/JIABR-03-2022-0069.

Morić, Zlatan, Vedran Dakić, Daniela Đekić, and Damir Regvart. "Protection of Personal Data in the Context of E-Commerce." *Journal of Cybersecurity and Privacy* 4, no. 3 (2024): 731–61. https://doi.org/https://doi.org/10.3390/jcp4030034.

Munifah, Munifah, and Mufrod Teguh Mulyo "Personal Data Hacking: A Critical Analysis of Islamic Criminal Law and Islamic Jurisprudence." *Ulul Albab: Jurnal Studi dan Penelitian Hukum Islam* 8, no. 2 (2025): 179–97. https://doi.org/10.30659/jua.v8i2.44585.

Negara, Tunggul Ansari Setia. "Normative Legal Research in Indonesia: Its Origin and Approaches." *Audito Comparative Law Journal* 4, no. 1 (2023): 1–9. https://doi.org/10.22219/aclj.v4i1.24855.

Nidhom, Misbahun, and Ali Murtadho. "Does Islam Protect Digital Privacy? An Islamic Studies Approach to Personal Data Protection." *Al-Afham: Journal of Islamic Studies* 2, no. 2 (2025): 107–28. https://doi.org/10.62509/ajis.v2i2.260.

Nurhayati, Yati, Ifrani Ifrani, and M Yasir Said. "Metodologi Normatif dan Empiris dalam Perspektif Ilmu Hukum." *Jurnal Penegakan Hukum Indonesia* 2, no. 1 (2021): 1–20. https://doi.org/10.51749/jphi.v2i1.14.

Putri, Resty Regina. "Perlindungan Data Pribadi Dan Etika Privasi Digital Dalam Perspektif Islam." *Qolamuna: Keislaman, Pendidikan, Literasi dan Humaniora* 3, no. 1 (2026): 175–80. https://jurnal.qolamuna.id/index.php/JQ/article/view/369.

Ridwan, Muannif, Ontran Sumantri Riyanto, Yatini Yatini, Usman Jayadi, and Rico Nur Ilham. "Approaches in Legal Research: An Introduction about Study Analysis of Western Law and Islamic Law." In *Proceedings of the Borneo International Conference on Education and Social Sciences*. European Alliance for Innovation (EAI), 2022. https://doi.org/10.4108/eai.11-10-2021.2319623.

Rofiq, Ahmad Faiqun Nawwar, Md Saidur Rahman, Ahmad Yusuf Shaikh, Mamadou Bobo Barry, and Akram M. Zeki. "Online Data Privacy Ethical Guidelines Based on Islamic Perspectives." *International Journal on Islamic Applications in Computer Science and Technology* 13, no. 2 (2025): 1–7. https://ijasat.com/index.php/ijasat_en/article/view/165.

Rosadi, Sinta Dewi, Andrey Noviandika, Rueben Walters, and Fitria Rahmadania Aisy. "Indonesia's Personal Data Protection Bill, 2020: Does It Meet the Needs of the New Digital Economy?" *International Review of Law, Computers & Technology* 37, no. 1 (2023): 78–90. https://doi.org/10.1080/13600869.2022.2114660.

Setyo, Utomo. "Personal Data Protection Through Law Number 27 Of 2022: Challenges of Cybercrime in The Era of Globalization and Digital." *Pena Justisia: Media Komunikasi dan Kajian Hukum* 23, no. 3 (2024): 2967–75. https://doi.org/10.31941/pj.v23i3.5611.

Shahrullah, Rina Shahriyani, Jinny Park, and Irwansyah. "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment." *Hasanuddin Law Review* 10, no. 1 (2024): 1–20. https://doi.org/10.20956/halrev.v10i1.5016.

Simbolon, Valerie Angel, and Vishnu Juwono. "Comparative Review of Personal Data Protection Policy in Indonesia and the European Union General Data Protection Regulation." *Publik: Jurnal Ilmu Administrasi* 11, no. 2 (2022): 178–90. http://dx.doi.org/10.31314/pjia.11.2.178-190.2022.

Umami, Ulul, and Abdul Ghofur. "Human Rights in Maqāṣid Al-Sharī'ah Al-'Āmmah: A Perspective of Ibn 'Āshūr." *Al-Ahkam* 32, no. 1 (2022): 91–108. https://doi.org/10.21580/ahkam.2022.32.1.9306.

Wathoni, Muhammad Ahmad. "Sociocultural Dynamics of Islamic Legal Reform Across Muslim-Majority Countries: A Comparative Perspective." *Diktum: Jurnal Syariah dan Hukum* 23, no. 2 (2025): 214–31. https://doi.org/10.35905/diktum.v23i2.13072.

Wicaksana, Kukuh Pandu, Tahegga Primananda Alfath, and Heru Kuswanto. "Personal Data Protection in the Digital Era: A Maqasid Al-Shariah Perspective on Contemporary Legal Challenges." *Mizan: Journal of Islamic Law* 14, no. 1 (2026): 114–22. https://doi.org/10.32832/mizan.v14i1.24363.