MIZAN:
JOURNAL OF ISLAMIC LAW
P-ISSN: 2598-974X. E-ISSN: 2598-6252
Vol. 14 No.1 (2026), pp.114-122
https://ejournal.uika-bogor.ac.id/index.php/MIZAN/index

Personal Data Protection in the Digital Era: *A Maqasid al-Shariah* Perspective on Contemporary Legal Challenges[1]

Kukuh Pandu Wicaksana[1], Tahegga Primananda Alfath[2], Heru Kuswanto[3]
[1,2,3]Universitas Narotama Surabaya, Jawa Timur, Indonesia
Corresponding author: kukuhpanduwicaksana@gmail.com

10.32832/mizan.V14i1.22997

Abstract:
Personal data has become one of the most valuable assets in the digital era, yet its extensive collection and processing by digital platforms, corporations, and government institutions have created significant risks of misuse, unauthorized disclosure, and violation of individual privacy. While Indonesia has responded through Law Number 27 of 2022 concerning Personal Data Protection, positive law alone provides limited ethical grounding for evaluating why such protection matters and how far it should extend, particularly in the face of emerging challenges such as algorithmic profiling and automated decision-making. This study examines personal data protection through the lens of Maqasid al-Shariah, the objectives of Islamic law, to identify the extent to which Islamic legal reasoning can complement and, in certain respects, extend the normative foundations of positive data protection law. Using normative legal research with statutory, conceptual, and comparative approaches, this study analyzes primary legal materials, including Qur'anic verses, authentic hadith, and Indonesian data protection legislation, alongside secondary materials drawn from classical and contemporary Maqasid al-Shariah scholarship. The analysis employs qualitative content analysis, categorizing findings according to the dimensions of hifzh al-din, al-nafs, al-'aql, al-nasl, al-mal, and the contemporary extension of hifzh al-'irdh. The findings show that core principles of Law Number 27 of 2022, namely lawfulness, transparency, purpose limitation, and accountability, are substantively consistent with the Islamic principles of taradhi (mutual consent), amanah (trustworthiness), 'adl (justice), and dar' al-mafasid (prevention of harm). However, the analysis also identifies areas where Maqasid al-Shariah offers a broader ethical horizon than current positive regulation, particularly regarding the algorithmic manipulation of human reasoning (hifzh al-'aql) and the moral, rather than merely administrative, character of data trusteeship. This study concludes that harmonizing Islamic legal objectives with

[1] Manuscript received date: May 2, 2026; revised: June 21, 2026; approved for publication: July 8, 2026.

positive data protection law can produce a more comprehensive, ethically grounded framework for digital governance in Muslim-majority societies such as Indonesia.

Keywords: *personal data protection; Maqasid al-Shariah; digital privacy; Islamic law; Law Number 27 of 2022.*

A. INTRODUCTION

The development of digital technology has brought significant change to human life across communication, economic activity, public service, education, and social interaction. In this environment, personal data has become one of the most valuable assets because it contains information related to an individual's identity, preferences, financial activity, location, and behavior. The massive collection and processing of personal data by digital platforms, corporations, and government institutions bring benefits in efficiency and innovation, but also generate legal challenges concerning privacy, data misuse, and individual rights (Kuner, 2020). Data breaches, identity theft, unauthorized surveillance, and commercial exploitation of personal information demonstrate that digital transformation must be accompanied by robust legal and ethical safeguards (OECD, 2013).

Internationally, personal data protection has developed as part of the recognition of privacy as a fundamental human right, as reflected in frameworks such as the European Union's General Data Protection Regulation (GDPR), which emphasizes transparency, purpose limitation, data minimization, and individual control over personal information (Voigt & Von dem Bussche, 2017). In Indonesia, Law Number 27 of 2022 concerning Personal Data Protection provides the legal foundation for data subjects' rights, data controllers' obligations, and mechanisms to prevent the misuse of personal information (Sinta et al., 2023). Nevertheless, legal regulation alone often struggles to keep pace with the speed of technological change, and compliance-based frameworks do not always articulate why privacy deserves protection in moral terms — a gap that ethical and religious legal traditions can help address.

From the perspective of Islamic law, personal data protection can be examined through the concept of Maqasid al-Shariah, the objectives underlying Islamic legal provisions that aim to secure human welfare (maslahah) and prevent harm (mafsadah). Al-Ghazali identified five essential objectives (al-dharuriyyat al-khamsah): the protection of religion (hifzh al-din), life (hifzh al-nafs), intellect (hifzh al-'aql), lineage (hifzh al-nasl), and wealth (hifzh al-mal) (Al-Ghazali, 1997). Contemporary scholars such as Ibn Ashur (2006) and Auda (2008) have extended this framework to include the protection of human dignity (hifzh al-'irdh) and argued that Maqasid al-Shariah is not confined to classical legal discourse but offers a flexible, objectives-oriented methodology capable of responding to new social realities, including questions of digital governance.

Islamic teaching places explicit emphasis on the protection of privacy. Qur'an, Surah Al-Hujurat (49): 12, prohibits tajassus — spying on and seeking out the private affairs of others — and this prohibition is reinforced by hadith narrated in Sahih Muslim, in which the Prophet Muhammad (peace be upon him) states that whoever conceals the faults of a fellow Muslim will have their own faults concealed by Allah in this world and the hereafter. Read together, these sources establish privacy not as a mere social courtesy but as a protected legal-ethical value. Unauthorized access to personal information, the dissemination of private data, and misuse of digital identity are, on this basis, inconsistent with Islamic principles because they generate injustice ('adl violation) and harm (mafsadah) (Kamali, 2008).

The relevance of personal data to hifzh al-mal (protection of wealth) is evident in the modern digital economy, where personal information carries direct commercial value for marketing, consumer profiling, and business decision-making; its unauthorized exploitation can produce real financial harm (Dusuki & Abdullah, 2007). The principle of dar' al-mafasid (prevention of harm) is likewise directly engaged, since Islamic legal theory treats the prevention of anticipated harm as a priority consideration in legal reasoning, even ahead of the pursuit of benefit (Auda, 2008).

Previous studies have examined the relationship between Islamic law and technological development in general terms. Kamali (2021) argues that Islamic legal principles can respond to modern challenges through the concepts of justice, responsibility, and public interest, while Auda (2008) emphasizes Maqasid al-Shariah as a methodological approach to addressing contemporary problems by reference to broader human needs. However, prior literature has concentrated primarily on general digital ethics, and studies that examine personal data protection specifically as a contemporary Maqasid al-Shariah issue — including a direct, provision-by-provision comparison with positive Indonesian data protection law — remain limited. This gap justifies the present study.

This article therefore aims to analyze personal data protection in the digital era from the perspective of Maqasid al-Shariah, and specifically to (1) identify the Islamic legal objectives engaged by digital personal data processing; (2) examine the extent to which these objectives are reflected in Law Number 27 of 2022; and (3) identify points of convergence and divergence between Islamic legal objectives and positive law, in order to assess what each framework can offer the other in building a more ethical and human-centered digital legal order.

B. METHODE

This research employs normative (doctrinal) legal research, integrated with a Maqasid-based analytical approach to examine Islamic legal objectives alongside positive law. Normative legal research examines legal materials to identify, systematize,

and analyze legal concepts and norms rather than relying on empirical field data (Soekanto & Mamudji, 2014; Marzuki, 2005). Three approaches are used in combination: the statute approach, applied to Law Number 27 of 2022 concerning Personal Data Protection and related regulations; the conceptual approach, applied to theoretical concepts of privacy, personal rights, and digital responsibility; and the comparative approach, used specifically to juxtapose the normative content of positive data protection law with the objectives (maqasid) derived from Islamic legal sources, so that convergence and divergence between the two systems can be identified systematically rather than asserted impressionistically.

Legal materials are classified into three categories. Primary legal materials comprise, on the positive-law side, binding legislation — principally Law Number 27 of 2022 concerning Personal Data Protection — and, on the Islamic-law side, the Qur'an and authentic hadith bearing directly on privacy, trust, and the prevention of harm. Secondary legal materials consist of classical and contemporary Maqasid al-Shariah scholarship (including the works of Al-Ghazali, Al-Shatibi, Ibn Ashur, Kamali, and Auda), legal commentaries, and prior academic studies on digital privacy and data protection. Tertiary legal materials consist of legal dictionaries and encyclopedic references used to clarify terminology. This tripartite classification corrects a common conflation in interdisciplinary legal studies, in which classical juristic works are mistakenly treated as primary sources on a par with revealed texts; here, only the Qur'an, hadith, and enacted legislation are treated as primary, while juristic elaboration is treated as secondary authority that interprets, but does not constitute, the primary sources.

Data are collected through library-based (doctrinal) research, gathering statutory texts, primary religious texts, and relevant scholarly literature. The analysis technique is qualitative content analysis conducted in four steps: (1) data reduction, in which provisions of Law Number 27 of 2022 and relevant Qur'anic and hadith material are extracted and organized; (2) categorization, in which each provision or textual reference is mapped against the maqasid categories of hifzh al-din, al-nafs, al-'aql, al-nasl, al-mal, and al-'irdh; (3) interpretation, using statutory and systematic interpretation for positive law and qiyas (analogical reasoning) for extending classical Islamic legal objectives to the unprecedented context of digital data, in which the shared 'illat (effective cause) between classical harms — such as exposing private matters or misappropriating property — and contemporary data misuse is identified as the basis for analogy; and (4) synthesis, in which convergences and divergences between the two normative systems are drawn out and evaluated against the standard of maslahah and prevention of mafsadah. The validity of the analysis is maintained through source triangulation and consistency checking across classical and contemporary references.

This study acknowledges methodological limitations inherent to normative legal research: it does not employ empirical data on actual data-processing practices or enforcement outcomes, and its qiyas-based extension of classical maqasid categories to digital data, while grounded in recognized methodological precedent (Auda, 2008),

remains an interpretive exercise rather than a settled juristic ruling (fatwa). The findings should therefore be read as a conceptual-normative contribution rather than an empirical assessment of regulatory effectiveness.

C. RESULTS AND DISCUSSION

1. Personal Data Protection in the Digital Era: A Contemporary Legal Challenge

The rapid development of digital technology has fundamentally changed the nature of social interaction, transforming personal data from mere biographical information into a resource with substantial economic, social, and strategic value. The extensive collection, storage, and processing of personal data by digital platforms create risks of misuse, unauthorized access, and privacy violations (Kuner, 2020). Without adequate protective mechanisms, individuals may lose effective control over their own information, exposing them to identity theft, financial loss, discrimination, and violations of personal dignity (OECD, 2013).

In the Indonesian legal system, Law Number 27 of 2022 concerning Personal Data Protection establishes legal protections for data subjects by recognizing their rights regarding personal information and imposing obligations of legality, transparency, security, and accountability on data controllers and processors. This reflects a shift in legal understanding: personal data is no longer treated as a mere administrative artifact but as an extension of personal rights requiring state protection (Sinta et al., 2023). However, the effectiveness of this protection remains constrained by rapid technological innovation, limited public awareness, and the growing complexity of digital ecosystems.

Viewed through the lens of maslahah, personal data protection cannot be reduced to a technical or administrative matter; it is fundamentally a question of human dignity and social justice, since data misuse affects individuals economically, socially, and psychologically at once. This normative starting point sets up the central inquiry of this study: whether, and how, Islamic legal objectives can supply the ethical justification that a purely administrative reading of data protection law leaves implicit.

2. Personal Data Protection Based on Maqasid al-Shariah: Textual Grounds and Analogical Reasoning

The prohibition of tajassus in the Qur'an, Surah Al-Hujurat (49):12, together with the hadith on concealing the faults of others narrated in Sahih Muslim, establishes two textual pillars for treating privacy as a protected interest under Islamic law. Classical exegesis of this verse situates the prohibition within the broader Qur'anic concern for safeguarding social trust ('adl) and preventing the harm (mafsadah) that follows from exposing what a person has legitimately kept private. The present analysis extends this textual foundation to digital personal data through analogical reasoning (qiyas): the 'illat (effective cause) underlying the prohibition of tajassus and the exposure of others'

private affairs is the harm caused to dignity, security, and social standing by unauthorized intrusion into what a person has not consented to disclose. Because unauthorized collection, profiling, or disclosure of digital personal data produces materially the same harm — reputational damage, loss of autonomy, exposure to exploitation — through a different technological medium, it shares the same 'illat and is therefore properly subject to the same normative prohibition, even though digital data processing did not exist at the time the classical texts were revealed or codified.

This analogical extension supports mapping personal data protection to multiple maqasid simultaneously, rather than to a single, isolated objective. First, hifzh al-'irdh (protection of dignity and honor) is engaged directly: unauthorized disclosure of private information, identity misuse, or the publication of confidential data can damage an individual's reputation in ways functionally equivalent to the classical harms the maqasid framework was designed to prevent (Kamali, 2008; Ibn Ashur, 2006). Second, hifzh al-mal (protection of wealth) is engaged because personal data carries direct commercial value in the digital economy; its exploitation without consent can produce financial harm through fraud, identity theft, or unauthorized transactions (Dusuki & Abdullah, 2007). Third — and this is a dimension modern positive law addresses only indirectly — hifzh al-'aql (protection of intellect) is engaged by practices such as algorithmic profiling, targeted manipulation, and disinformation built from harvested personal data, which can distort an individual's capacity for autonomous, rational decision-making. Classical hifzh al-'aql was concerned primarily with intoxicants that impair reasoning; extending it, by the same analogical logic, to the technological manipulation of judgment is a more novel application than extending it to privacy or wealth, and should be treated as a suggestive rather than a settled analogy, pending further juristic scrutiny.

Underlying all three applications is the principle of maslahah: personal data protection generates public benefit by strengthening trust in digital systems and encouraging responsible use of technology, while its absence produces mafsadah through privacy violations, economic exploitation, and structural inequality between individuals and powerful data-holding institutions (Auda, 2008). The principle of amanah (trustworthiness) further frames organizations that collect personal data as holders of an entrusted responsibility rather than mere technical custodians, meaning that data misuse is not only a regulatory breach but a breach of moral trust — a framing that adds an ethical dimension not fully captured by compliance-oriented legal drafting.

3. Privacy, Consent, and Prevention of Harm in Islamic Legal Perspective

Beyond the textual basis discussed above, Islamic legal ethics offer three interlocking principles directly applicable to digital data governance: privacy (established through the prohibition of tajassus), consent (taradhi), and prevention of harm (dar' al-mafasid). The concept of taradhi, mutual agreement free from coercion or

deception, parallels the modern data protection principle of informed consent: individuals should understand what information is collected, why it is collected, and how it will be used before granting permission. Processing personal data without adequate explanation or valid consent introduces uncertainty (gharar) and potential exploitation, which Islamic ethics treat as independently objectionable, not merely as a procedural lapse (Kamali, 2008).

The principle of dar' al-mafasid holds that a practice producing significant harm must be prevented even where it yields benefit to some parties, and that legal systems should act preventively rather than only in response to harm already caused (Auda, 2008). Applied to digital governance, this supports ex ante regulatory measures — data security requirements, purpose limitation, and accountability mechanisms — as consistent with, rather than merely tolerated by, Islamic legal objectives. It is worth noting that contemporary fiqh institutions, including national fatwa bodies and international fiqh academies, have increasingly begun to address questions of information ethics and digital conduct, suggesting that this is a live area of ongoing juristic engagement rather than a purely academic extrapolation; a fuller mapping of specific contemporary fatwa positions is identified here as a direction for further research rather than exhaustively undertaken in this study.

4. Harmonization and Critical Comparison Between Islamic Law and Positive Law

Law Number 27 of 2022 establishes principles of legality, transparency, purpose limitation, security, and accountability. Mapped against Maqasid al-Shariah, these principles correspond closely to identifiable Islamic concepts: the requirement of a lawful basis for processing corresponds to taradhi; the accountability obligations imposed on data controllers correspond to amanah; and the overall protective orientation of the law toward data subjects corresponds to 'adl (justice) and dar' al-mafasid. At this level, the two normative systems are substantively convergent rather than merely superficially compatible.

However, a genuinely comparative analysis must also identify points of divergence, and two are notable. First, Law Number 27 of 2022 is oriented toward procedural and administrative compliance — consent mechanisms, breach notification, administrative sanctions — and does not explicitly address the manipulation of reasoning and judgment through algorithmic profiling or automated decision-making. Maqasid al-Shariah, through the extended application of hifzh al-'aql discussed above, arguably reaches further into this territory by treating the protection of autonomous human judgment as an independent objective, suggesting that Indonesian data protection regulation may need to be supplemented — through implementing regulations or sectoral guidance on automated decision-making — to fully address this dimension. Second, positive law frames obligations primarily in terms of external, sanction-backed compliance, whereas Maqasid al-Shariah frames the same obligations

additionally as internal moral responsibility (amanah) that operates independently of external supervision. This distinction is not merely rhetorical: it implies that Islamic legal ethics can motivate compliance in precisely the gaps — under-resourced enforcement, novel technologies not yet covered by implementing regulations — where administrative sanctions are least effective.

Conversely, positive law offers Maqasid al-Shariah discourse something classical jurisprudence cannot supply on its own: concrete institutional mechanisms — a supervisory authority, defined administrative sanctions, mandatory breach notification timelines, and data protection officer requirements — through which abstract objectives such as amanah and 'adl can be operationalized and enforced at scale. The relationship between the two systems is therefore better characterized as complementary rather than unidirectional: positive law supplies an enforceable structure, and Maqasid al-Shariah supplies ethical justification and identifies normative gaps, particularly around emerging technologies, that positive law has not yet caught up with.

This complementary relationship also underscores that harmonization is an ongoing process rather than a fixed conclusion. As artificial intelligence, automated decision-making, and large-scale data analytics continue to evolve, both legal interpretation and Maqasid-based reasoning must remain adaptive. The principle of maslahah supports this adaptability, as it directs legal reasoning toward achieving objectives rather than confining it to specific historical applications (Auda, 2008).

D. CONCLUSION

This study concludes that personal data protection in the digital era is a contemporary legal issue requiring an approach that integrates legal, ethical, and philosophical perspectives. From the standpoint of *Maqasid al-Shariah*, personal data protection is consistent with the Islamic legal objectives of achieving human welfare (maslahah) and preventing harm (mafsadah), and can be understood as an application of *hifzh al-'irdh* (dignity), *hifzh al-mal* (wealth), and, more tentatively, *hifzh al-'aql* (intellect), grounded textually in the Qur'anic prohibition of tajassus and reinforced by hadith on the concealment of others' faults, and extended to the digital context through explicit analogical reasoning (qiyas) rather than assertion alone.

The comparative analysis shows that Law Number 27 of 2022 and Maqasid al-Shariah share substantial common ground in their treatment of consent, accountability, and justice, but are not fully coextensive: positive law provides enforceable institutional structure that Islamic legal objectives alone cannot supply, while Maqasid al-Shariah identifies an ethical horizon — particularly concerning algorithmic manipulation of human judgment and the moral character of data trusteeship — that current positive regulation has not yet fully addressed. Harmonizing the two frameworks, rather than treating either as sufficient on its own, offers a more comprehensive foundation for

ethical and human-centered digital governance in Indonesia. Future research incorporating a systematic review of contemporary fatwa positions on digital data, as well as an empirical study of enforcement practice under Law Number 27 of 2022, would extend and test the conceptual claims advanced in this study.

REFERENCES:

Al-Ghazali. (1997). Al-Mustasfa min Ilm al-Usul. Beirut: Dar al-Kutub al-Ilmiyyah.

Al-Qur'an, Surah Al-Hujurat (49): 12.

Al-Shatibi. (2004). Al-Muwafaqat fi Usul al-Shariah. Beirut: Dar al-Kutub al-Ilmiyyah.

Auda, J. (2008). Maqasid al-Shariah as Philosophy of Islamic Law: A Systems Approach. London: The International Institute of Islamic Thought (IIIT).

Dusuki, A. W., & Abdullah, N. I. (2007). Maqasid al-Shariah, Maslahah and Corporate Social Responsibility. The American Journal of Islamic Social Sciences, 24(1), 25–45.

Ibn Ashur, M. T. (2006). Treatise on Maqasid al-Shariah. London: The International Institute of Islamic Thought (IIIT).

Kamali, M. H. (2008). Shari'ah Law: An Introduction. Oxford: Oneworld Publications.

Kamali, M. H. (2021). Maqasid al-Shariah Made Simple. London: The International Institute of Islamic Thought (IIIT).

Kuner, C. (2020). The European Union and the General Data Protection Regulation: The New Data Protection Regime. Oxford: Oxford University Press.

Marzuki, P. M. (2005). Penelitian Hukum. Jakarta: Kencana Prenada Media Group.

OECD. (2013). The OECD Privacy Framework. Paris: OECD Publishing.

Sahih Muslim, Hadith on concealing the faults of a fellow Muslim (Kitab al-Birr wa al-Silah wa al-Adab).

Sinta, R., et al. (2023). Perlindungan Data Pribadi dalam Perspektif Hukum Nasional dan Tantangan Era Digital. Jurnal Hukum dan Pembangunan.

Soekanto, S., & Mamudji, S. (2014). Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: Rajawali Pers.

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

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.