

***Contemporary Ijtihad on Biometric Data Protection
in the Perspective of Maqashid al-Syariah***

**Syifa Fedira Az Zahra¹, Zakiyudin Fikri², Afif Nidhomul Ilmi³, Friska Ayudia Ariani⁴,
Muhammad Rizal Firdaus⁵**

^{1,3,4,5}UIN Walisongo Semarang, Indonesia

²Institut Pahlawan 12 Bangka Belitung, Indonesia

Email: fedirasyifa@gmail.com

Abstract

The rapid development of biometric technology carries a high risk to privacy due to the unique and permanent nature of such data. The recurring phenomenon of biometric data breaches in Indonesia indicates significant gaps in the existing data protection system. This research aims to analyze the legal formulation of biometric data protection through contemporary ijtihad and to examine the relevance of the Maqashid Sharia approach in providing protection within the digital era. The research method employed is normative legal research using a statute approach and a conceptual approach. The results indicate that under positive law, biometric data is classified as specific personal data based on Law Number 27 of 2022 concerning Personal Data Protection. From the perspective of Islamic law, contemporary ijtihad based on Maqashid Sharia views the protection of biometric data as an effort to achieve welfare through five essential elements (al-daruriyyat al-khamsah): the protection of life (hifz al-nafs), intellect (hifz al-'aql), property (hifz al-mal), lineage (hifz al-nasl), and honor and privacy (hifz al-'irdh). This approach serves as an ethical-moral foundation that complements the positive legal framework in addressing the rapid dynamics of digital technology.

Keywords: *Contemporary Ijtihad, Biometric Data, Maqashid Sharia, Personal Data Protection.*

Abstrak

Perkembangan teknologi biometrik membawa risiko tinggi terhadap privasi karena sifat datanya yang unik dan permanen. Fenomena kebocoran data biometrik di Indonesia yang terus berulang menunjukkan adanya celah dalam sistem perlindungan data yang ada. Penelitian ini bertujuan untuk menganalisis rumusan hukum perlindungan data biometrik melalui ijtihad kontemporer dan mengkaji relevansi pendekatan Maqashid Syariah dalam memberikan perlindungan di era digital. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Hasil penelitian menunjukkan bahwa dalam hukum positif, data biometrik diklasifikasikan sebagai data pribadi spesifik berdasarkan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dalam perspektif hukum Islam, ijtihad kontemporer berbasis Maqashid Syariah memandang perlindungan data biometrik sebagai upaya mewujudkan kemaslahatan melalui lima unsur pokok (al-daruriyyat al-khamsah), yaitu perlindungan jiwa (hifz al-nafs), akal (hifz al-'aql), harta (hifz al-mal), keturunan (hifz al-nasl), serta kehormatan dan privasi (hifz al-'irdh). Pendekatan ini berfungsi sebagai landasan etis-moral yang melengkapi kerangka hukum positif guna menghadapi dinamika teknologi digital yang pesat.

Kata Kunci: *Ijtihad Kontemporer, Data Biometrik, Maqashid Syariah, Perlindungan Data Pribadi.*

Copyright: © 2026. The Author(s).

KARTIKA: Jurnal Studi Keislaman is licensed under a Creative Commons Attribution- NonCommercial 4.0 International License

A. Introduction

The development of digital technology has brought significant changes in various aspects of human life, including identity management and data security.¹ One prominent form of development is the use of biometric data, such as fingerprints, facial recognition, retina of the eyes, and voice, which are currently widely used in digital security systems, financial services, and government administration.²

In contrast to conventional personal data such as passwords or PINs that can be modified in the event of a leak. Biometric data is unique, permanent, and cannot be modified. These characteristics make it have a very high level of risk in the event of leakage or misuse.³ The impact is not only limited to technical aspects, but also concerns the protection of privacy and human rights.⁴

The phenomenon of data leakage in Indonesia continues to recur on a large scale and increasingly diverse types of data. The data in Table 1.1 shows that leaks involve biometric data directly or indirectly, ranging from facial photos, implicit fingerprints, to immigration data.

Table 1. Data Leak Cases in Indonesia

<i>Year</i>	<i>Types of Leaked Data</i>	<i>Scale (Million Records)</i>	<i>Source</i>
2021	Face photo (KTP-el), implicit fingerprint (NIK connected to Dukcapil)	279	Akbar, 2021 ⁵
2023	Face photo (integrated e-KTP), NIK, biographical data	105	Putri, 2022 ⁶
2024	ASN biometric data, ID card photo, immigration data (fingerprint & implicit iris)	34	Kharismaningtyas, 2024 ⁷
2026	NIK, photo ID card (face), complete biographical data of Dukcapil	240	Dhanya, 2026 ⁸

¹ A. F. Fo et al., "Kemajuan Teknologi Memberikan Kemudahan dalam Interaksi Digital Manusia," *Jurnal Komunikasi Digital* (2025).

² D. A. D. I. Sujiyanto, "Penggunaan Sidik Jari sebagai Otentikasi Identitas Penghadap dalam Minuta Akta Notaris Berbasis Sistem Elektronik" (Master's thesis, Universitas Islam Sultan Agung, 2025).

³ I. P. A. Rizki et al., "Tanggung Jawab Hukum Platform Digital Worldapp Terhadap Pelanggaran Perlindungan Kerahasiaan Data Biometrik Berdasarkan Sistem Hukum Indonesia," *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 1 (2026): 3815–3825.

⁴ M. F. Rizki and A. Salam, "Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. di Yunani dan Inggris)," *Lex Patrimonium* 2, no. 2 (2023).

⁵ C. Akbar, "Data 279 Juta Penduduk Diduga Bocor, BPJS Kesehatan: Pengamanan Ketat Berlapis," *Tempo.co*, 2021.

⁶ A. A. Putri, "Data 105 Juta Penduduk Indonesia Hingga BIN Diduga Bocor, Dave Laksono: Bukti Keamanan Siber Lemah," *Kompas.TV*, 2022.

⁷ Kharismaningtyas, "Hacker" Minta Rp131 Miliar saat Pusat Data Nasional Diserang, Begini Keterangan BSSN,' *Kompas.TV*, 2024.

⁸ D. Dhanya, "Benarkah Data 240 Juta Penduduk Indonesia Dijual di Dark Web," *Tempo.Co*, 2026.

This condition is exacerbated by the practice of massive data collection (*data harvesting*) by certain parties without clear consent from the data owner.⁹ In addition, technological developments allow systems or applications to collect data automatically without direct intervention from the user.¹⁰ This raises the possibility of data being used outside the destination (*data repurposing*)¹¹ and the exploitation of biometric data as a commodity, including through economic incentives such as retinal scans of the eye in exchange for money.¹²

From a positive legal perspective, biometric data protection in Indonesia is regulated through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which classifies biometric data as specific personal data. Prior to the PDP Law, similar arrangements were based on Law Number 11 of 2008 concerning Information and Electronic Transactions. Although this legal framework has been present, its implementation still faces various challenges, especially in keeping up with the dynamics of rapid technological developments.

From an Islamic perspective, data protection is an integral part of efforts to safeguard human welfare.¹³ Maqashid Syariah through five aspects, namely the protection of life (*hifz al-nafs*), heredity (*hifz al-nasl*), reason (*hifz al-'aql*), property (*hifz al-mal*), and honor (*hifz al-'irdh*), provides a relevant normative foundation to respond to the issue of biometric data protection in the digital era.¹⁴ Contemporary ijtihad serves as an instrument to formulate laws on new issues that have not been specifically regulated in the *nash*, while adhering to Sharia principles.¹⁵

Several previous studies have discussed the protection of biometric data and legal responsibility in collecting data without consent, but with different focuses, including the research of Miyuki Fattah Rizki and Abdul Salam¹⁶ review the legal liability of biometric data collection through AI without the consent of the data owner. Then, the Scientific Journal written by Taufik and Zahara¹⁷ discussing the protection of personal data in e-commerce from the perspective of maqashid Sharia. Research by Nurhaida Fahrismia Putri Sembiring and Cahaya

⁹ R. Lesmana and M. I. P. Nasution, "Kebocoran Data di Media Sosial: Analisis Pola dan Strategi Pencegahannya," *Jurnal Administrasi Publik* 2, no. 10 (2025): 123–128.

¹⁰ S. Javaid, "Data Collection Automation: Pros, Cons, & 3 Methods in 2023," Research.Aimultiple.Com, 2023.

¹¹ G. Pearce, "Beware the Privacy Violations in Artificial Intelligence Applications," Isaca.Org, 2023.

¹² K. Safitri and D. Damarjati, "Komdigi: Worldcoin Sudah Kumpulkan Lebih dari 500.000 Data Retina di RI," Nasional.Kompas.Com, 2025.

¹³ Zulham, *Hukum Perlindungan Konsumen* (Edisi Revi) (Jakarta: Kencana, 2013).

¹⁴ N. F. P. Sembiring and C. Permata, "Perlindungan Konsumen Terhadap Keamanan Data Pribadi Pasca Rekam Retina Mata Perspektif Maqashid Syariah," *QANUN: Journal of Islamic Laws and Studies* 4, no. 3 (2026): 1411–1423.

¹⁵ Z. Abidin et al., "Dinamika Tajdid dan Ijtihad dalam Transformasi Pemikiran Hukum Islam Kontemporer," *Journal Research and Education Studies* 6, no. 3 (2025): 1448–1461.

¹⁶ Rizki and Salam, "Pertanggungjawaban Hukum Pengumpulan Data Biometrik."

¹⁷ M. Taufik and F. Zahara, "Pengaturan Perlindungan Data Pribadi dalam E-Commerce Menurut Perspektif Maqashid Syariah (Studi Kasus Marketplace Facebook)," *Jurnal Ilmu Hukum, Humaniora, Dan Politik (JIHHP)* 4, no. 6 (2024): 2378–2392.

Permata¹⁸ researching consumer protection after retinal eye recording. However, the three studies have not specifically integrated contemporary ijtihad as an instrument for the formation of Islamic law with a comprehensive analysis of sharia maqashid in the context of biometric data that covers the entire data management cycle from collection, storage, to misuse. This gap is the focus of this research.

Thus, this research aims to present a construction of Islamic law that is relevant and adaptive to the issue of biometric data protection in the digital era, as well as affirming the function of contemporary ijtihad based on sharia maqashid as a solution to today's technological challenges.

Previous research is an important source of reference for the author in carrying out his research. Through previous research, the author can enrich the theory to be used and add study material in the research being conducted.

First, research conducted by Nurhaida Fahrisma Putri Sembiring and Cahaya Permata entitled "Consumer Protection of Personal Data Security After Retina Eye Recording from the Perspective of Maqashid Syariah". The results of the study show that the phenomenon of retinal eye recording poses a threat to the security of personal data. Based on the perspective of sharia maqashid, the protection of personal data is part of protecting the soul (*hifz al-nafs*), reason (*hifz al-'aql*), and property (*hifz al-mal*). Therefore, specific regulations are needed to determine the parties who have the right to record the retina of the eye and provide protection for consumers in the digital era.

Second, research conducted by Syarifah Tri Utami Wahyuningati,¹⁹ entitled "Supervision of Personal Data Protection in Indonesia from the perspective of Maqashid Syariah". The results of the study explain the increase in supervision of personal data protection, especially in the security sector. Then, from the perspective of maqashid Sharia, it illustrates that in protecting this personal data, we must be able to protect our souls and protect our property, where the property in question is personal data.

Third, research conducted by Miyuki Fattah Rizki and Abdul Salam²⁰ titled "Legal Accountability of Biometric Data Collection Through Artificial Intelligence Without Data Owner's Consent (Clearview AI Inc. Case Study in Greece and the United Kingdom)". Where this study concludes that biometric data protection in Indonesia can be found in the provisions of the Law on Information and Electronic Transfer and the Law on Personal Data Protection,

¹⁸ Sembiring and Permata, "Perlindungan Konsumen Terhadap Keamanan Data Pribadi."

¹⁹ S. T. U. Wahyuningati, "Pengawasan Terhadap Perlindungan Data Pribadi di Indonesia Perspektif Maqashid Syariah" (Thesis, UIN Maulana Malik Ibrahim Malang, 2023).

²⁰ Rizki and Salam, "Pertanggungjawaban Hukum Pengumpulan Data Biometrik."

examples of such protection are the rights of the data owner and consent related to data processing.

From previous research, there are similarities and differences with the current research. This research has similarities with previous research in terms of both discussing the issue of personal data protection, especially biometric data, as a contemporary legal issue that requires adequate regulation and protection. This research also has similarities in the use of the perspective of maqashid sharia as an analytical framework to see data protection as part of efforts to maintain benefits and prevent harm.

The difference between this research and previous researches, this study specifically examines the protection of biometric data through the construction of contemporary ijtihad as a method of discovering Islamic law on modern digital issues, by making maqashid sharia as a normative as well as methodological framework. This study not only discusses data protection from a positive legal aspect or consumer security, but also analyzes the status of biometric data protection as part of the protection of life (*hifz al-nafs*), reason (*hifz al-'aql*), property (*hifz al-mal*), heredity (*hifz al-nasl*), and honor and privacy (*hifz al-'irdh*). Thus, the novelty of this research lies in the integration of contemporary ijtihad and sharia maqashid in formulating biometric data protection in response to the development of digital technology.

B. Research Methods

The type of research used is normative juridical, which is a research approach method that is carried out based on the main legal material by examining theories, concepts, legal principles, and laws and regulations.²¹ The research method used is normative law. According to Mahmud Marzuki, normative legal research is a process to find a legal rule, legal principles and legal doctrines to answer the legal problems that are being faced related to the phenomenon of biometric data.²²

The approaches used include the statute approach, and the conceptual approach. Statute approach is an approach to review laws and regulations or regulations that are relevant to problem research.²³ Conceptual approach is an approach that moves from the views and doctrines that develop in law, so that the researcher will find an idea or thought and will be a support for the researcher in stringing together a legal argument in solving a legal problem related to contemporary ijtihad on biometric data protection in the perspective of sharia maqashid.²⁴

²¹ J. Efendi and J. Ibrahim, *Metode Penelitian Hukum Normatif dan Empiris (Pertama)* (Jakarta: Prenada Media Group, 2016).

²² P. M. Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Group, 2007).

²³ Marzuki, *Penelitian Hukum*.

²⁴ F. Setyawan, "Metodologi Pendekatan dalam Penelitian Hukum," Bahan ajar makalah disampaikan dalam Pelatihan Metodologi Penelitian dan Penulisan Hukum, Universitas Jember, 2010.

C. Result and Discussion

1. Legal Protection of Biometric Data in Applicable Laws and Regulations in Indonesia

Biometric technology has become one of the leading innovations in physical security systems, allowing organizations to improve the security and reliability of access through identification and verification based on an individual's biological or behavioral characteristics. While biometric technology offers a high level of security, it is inevitable that it also has its drawbacks and drawbacks. Biometric data leaks, technology manipulation, and fake attacks are some of the risks that need to be addressed. Legal protection is a protection given to legal subjects in accordance with the rule of law, both written and unwritten in the context of law enforcement. Legal protection can be divided into two types, namely:²⁵

First, preventive legal protection is a form of protection that is oriented towards prevention efforts so that problems or disputes do not occur. This form of protection is realized through laws and regulations designed to prevent violations, especially the misuse of personal data, while providing limitations and guidelines in the implementation of rights and obligations.²⁶ Through this preventive approach, the state seeks to minimize the potential for data misuse that still often occurs in Indonesia. Law Number 27 of 2022 concerning Personal Data Protection is present as a legal instrument that provides guarantees certainty and protection for the personal data of Indonesian citizens, especially in the face of rapid developments in digital technology.²⁷

One type of personal data that gets special regulation in the Personal Data Protection Law is biometric data. Based on the provisions of Article 4 paragraph (1) and paragraph (2) of the PDP Law, biometric data is included in a specific category of personal data. This classification is based on the nature of biometric data that is closely related to a person's physical characteristics or characteristics, so it can be used to identify individuals, such as through face, fingerprints, retina of the eye, or DNA. If biometric data is collected and stored in a database system, it can be used as a means of identity verification.

Article 1 number 6 of the PDP Law explains that the subject of personal data is an individual who has a direct relationship with the personal data attached to him. Furthermore, Article 3 of the PDP Law regulates several principles in the protection of

²⁵ Muchsin, *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia* (Surakarta: Universitas Sebelas Maret, 2003).

²⁶ S. T. U. Wahyuningati, "Pengawasan Terhadap Perlindungan Data Pribadi di Indonesia Perspektif Maqashid Syariah" (Thesis, UIN Maulana Malik Ibrahim Malang, 2023).

²⁷ E. Priliyasi, "Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan di Indonesia," *Jurnal RechtsVinding* 12, no. 2 (2023): 261–279.

personal data, including: 1) The principle of protection, which requires the processing of personal data to be carried out with the aim of protecting data from misuse; 2) The principle of legal certainty, which requires the processing of personal data on a legal basis to ensure the legality of data protection; 3) The principle of accountability, where the party processing the data must act responsibly and maintain a balance of rights and obligations of all related parties; and 4) The principle of confidentiality, which requires that personal data be protected from unauthorized access or processing by unauthorized parties.²⁸

According to Article 16 paragraph (1) of the PDP Law, the processing of personal data includes the acquisition and collection, processing and analysis, storage, dissemination, and deletion of data. In addition, Article 16 paragraph (2) of the PDP Law stipulates principles in the processing of personal data, such as the collection of data must be lawful and transparent, the processing must be in accordance with the purpose, guarantee the rights of the data subject, and be carried out accurately and not misleadingly.²⁹ Then, in Articles 20 and 21 of the PDP Law, it is emphasized that the rights of data subjects must be maintained comprehensively, starting from the provision of information to control over the period and purpose of processing.³⁰

Therefore, given that biometric data has a high level of sensitivity and is able to accurately represent an individual's identity, the process of collecting, storing and managing it must be carried out carefully. This is important because misuse of biometric data by unauthorized parties can pose a serious risk to the security, privacy, and rights of individuals.

Second, the protection of Repressive Law is protection that aims to solve a problem that occurs, with an end that is manifested in the form of sanctions, for example fines, imprisonment, and additional punishments if there is a dispute or if there is a violation.³¹ In Law Number 27 of 2022 concerning Personal Data Protection, which discusses the resolution of a problem that occurs and the rule is stated in Article 68 which regulates every person who deliberately falsifies personal data for the benefit of themselves or other parties to the detriment of others, can be sentenced to a maximum of 6 years in prison and/or a maximum fine of IDR 6 billion. Furthermore, Law No. 19 of 2016 concerning

²⁸ M. E. Darnia et al., "Perlindungan Data Identitas Konsumen Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Jurnal Ilmiah Wahana Pendidikan* 10, no. 9 (2024): 405–412.

²⁹ U. Mutiara and R. Maulana, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi," *Indonesian Journal of Law and Policy Studies* 10, no. 1 (2020).

³⁰ M. F. Rizki and A. Salam, "Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. di Yunani dan Inggris)," *Lex Patrimonium* 2, no. 2 (2023).

³¹ Muchsin, *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia*.

Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions listed in Article 45B also explains that people who deliberately and without the right send Electronic Information and/or Electronic Documents containing threats of violence or intimidation aimed at them personally, are punished with a maximum prison sentence of 4 (four) years and/or a maximum fine of Rp750,000,000, 00 (seven hundred and fifty million rupiah).³²

2. Contemporary Ijtihad Formulating Biometric Data Protection Law in the Perspective of Sharia Maqashid

The UUPK and the PDP Law affirm the importance of safe, transparent, and responsible management of personal data as a form of legal protection for consumers in the digital era.³³ Not only from a positive legal perspective, personal data protection also needs to be carried out in the concept of sharia maqashid.

Maqashid al-Shari'ah is composed of two terms, namely maqashid and shari'ah. The term maqashid is a plural form of maqṣad which means purpose or purpose, while shari'ah is interpreted as a set of legal provisions of Allah SWT that are set for humans as a guideline for life in order to achieve benefits and happiness, both in this world and in the hereafter.³⁴ According to Imam al-Ghazali quoted from Nurhaida's research, maqashid al-shari'ah is a concept that focuses on efforts to maintain the five main elements (al-ḍaruriyyat al-khamsah), namely maintaining religion (ḥifẓ al-din), preserving the soul (ḥifẓ al-nafs), preserving reason (ḥifẓ al-'aql), preserving posterity (ḥifẓ al-nasl), and preserving wealth (ḥifẓ al-mal). These five elements must be maintained and realized in various levels of benefit, starting from the level of dharuriyah, hajiyah, and tahsiniyah.³⁵ Some contemporary scholars add a sixth element, namely honor (ḥifẓ al-'irdh), which is increasingly relevant in the context of protecting human privacy and dignity in the digital age.³⁶ The following is an explanation of biometric data protection from the perspective of digital Sharia maqashid:³⁷

³² Wahyuningati, "Pengawasan Terhadap Perlindungan Data Pribadi di Indonesia Perspektif Maqashid Syariah."

³³ Herman and A. E. F. Anatasya, "Perlindungan Konsumen Online Dalam Perspektif Maqashid al-Shari'ah: Studi Sosio-Legal di Indonesia," *Qisthosia "Jurnal Syariah & Hukum"* 6, no. 1 (2025): 50–60.

³⁴ Z. Abidin et al., "Dinamika Tajdid dan Ijtihad dalam Transformasi Pemikiran Hukum Islam Kontemporer," *Journal Research and Education Studies* 6, no. 3 (2025): 1448–1461.

³⁵ N. F. P. Sembiring and C. Permata, "Perlindungan Konsumen Terhadap Keamanan Data Pribadi Pasca Rekam Retina Mata Perspektif Maqashid Syariah," *QANUN: Journal of Islamic Laws and Studies* 4, no. 3 (2026): 1411–1423.

³⁶ A. C. Ibriy, "Kedaulatan Data: Menjaga Martabat Digital Umat dalam Perspektif Maqashid al-Syari'ah," *Islami.Co*, 2025.

³⁷ M. Anshari and C. Permata, "Deforestasi Hutan Lindung dalam Proyek Strategis Nasional Food Estate: Perspektif Maqashid Syariah," *Al Qalam: Jurnal Ilmiah Keagamaan Dan Kemasyarakatan* 18, no. 3 (2024): 2031–2047.

- *Hifz al-nafs* (Life Protection), *Hifz al-nafs* means maintaining and protecting the safety of human life from all forms of physical and non-physical threats, including threats. An example of a case of biometric data that occurs is INAFIS fingerprint data related to a person's forensic track record, if leaked or manipulated, can threaten the safety of an individual's life (*hifz al-nafs*) through abuses in the justice system.³⁸

Within the framework of *hifz al-nafs*, all forms of actions that have the potential to threaten the safety of human lives directly or indirectly are something that must be prevented. Therefore, the practice of collecting biometric data without consent is an act contrary to this principle, as it puts individuals in vulnerable conditions without being able to protect themselves.

- *Hifz al-'aql* (Protection of Reason), *Hifz al-'aql* means to protect the intellect from all forms of manipulation, misrepresentation of information, and actions that can damage the consciousness of rational human thinking. Biometric data leaks that are carried out without adequate explanation, or in a way designed to obscure risks, are a form of manipulation of a person's rational capacity to make decisions. Islam requires that every transaction and legal action be based on free will and sufficient understanding. When a person submits his biometric data without fully understanding the consequences to be incurred, the consent given becomes invalid under Islamic law, because it does not meet the conditions of *'ilm* (knowledge) and *ikhtiyar* (freedom of choice) which are the foundation of the validity of the contract in fiqh.
- *Hifz al-mal* (Property Protection), *Hifz al-mal* means protecting property from theft, fraud, and all forms of economic abuse that can harm individuals or society. Biometric data leaks can lead to financial losses, such as account break-ins, illegal online loans, or identity theft for financial transactions. An example of a case that has occurred is an online loan that is disbursed by an unauthorized party, only with a photo of an ID card that shows a person's face.³⁹ This case violates the side *Hifz Al-Mal*, the misuse of facial photos for illegal credit access is property theft that is tricked through biometric technology as a form of forfeiture. In muamalah, Islam demands that no one should be treated as an object of exploitation, and that every transaction must be based on willingness (*Taradin*) that is free from manipulation.

³⁸ S. Hartini, "Penggunaan Teknologi Biometrik dalam Identifikasi Perlindungan Data Pribadi Berdasarkan Peraturan Menteri Hukum dan HAM Nomor 37 Tahun 2016" (Thesis, UIN Sayyid Ali Rahmatullah Tulungagung, 2024).

³⁹ S. T. Ardana and Y. Kornelis, "Penyalahgunaan Data Pribadi Pada Pinjaman Online di Indonesia: Analisis Perlindungan dan Sanksi Hukum," *Jurnal Perundang Undangan Dan Hukum Pidana Islam* 9, no. 1 (2024): 1–11.

- *Hifz al-Nasl* (Ancestry Protection), *Hifz Al-Nasl* Actually, it is related to the issue of genetic and biometric data that is hereditary. DNA data, for example, not only contains information about the individual in question, but also reveals the biological profile of the entire family and its descendants. This kind of data leak has the potential to cause genetic-based discrimination that has a direct impact on the fate of a person's descendants. In the framework *maqashid*, protection of offspring not only means maintaining the continuity of reproduction, but also protecting the dignity and future of future generations from all forms of exploitation rooted in inherited biological identity. As AI technology develops, leaked facial and voice data can be used to create content *deepfake* or video and audio manipulation that shows someone doing things they never did.⁴⁰ This case not only harms the honor of individuals, but also impacts their families and descendants through defamation that is difficult to remove from the digital space.
- *Hifz al-'Irdh* (Protection of Honor and Privacy), *hifz al-'irdh* is the most directly in contact with the issue of biometric data. Biometric data is an identity that is inherent and inseparable from a person's personality, this data is not just a number or code that can be replaced, but is a physical manifestation of the dignity and identity of the individual. When biometric data is leaked or misused, what is harmed is not only material interests, but also the honor (*'irdh*) of a person in the deepest sense, namely the right to control one's image, identity, and existence in front of others.

Islam takes great care of the privacy of individuals. This is reflected in various *nash* that prohibit the act of spying (*tajassus*), reveal the secrets of others (*ifsha' al-sirr*), and degrade human dignity. In the digital context, all of these prohibitions have a tangible equivalent: unauthorized facial scanning is a form of contemporary *tajassus*, the dissemination of biometric data is *ifsha' al-sirr* in the digital age, and the commodification of one's biological identity is a form of insult to human dignity that is fundamentally contrary to Islamic values.

3. The Relevance of the Maqashid Syariah Approach in Providing Protection for Biometric Data in the Digital Era

The relevance of sharia *maqashid* does not stop at the internal normative level of Islamic law, but also serves as an ethical foundation that can strengthen and complement the existing positive legal framework. Law Number 27 of 2022 concerning Personal Data Protection has indeed regulated a juridical-formal protection mechanism, but positive law

⁴⁰ M. A. Chairani, K. Yitawati, and A. P. Pradhana, "Urgensi Pengaturan Hukum bagi Penyalahgunaan Aplikasi Deepfake," *Jurnal Rechtsens* 13, no. 1 (2024): 81–96.

has inherent limitations in keeping up with the pace of technological development. This is where the sharia maqashid plays a significant complementary role.

One of the verses relevant to the protection of personal data is Q.S An-Nur [24]:27

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْذِنُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكَ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ

O you who have believed, do not enter a house that is not your home before asking permission and greeting its occupants. Thus it is better for you to take a lesson.

Ibn Assyria, a commentator, explained that the house is the most personal place for a person. Islam prohibits entry without permission because there may be things in it that you do not want to show to others. This concept can be extended to the digital era, where personal data is like a person's digital home. Just like a physical house that cannot be entered without permission, personal data should also not be accessed or used without the owner's permission. QS. An-Nur verse 27 is relevant and has a correlation with this research, namely the collection and processing of biometric data without the clear consent of the owner is contrary to Islamic sharia values and the principles of maqashid shari'ah which emphasizes the protection of life, property, intellect, descendants, as well as honor and privacy.

In addition, the practice of collecting biometric data without consent also violates the principles of fiqh in accordance with the words of the Prophet (peace and blessings of Allaah be upon him) from Ibn Abbas (may Allah be pleased with him) narrated by Imam Ahmad, Ibn Majah, and others:

لَا ضَرَرَ وَلَا ضِرَارَ

It is not permissible to do anything that endangers oneself or others.

From this it can be seen that dharar (doing something harmful) is forbidden in the Shari'a. Therefore, it is not permissible for a Muslim to do something that endangers himself or his fellow Muslims, either in the form of words or deeds, without a valid reason.⁴¹ Biometric data collected without the owner's knowledge is a form of violation of the rights of individuals protected by sharia, as it puts a person at risk of being unknown and unapproved by.

If the PDP Law works through external mechanisms of regulation, sanctions, and law enforcement, then the sharia maqashid instills an internal moral awareness in every actor, whether individuals, corporations, or state administrators, that the protection of biometric data is not just a legal obligation, but a religious moral obligation whose

⁴¹ Almanhaj, "Kaidah Ke. 15: Tidak Boleh Melakukan Sesuatu yang Membahayakan," *Almanhaj.or.Id*, 2009.

responsibility goes beyond the boundaries of secular judicial institutions. The integration of the two will create a stronger protection system from the outside through the rule of law, and from the inside through ethical values rooted in the belief to protect the benefit of self and others.

Thus, the sharia maqashid approach has proven to be relevant, adaptive, and urgent as a solution to the problem of biometric data protection in the digital era. It is not only able to respond to the challenges that exist today, but also equips Islamic law with normative flexibility to continue to evolve as technology develops.

D. Conclusion

Based on the discussion that has been described, it can be concluded that biometric data protection is a contemporary legal issue that requires a multidimensional approach, both through positive law and Islamic law. In Indonesia's positive legal perspective, the protection of biometric data has gained a juridical basis through Law Number 27 of 2022 concerning Personal Data Protection.

From the perspective of Islamic law, contemporary ijthad is an important instrument in formulating laws on the issue of biometric data that has not been explicitly regulated in the nash. Through the sharia maqashid approach, biometric data protection is understood as part of efforts to realize the benefits and prevent mafsadat, especially in protecting the soul (*hifz al-nafs*), reason (*hifz al-'aql*), property (*hifz al-mal*), heredity (*hifz al-nasl*), and honor and privacy (*hifz al-'irdh*). Thus, the collection, processing, or use of biometric data without valid consent is contrary to sharia principles. Contemporary ijthad based on sharia maqashid can be a solution in responding to the dynamics of modern technology, especially related to biometric data protection.

References

- Abidin, Z., F. A. Sari, I. F. Sitorus, A. N. Sitorus, and A. Rahmadani. "Dinamika Tajdid dan Ijtihad dalam Transformasi Pemikiran Hukum Islam Kontemporer." *Journal Research and Education Studies* 6, no. 3 (2025): 1448–1461.
- Akbar, C. "Data 279 Juta Penduduk Diduga Bocor, BPJS Kesehatan: Pengamanan Ketat Berlapis." [Tempo.Co](https://tempo.co), 2021.
- Almanhaj. "Kaidah Ke. 15: Tidak Boleh Melakukan Sesuatu yang Membahayakan." *Almanhaj.or.Id*, 2009.
- Anshari, M., and C. Permata. "Deforestasi Hutan Lindung dalam Proyek Strategis Nasional Food Estate: Perspektif Maqashid Syariah." *Al Qalam: Jurnal Ilmiah Keagamaan Dan Kemasyarakatan* 18, no. 3 (2024): 2031–2047.
- Ardana, S. T., and Y. Kornelis. "Penyalahgunaan Data Pribadi Pada Pinjaman Online di Indonesia: Analisis Perlindungan dan Sanksi Hukum." *Jurnal Perundang Undangan Dan Hukum Pidana Islam* 9, no. 1 (2024): 1–11.
- Chairani, M. A., K. Yitawati, and A. P. Pradhana. "Urgensi Pengaturan Hukum bagi Penyalahgunaan Aplikasi Deepfake." *Jurnal Rechts* 13, no. 1 (2024): 81–96.

- Darnia, M. E., M. Amelia, I. Wulandari, T. Ariani, O. Anggraini, M. F. Syahputra, and M. A. S. Syuhada. "Perlindungan Data Identitas Konsumen Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Jurnal Ilmiah Wahana Pendidikan* 10, no. 9 (2024): 405–412.
- Dhanya, D. "Benarkah Data 240 Juta Penduduk Indonesia Dijual di Dark Web." [Tempo.Co](https://tempo.co), 2026.
- Efendi, J., and J. Ibrahim. *Metode Penelitian Hukum Normatif dan Empiris*. Pertama. Jakarta: Prenada Media Group, 2016.
- Fo, A. F., G. R. Bunga, S. C. A. Kawengian, and V. K. Saragih. "Kemajuan Teknologi Memberikan Kemudahan dalam Interaksi Digital Manusia." *Jurnal Komunikasi Digital*, 2025.
- Hartini, S. "Penggunaan Teknologi Biometrik dalam Identifikasi Perlindungan Data Pribadi Berdasarkan Peraturan Menteri Hukum dan HAM Nomor 37 Tahun 2016." Thesis, UIN Sayyid Ali Rahmatullah Tulungagung, 2024.
- Herman, and A. E. F. Anatasya. "Perlindungan Konsumen Online Dalam Perspektif Maqāṣid al-Shari'ah: Studi Sosio-Legal di Indonesia." *Qisthosia "Jurnal Syariah & Hukum"* 6, no. 1 (2025): 50–60.
- Ibriy, A. C. "Kedaulatan Data: Menjaga Martabat Digital Umat dalam Perspektif Maqashid al-Syari'ah." [Islami.Co](https://islami.co), 2025.
- Javaid, S. "Data Collection Automation: Pros, Cons, & 3 Methods in 2023." [Research.Aimultiple.Com](https://research.aimultiple.com), 2023.
- Kharismaningtyas. "'Hacker' Minta Rp131 Miliar saat Pusat Data Nasional Diserang, Begini Keterangan BSSN." [Kompas.TV](https://kompas.tv), 2024.
- Lesmana, R., and M. I. P. Nasution. "Kebocoran Data di Media Sosial: Analisis Pola dan Strategi Pencegahannya." *Jurnal Administrasi Publik* 2, no. 10 (2025): 123–128.
- Marzuki, P. M. *Penelitian Hukum*. Jakarta: Kencana Prenada Group, 2007.
- Muchsin. *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia*. Surakarta: Universitas Sebelas Maret, 2003.
- Mufatikhaturohmah, S., and Zulaikha. "Pengaruh Teknologi Biometrik dan Jaminan Keamanan Cyber Terhadap Minat Transaksi Perbankan Online di Provinsi Lampung dalam Perspektif Islam." *Jurnal Informatika Ekonomi Bisnis* 7, no. 2 (2025).
- Mutiara, U., and R. Maulana. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi." *Indonesian Journal of Law and Policy Studies* 10, no. 1 (2020).
- Pearce, G. "Beware the Privacy Violations in Artificial Intelligence Applications." [Isaca.Org](https://isaca.org), 2023.
- Priliasari, E. "Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan di Indonesia." *Jurnal RechtsVinding* 12, no. 2 (2023): 261–279.
- Putri, A. A. "Data 105 Juta Penduduk Indonesia Hingga BIN Diduga Bocor, Dave Laksono: Bukti Keamanan Siber Lemah." [Kompas.TV](https://kompas.tv), 2022.
- "QS. An Nur Ayat 27." *Quran.Nu.or.Id*. n.d.
- Rizki, I. P. A., B. G. A. Rama, N. P. S. Nandari, and K. S. W. Putra. "Tanggung Jawab Hukum Platform Digital Worldapp Terhadap Pelanggaran Perlindungan Kerahasiaan Data Biometrik Berdasarkan Sistem Hukum Indonesia." *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 1 (2026): 3815–3825.
- Rizki, M. F., and A. Salam. "Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. di Yunani dan Inggris)." *Lex Patrimonium* 2, no. 2 (2023).
- Safitri, K., and D. Damarjati. "Komdigi: Worldcoin Sudah Kumpulkan Lebih dari 500.000 Data Retina di RI." [Nasional.Kompas.Com](https://nasional.kompas.com), 2025.

- Sembiring, N. F. P., and C. Permata. "Perlindungan Konsumen Terhadap Keamanan Data Pribadi Pasca Rekam Retina Mata Perspektif Maqashid Syariah." *QANUN: Journal of Islamic Laws and Studies* 4, no. 3 (2026): 1411–1423.
- Setyawan, F. "Metodologi Pendekatan dalam Penelitian Hukum." Bahan ajar makalaah disampaikan dalam Pelatihan Metodologi Penelitian dan Penulisan Hukum. Universitas Jember, 2010.
- Sujiyanto, D. A. D. I. "Penggunaan Sidik Jari sebagai Otentikasi Identitas Penghadap dalam Minuta Akta Notaris Berbasis Sistem Elektronik." Master's thesis, Universitas Islam Sultan Agung, 2025.
- Taufik, M., and F. Zahara. "Pengaturan Perlindungan Data Pribadi dalam E-Commerce Menurut Perspektif Maqashid Syariah (Studi Kasus Marketplace Facebook)." *Jurnal Ilmu Hukum, Humaniora, Dan Politik (JIHHP)* 4, no. 6 (2024): 2378–2392.
- Wahyuningati, S. T. U. "Pengawasan Terhadap Perlindungan Data Pribadi di Indonesia Perspektif Maqashid Syariah." Thesis, UIN Maulana Malik Ibrahim Malang, 2023.
- Zulham. *Hukum Perlindungan Konsumen*. Edisi Revisi. Jakarta: Kencana, 2013.