



Building Digital Justice: Reinterpreting *Hifz al- 'Irḍ* in Personal Data Protection and Legal Aid for Data Breach Victims in Indonesia

**Ika Pusparini Anindita Jayasinga,¹ Agus Triono,^{2*} Muhammad Akib,³ Elfa Murdiana,⁴
Muhimmatul Mukaromah⁵**

^{1 2 3} Universitas Lampung, Indonesia

⁴ Universitas Islam Negeri Jurai Siwo Lampung, Indonesia

⁵ International Islamic University Malaysia

*Corresponding Author: agus.triono@fh.unila.ac.id

DOI: <https://doi.org/10.21154/justicia.v23i2.13432>

Received: March 13, 2026

Revised: June 28, 2026

Accepted: July 30, 2026

Abstract: This article examines the systemic failure of personal data protection in Indonesia as an issue that goes beyond technical and regulatory shortcomings and touches the very core of human dignity. Although Law No. 27 of 2022 on Personal Data Protection has provided normative consolidation, the legal ecosystem underpinning it remains fragile: a non-independent supervisory body, structurally weak enforcement mechanisms, and systemic inequities in access to justice render data subjects' rights illusory. This article employs a normative-empirical method with three complementary approaches: the legal philosophy approach is used to deconstruct the paradigmatic assumptions underpinning the data protection regime and reconstruct it on the foundation of human dignity; the conceptual approach is used to redefine *'irḍ* from social reputation toward digital identity and data sovereignty; and the *maqāsid al-sharīa* approach within Jasser Auda's framework is used to assess the normative adequacy of the existing regime and to construct an argument that data protection must be classified as *ḍarūriyyāt*—a primary necessity—because its violation simultaneously threatens *hifz al-nafs*, *hifz al- 'aql*, *hifz al-māl*, and *hifz al- 'irḍ*. Based on these findings, this article proposes a *Maqasid-Oriented Legal Aid* (MOLA) model that operates across three dimensions: restorative, preventive-structural, and community-based accessibility. The main contribution of this article is the redefinition of data protection as an active and affirmative mandate of *hifz al- 'irḍ*, while also offering a framework for legal aid that is normatively robust and institutionally realistic in the Indonesian context.

Keywords: personal data protection; legal aid; digital justice.

Abstrak: Artikel ini bertujuan mengkaji kegagalan sistemik perlindungan data pribadi di Indonesia sebagai persoalan yang melampaui defisit teknis-regulatif

dan menyentuh inti martabat manusia. Meskipun UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi telah menghadirkan konsolidasi normatif, ekosistem hukum yang menopangnya tetap rapuh: lembaga pengawas yang tidak independen, mekanisme penegakan yang lemah secara struktural, dan ketimpangan akses keadilan yang sistemik menjadikan hak-hak subjek data bersifat *illusory*. Artikel ini menggunakan metode normatif-empiris dengan tiga pendekatan yang saling melengkapi: pendekatan filsafat hukum digunakan untuk membongkar asumsi paradigmatis yang mendasari rezim perlindungan data dan merekonstruksinya di atas fondasi martabat manusia; pendekatan konseptual digunakan untuk mendefinisikan ulang *‘ird* dari reputasi sosial menuju identitas digital dan kedaulatan data; serta pendekatan *maqāṣid al-syarīah* dalam kerangka Jasser Auda digunakan untuk menilai kecukupan normatif rezim yang ada dan membangun argumen bahwa perlindungan data harus diklasifikasikan sebagai *darūriyyāt* sebagai keniscayaan primer karena pelanggarannya secara simultan mengancam *ḥifẓ al-naḥs*, *ḥifẓ al-‘aql*, *ḥifẓ al-māl*, dan *ḥifẓ al-‘ird*. Berdasarkan temuan tersebut, artikel ini mengusulkan model *Maqasid-Oriented Legal Aid* (MOLA) yang beroperasi dalam tiga dimensi: restoratif, profilaktis-struktural, dan aksesibilitas berbasis komunitas. Kontribusi utama artikel ini adalah redefinisi perlindungan data sebagai mandat *ḥifẓ al-‘ird* yang aktif dan afirmatif, sekaligus menawarkan kerangka bantuan hukum yang secara normatif kuat dan secara institusional realistis dalam konteks Indonesia.

Kata Kunci: perlindungan data pribadi; bantuan hukum; keadilan digital.



Copyright: © 2026 by author (s). This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Introduction

Digital transformation in Indonesia has brought about fundamental changes in the relationship between citizens, the state, and electronic system operators. Yet beneath this expanded access and the gains in service efficiency lies a structural problem: the escalating leakage and exploitation of personal data on an ever-widening scale. A 2024 report by the Indonesian Cyber Security Forum (ICSF) indicates that more than 2.3 billion records allegedly belonging to Indonesian citizens have circulated across various dark web forums over the past three years.¹ The official National Cyber Security Report issued by the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN) confirms the unauthorized exploitation of more than 56 million

¹ verihubs, "Statistik Cybercrime Indonesia 2025-2026: Data Dan Tren Terbaru," accessed April 17, 2026, <https://verihubs.com/blog/statistik-cybercrime-indonesia>; Sholahuddin Al-Fatih and Zaka Firma Aditya, "The legal protection against terrorism suspects in indonesia (case study of the arrest process of terrorism suspects by densus 88)," *Legality : Jurnal Ilmiah Hukum* 27, no. 1 (July 2019): 14–26.

personal records drawn from 461 public and private institutions.² The government sector sits at the epicenter of this vulnerability, accounting for the highest impact at 58.34%, followed by the financial sector at 3.58%.³ This systemic failure is borne out by a succession of breaches of staggering magnitude, including the compromise of 6 million Taxpayer Identification Number (Nomor Pokok Wajib Pajak, NPWP) records and the exfiltration of data belonging to 200 million BPJS Kesehatan members.⁴ The tangible implications of this vulnerability have now mutated from mere conventional financial loss into an instrument for the destruction of human dignity.⁵ As a consequence, victims of these breaches endure a form of secondary digital repression, massive psychological intimidation through entrapment by illegal online lending⁶, cyber-enabled extortion⁷, and even character assassination that corrodes their social reputation.⁸

The crisis reached a more severe juncture with the Brain Cipher ransomware attack on the Temporary National Data Center (Pusat Data Nasional Sementara, PDNS) 2 in June 2024, which disrupted services for hundreds of government agencies and impaired public services across multiple sectors.⁹ This incident demonstrated that data vulnerability inflicts not only economic harm but also obstructs the exercise of citizens' rights to education, public administration, and access to basic services. Against this backdrop, national law has in fact already laid a normative foundation

² Iskandar, "Data Pemerintah Dominasi 58 Persen Kebocoran Di Dark Web, Platform Baru Ini Tawarkan Deteksi Dini," *Liputan6.Com* (Jakarta), 2025.

³ Fendi Darmawan and Henry Arianto, "Upaya Perlindungan Hukum Dan Tanggung Jawab Kemkomdigi Terhadap Korban Kebocoran Data Pribadi Di Indonesia," *Arus Jurnal Sosial Dan Humaniora* 5, no. 3 (December 2025): 3678–88, <https://doi.org/10.57250/ajsh.v5i3.1741>; Sholahuddin Al-Fatih et al., "Academic Freedom of Expression in Indonesia: A Maqashid Sharia Notes," *El-Mashlahah* 13, no. 2 (December 2023): 203–24, <https://doi.org/10.23971/el-mashlahah.v13i2.7573>.

⁴ Aryo Putranto, "Kebocoran Data 6 Juta Wajib Pajak Termasuk Jokowi Diklaim Ulah Peretas Bjorka," *Kompas.Com* (Jakarta), 2024.

⁵ Saleh Hashem Al-Farjani and Waheed Alazhari, "Bridging Law, Technology, and Justice in the Digital Ag," *Indonesian journal of sustainability* 5, no. 1 (February 2026): 37, <https://doi.org/10.30659/ijsunissula.5.1.37-49>.

⁶ Shohiban Azkaa Muzakkie and Eka Juarsa, "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Pada Aplikasi Pinjaman Online Ilegal Menurut Undang-Undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Bandung Conference Series: Law Studies* 3, no. 2 (August 2023): 984–87, <https://doi.org/10.29313/bcsls.v3i2.7284>.

⁷ Uu Nurul Huda, Dian Rachmat Gumelar, and Alwi Al Hadad, "Fortifying Democracy: Deploying Electoral Justice for Robust Personal Data Protection in the Indonesian Election," *Khazanah Hukum* 6, no. 1 (March 2024): 24–33, <https://doi.org/10.15575/kh.v6i1.30734>.

⁸ Arabin Sandika, Cholidi Zainuddin, and Arief Wisnu Wardhana, "Legal Protection For Victims Of Misuse Of Personal Data When Making Online Loans," *Jurnal ilmiah advokasi* 12, no. 2 (August 2024): 305–16, <https://doi.org/10.36987/jiad.v12i2.5503>.

⁹ BBC.News Indonesia, "Pusat Data Nasional Sementara Lumpuh Akibat Ransomware, Mengapa Instansi Pemerintah Masih Rentan Terhadap Serangan Siber?," accessed 2024, <https://www.bbc.com/indonesia/articles/cxee2985jrvo>.

through Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia and Law Number 27 of 2022 on Personal Data Protection (UU PDP). These legal instruments, however, have yet to address the problem of victim recovery fully. Because the regulatory orientation still rests on administrative compliance and institutional governance, data protection is understood largely as safeguarding information rather than protecting the human beings behind that data.

These limitations become evident in the lived experiences of victims. Preliminary findings from interviews with several data-breach victims who received assistance from a legal aid office in Lampung Province reveal that the impact of data leakage does not end with the loss of control over personal information. Informants described experiences ranging from the unauthorized use of their identities and demands for payment on transactions they had never made, to intimidation through contact with family members and psychological pressure stemming from damaged social reputation.¹⁰ Tellingly, most victims did not regard their principal loss as economic; rather, it was the loss of a sense of security and the violation of their personal honor. These findings reinforce those of Kurdi,¹¹ Wairimu, et al.,¹² which show that, in practice, data breaches produce harms that are relational and existential in nature, harms to human dignity (dignity harm) that remain inadequately accommodated within the design of national legal protection.

Scholarship on data protection in Indonesia has expanded considerably in recent years, yet most of it still operates within a linear, legal-formal, and positivist framework. The studies by Kriswandaru et al.,¹³ Irmawati et al.,¹⁴ Sabina and Faisal,¹⁵ and Kurdi¹⁶ generally focus on evaluating the implementation of the Personal Data

¹⁰ ST and DN, *Observations and interviews*, Lampung, May 2, 2026.

¹¹ Kurdi Kurdi and Joko Cahyono, "Perlindungan Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Juncto: Jurnal Ilmiah Hukum* 6, no. 2 (December 2024): 330–39, <https://doi.org/10.31289/juncto.v6i2.5443>.

¹² Samuel Wairimu and Lothar Fritsch, "Modelling Privacy Harms of Compromised Personal Medical Data - beyond Data Breach," *Proceedings of the 17th International Conference on Availability, Reliability and Security* (New York, NY, USA), August 23, 2022, 1–9, <https://doi.org/10.1145/3538969.3544462>.

¹³ Althea Serafim Kriswandaru, Berliant Pratiwi, and Suwardi Suwardi, "Efektivitas Kebijakan Perlindungan Data Pribadi Di Indonesia: Analisis Hukum Perdata Dengan Pendekatan Studi Kasus," *Hakim: Jurnal Ilmu Hukum Dan Sosial* 2, no. 4 (2024): 740–56, <https://doi.org/10.51903/hakim.v2i4.2157>.

¹⁴ Ema Irmawati, John Pieries, and Wiwik Sri Widiarty, "Perlindungan Hukum Atas Data Pribadi Nasabah Bank Pengguna Mobile Banking Dalam Perspektif Uu No 27 Tahun 2022 Tentang Kebocoran Data," *Jurnal Syntax Admiration* 5, no. 1 (January 12, 2024): 12–27, <https://doi.org/10.46799/jsa.v5i1.964>.

¹⁵ Sabina Tiffani and Faisal, "Analisis Hukum Terhadap Perlindungan Data Pribadi (Studi Kasus @farida.Nurhan Dan @codebluuuu)," *Jurnal Ilmu Hukum, Humaniora Dan Politik* 4, no. 3 (April 5, 2024): 291–300, <https://doi.org/10.38035/jihhp.v4i3.1915>.

¹⁶ Kurdi and Cahyono, "Perlindungan Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022."

Protection Law (UU PDP), the protection of banking customers, and criminal liability for data misuse on social media. Meanwhile, Rista and Prakoso,¹⁷ Loso et al.,¹⁸ and Anggraini et al.,¹⁹ develop their analyses through the lenses of digital consumer protection, e-commerce, and international human rights instruments. All of these studies make important contributions to mapping the weaknesses of national regulation and the challenges of its implementation. Even so, most stop at a normative-institutional reading and have yet to engage the more fundamental questions of why failures to mitigate data breaches keep recurring, and how victims' experiences ought to reshape the very way the law conceives of data protection.

These limitations point to the need to broaden the theoretical horizon—to read data protection not merely as a matter of regulatory compliance, but also as a question of power relations, digital governance, and the protection of human dignity. In contemporary global discourse, McGregor,²⁰ Tauchnitz,²¹ Srinath,²² and Muh Habibullo²³ position platform accountability, digital governance, and algorithmic justice not as mere instruments of cybersecurity but as mechanisms for safeguarding fundamental human rights. In a similar vein, Oskar J. Gstrein²⁴ and Lusine Vardanyan²⁵

¹⁷ Rista Maharani and Andria Luhur Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital," *Jurnal usm law review* 7, no. 1 (March 29, 2024): 333–47, <https://doi.org/10.26623/julr.v7i1.8705>.

¹⁸ Loso Judijanto, Nuryati Solapari, and Irman Putra, "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia," *The Easta Journal Law and Human Rights* 3, no. 01 (October 31, 2024): 20–29, <https://doi.org/10.58812/eslhr.v3i01.351>.

¹⁹ Sherlyna Resti Anggraini, Aisyah Amini, and Lucky Dafira Nugroho, "Keabsahan Kontrak Elektronik (E-Contract) Dalam Transaksi E-Commerce Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Ahkam* 4, no. 2 (June 21, 2025): 609–23, <https://doi.org/10.58578/ahkam.v4i2.6318>.

²⁰ Lorna McGregor, Daragh Murray, and Vivian Ng, "International Human Rights Law As A Framework For Algorithmic Accountability," *International and Comparative Law Quarterly* 68, no. 2 (April 17, 2019): 309–43, <https://doi.org/10.1017/S0020589319000046>.

²¹ Evelyn Tauchnitz and Shamira Ahmed, "Framing Ethical E-Governance: A Plaidoyer for a Human-Rights Based Digital Democracy Approach," in *Proceedings of the 17th International Conference on Theory and Practice of Electronic Governance* (New York, NY, USA: ACM, 2024), 22–27, <https://doi.org/10.1145/3680127.3680182>.

²² Srinath Muralinathan, "Balancing Data Protection and Human Rights in the Digital Age: A Review," *International Journal of Science and Research Archive* 16, no. 1 (July 30, 2025): 505–15, <https://doi.org/10.30574/ijrsra.2025.16.1.2031>.

²³ Muh Habibullo, "Digital Governance And The Right To Privacy: A Comparative Analysis Of AI Regulation In Southeast Asia And The European Union," *Journal of Law, Policy and Global Development* 1, no. 1 (June 28, 2025): 19–35, <https://doi.org/10.71305/jlpgd.v1i1.333>.

²⁴ Oskar J. Gstrein and Anne Beaulieu, "How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches," *Philosophy & Technology* 35, no. 1 (March 29, 2022): 3, <https://doi.org/10.1007/s13347-022-00497-4>.

²⁵ Lusine Vardanyan, Václav Stehlik, and Hovsep Kocharyan, "Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity," *TalTech Journal of European Studies* 12, no. 1 (May 2022): 159–85, <https://doi.org/10.2478/bjes-2022-0008>.

maintain that modern data-protection theory is moving toward an understanding of privacy as a manifestation of human dignity (privacy as dignity) and, at the same time, as a right to informational self-determination. Yet these theoretical developments have rarely been connected to the constructs of Islamic law, particularly the perspective of *maqāṣid al-sharīa*,²⁶ and have not been tested against the empirical experiences of data-breach victims in Indonesia. It is precisely here that the present study takes its position: not only explaining the failure of data protection in normative terms, but reconstructing data protection as the protection of digital dignity through a rereading of the concept of *ḥifẓ al-ʿird*, brought into dialogue with victims' social experiences and contemporary data-protection theory.

Building on these limitations, this study advances a rereading through the perspective of *maqāṣid al-sharīa*, and specifically the concept of *ḥifẓ al-ʿird*. In contrast to classical understandings, which tend to cast *ḥifẓ al-ʿird* as the protection of honor within conventional physical and social relations, this article argues that digital identity constitutes a new manifestation of human honor in the digital age. Personal data violations must therefore be understood as violations of digital dignity. Herein lies the novelty of this research: in the effort to reconstruct the concept of *ḥifẓ al-ʿird* as a normative foundation for personal data protection and for victims' access to legal aid, achieved by integrating victims' empirical experiences, modern data-protection theory, and *maqāṣid* hermeneutics.

On this basis, the study seeks to address two central questions: first, how data breaches operate as a form of violation against the digital dignity of the public; and second, how a reinterpretation of *ḥifẓ al-ʿird* can serve as a normative basis for strengthening personal data protection and legal aid for data-breach victims in Indonesia. To answer these questions, the study employs an empirical legal research method that combines socio-legal and conceptual approaches. Primary data were obtained through in-depth interviews with nine victims of data breaches, randomly selected in Lampung Province. In contrast, secondary data were drawn from legislation, the data-protection literature, and studies of *maqāṣid al-sharīa*. All data were analyzed qualitatively through *maqāṣid* hermeneutics to bring victims' social experiences into dialogue with a reconstruction of digital-dignity protection in Indonesian law.

²⁶ Jasser Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach* (International Institute of Islamic Thought (IIIT), 2008).

Beyond Economic Loss: Data Breaches, Digital Identity Control, and Human Dignity

In the victims' own experience, a data breach is understood not merely as the loss of administrative information but as the loss of control over their identity, sense of security, and social standing. In-depth interviews with nine data-breach victims who received assistance through a legal aid office in Lampung Province revealed two principal patterns of harm. Four informants were victims of social-engineering scams, while the other five had suffered phishing and malware attacks. In the first group, perpetrators exploited personal data, including full names, National Identification Numbers (NIK), and even Taxpayer Identification Numbers (NPWP), to establish legitimacy and win the victims' trust.²⁷ The most common ploy took the form of telephone calls made in the name of banks, law enforcement officers, courier staff, or particular administrative services, which then directed victims to transfer funds or hand over their OTP codes. In the second group, attacks were carried out through text messages, emails, and digital links resembling official services, leading victims to surrender access to their accounts and personal data unwittingly.²⁸

Of the nine informants interviewed, five reported suffering direct economic losses once their data had been misused. These losses took the form of transactions they had never made, deductions from their account balances, the use of their identity to apply for online loans, and additional costs incurred to recover accounts and re-secure the digital services they used. As NP and ZL explained, "We received a message that looked exactly like an official notification. After I opened it and logged in with my account, a few hours later, transactions and activity appeared that I had never carried out."²⁹ Both LR and MR stated that, once others had used their data, they were left to bear the administrative and financial consequences, even though they were not the ones who had made the transactions. These experiences show that the economic harm caused by data breaches does not stop at financial loss; it also imposes a burden of proof on victims to restore their legal position.³⁰ This is

²⁷ DN, MW, ST, and DW, *Interview*, Lampung, May 17, 2026

²⁸ YQ, LR, ZL, MR, and NP, *Interview*, Lampung, May 20, 2026

²⁹ NP and ZL, *Interview*, Lampung, May 20, 2026

³⁰ LR and MR, *Interview*, Lampung, May 20, 2026

consistent with the findings of Irmawati, Pieries, and Widiarty,³¹ who show that breaches in the financial and financial-technology sectors often culminate in illegal transactions, account hacking, and fictitious online loans that prove difficult to reverse, given the complexity of tracing perpetrators and the weak coordination among institutions. To facilitate a reading of the patterns in the victims' experiences and the forms of harm that emerged, the results of the field-finding categorization are presented in Table 1.

Table 1. A Typology of Data-Breach Victims' Experiences

Victim Experience	Informants	Perpetrator's Method	Form of Harm	Impact on Identity Control
Legitimacy-based exploitation (Social Engineering/Scam)	4 People	Perpetrators used identity data (name, NIK, NPWP, phone number, OTP) to build trust by posing as banks, officials, courier services, or administrative services.	Fund transfers, identity misuse, and the administrative burden of recovery	Loss of a sense of security and diminished control over the use of personal identity
Access-manipulation-based exploitation (Phishing and Malware)	5 People	Perpetrators gained access via messages, emails, or links that resembled official services, leading victims to surrender their credentials and account access.	Unauthorized transactions, account takeover, identity misuse, and recovery costs	Uncertainty over data use and loss of control over identity and digital activity

Source: Compiled from the researcher's interview findings, 2026

³¹ Haekal Al Asyari, "Between Freedom And Protection: A Critical Review Of Indonesia'S Cyberspace Law," *Prophetic Law Review*, July 4, 2023, 79–103, <https://doi.org/10.20885/PLR.vol5.iss1.art5>.

These field findings also reveal a pattern consistent with experiences in various highly digitalized countries. In South Korea, one of the largest data breaches on record revealed that some 20 million credit card customer records—including records of public figures—were illegally accessed and disseminated, affecting nearly 70 percent of the country's population.³² That case generated not only economic loss but also a crisis of public trust in the digital identity system and in national data governance. In India, the Aadhaar biometric identity system,³³ which integrates identification numbers, fingerprints, and retinal scans of more than one billion citizens, came under scrutiny after an investigation found that access to the database could be illegally bought and sold through WhatsApp groups for a remarkably low fee.³⁴ In the United Kingdom, meanwhile, a report by the Information Commissioner's Office found the health sector to be among those most vulnerable to data breaches, owing to a combination of human error and cyberattacks.³⁵ One major incident involving the National Health Service (NHS) led to the leak of patients' medical histories and mental health information, raising serious concerns about social stigma and the violation of individual dignity.³⁶ All three cases display the same pattern observed in the experiences of this study's informants: the more deeply digital identity is integrated into social life, the greater the risk that individuals will lose control over their own representation.

Even so, the most significant impact in this study was observed in the social and psychological dimensions. Five informants reported changes in their behavior following the breach—ranging from limiting their use of digital

³² Ampuan Situmeang et al., "Evaluating Data Breach Notification Protocols," *Lentera Hukum* 12, no. 1 (April 2025): 42–61, <https://doi.org/10.19184/ejlh.v12i1.47621>.

³³ "Aadhaar: 'Leak' in World's Biggest Database Worries Indians," BBC News, 2018, <https://www.bbc.com/news/world-asia-india-42575443>.

³⁴ Devyani Nighoskar, "Are Our Aadhaar Identities Available On WhatsApp For Just Rs. 500?," Homegrown, 2021, <https://homegrown.co.in/homegrown-explore/are-our-aadhar-identities-available-on-whatsapp-for-just-rs-500>.

³⁵ Mark Evans et al., "Evaluating Information Security Core Human Error Causes (IS-CHEC) Technique in Public Sector and Comparison with the Private Sector," *International Journal of Medical Informatics* 127 (July 2019): 109–19, <https://doi.org/10.1016/j.ijmedinf.2019.04.019>.

³⁶ Saira Ghafur et al., "The Challenges of Cybersecurity in Health Care: The UK National Health Service as a Case Study," *The Lancet Digital Health* 1, no. 1 (May 2019): e10–12, [https://doi.org/10.1016/S2589-7500\(19\)30005-6](https://doi.org/10.1016/S2589-7500(19)30005-6); Muhammad deniardi et al., "criminal law arrangements in indonesia related to judicial review," *Russian Law Journal* 11, no. 3 (April 2023), <https://doi.org/10.52783/rlj.v11i3.1835>.

services and deleting certain accounts to avoiding online transactions altogether for fear of falling victim again. Four other informants admitted to experiencing social pressure when their family members, colleagues, or personal contacts were themselves contacted by the perpetrators, leaving them feeling ashamed and diminishing the trust of those around them. One informant (DN) put it this way: “What made me uncomfortable wasn't the money. I felt as though I had lost control, because my data was being used to convince other people that it was really me.” Similar accounts emerged from MW and ST, who described mounting anxiety, a difficulty in trusting digital communication, and a fear that their identities could be used again without their knowledge.³⁷ These experiences show that victims lose not only information security but also their sense of safety, self-esteem, and the social relationships that have long been part of their daily lives. The finding also aligns with the APJII National Survey, which reports that 7–8 percent of internet users in Indonesia admit to experiencing personal data theft hacking, and phishing, underscoring that digital vulnerability has become an increasingly widespread social experience.

This pattern accords with several earlier studies. Sabina and Faisal³⁸ show that breaches of personal data, particularly on social media, frequently escalate into privacy violations accompanied by public humiliation, doxing, and psychological pressure that directly affects victims' reputations and mental health. Many victims experience shame, a loss of their sense of security, and even withdrawal from digital spaces. Broader social consequences were likewise documented by Rista Maharani and Andria Luhur Prakoso,³⁹ who found that most e-commerce users who experienced a data breach reported diminished trust in digital systems, with roughly 64% choosing to stop using certain online services altogether. This suggests that data breaches generate

³⁷ DN, MW, and ST, *Interview*, Lampung, May 17, 2026

³⁸ Sabina Tiffani and Faisal, “Analisis Hukum Terhadap Perlindungan Data Pribadi (Studi Kasus @farida.Nurhan Dan @codebluuuu),” *Jurnal Ilmu Hukum, Humaniora dan Politik* 4, no. 3 (April 2024): 291–300, <https://doi.org/10.38035/jihhp.v4i3.1915>; Imroatul Azizah et al., “Digitalization and Cyberfeminism: Reinterpreting Islamic Criminal Law for Gender Equality and Women's Rights,” *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, May 17, 2026, 127–43, <https://doi.org/10.24090/volksgeist.v9i1.15378>.

³⁹ Rista Maharani and Andria Luhur Prakoso, “Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital,” *Jurnal USM Law Review* 7, no. 1 (March 2024): 333–47, <https://doi.org/10.26623/julr.v7i1.8705>.

not only individual harm but also a trust deficit in the digital public sphere. Once the public loses confidence in the security of digital services, the very digital transformation meant to widen access may instead create new forms of exclusion for those who choose to withdraw out of trauma and fear.

From a socio-legal perspective, the informants' experiences and cross-country comparisons reveal that the relationship between the individual and their data has undergone a fundamental shift. Personal data no longer functions merely as a means of administrative identification; it has become a representation of a person's honor and social existence. Cybercriminals do not simply harvest information for economic gain—they use the victim's identity to construct legitimacy, dictate actions, and shape how others perceive that victim. The South Korean case shows how a data breach can shake public trust in a national system. The Aadhaar case in India demonstrates that even biometric data, regarded as the most secure, can be illegally commodified. The NHS case in the United Kingdom, meanwhile, illustrates that when data concerns health conditions and personal life, the impact shifts from administrative loss to a violation of human dignity.⁴⁰ Under such conditions, what is truly stripped away is not only privacy but also the individual's capacity to preserve their good name, sense of security, and social recognition.

The theories of privacy as dignity and informational self-determination⁴¹ help explain that personal data is, in essence, part of the individual's capacity to maintain autonomy and to determine how they present themselves within the social sphere.⁴² The findings indicate that a data breach operates not directly through the loss of information, but through the surrender of the individual's control over their digital identity. Once personal data circulates and is used by others, victims lose the ability to determine who may access, use, and represent them.⁴³ At that point, perpetrators acquire not

⁴⁰ Siti Rahmadani and Rina Arum Prastyanti, "Human Rights and Cybersecurity: Reinforcing Legal Protections for Personal Data," *International Journal of Law Dynamics Review* 3, no. 1 (May 2025): 20–29, <https://doi.org/10.62039/ijldr.v3i1.80>.

⁴¹ J. C. Buitelaar, "Post-Mortem Privacy and Informational Self-Determination," *Ethics and Information Technology* 19, no. 2 (June 2017): 129–42, <https://doi.org/10.1007/s10676-017-9421-9>.

⁴² Ahmad Fadii and Khaled Aljasmi Najlaa Flayyih, Mohammed Hasson Ali, "The Right to Informational Self-Determination between Legislation and Implementation," *Access to Justice in Eastern Europe* 8, no. 3 (2025): 362–89, <https://doi.org/10.33327/AJEE-18-8.3-a000116>.

⁴³ Yuval Goldfus, "Tell Me Who Your Friends Are and I'll Tell You Who You Are: Privacy and the Social Self," *SSRN Electronic Journal*, ahead of print, 2023, <https://doi.org/10.2139/ssrn.4539608>.

merely the data but the very function of the victim's identity, deploying it to construct social legitimacy and influence others' actions. As a result, victims cease to be the authority over themselves, since their identity can be reproduced and exploited against their will.⁴⁴ A data breach thus serves as a mechanism to divest individuals of control over their digital identity, ultimately resulting in a violation of human dignity. Data protection, accordingly, cannot be understood merely as safeguarding the confidentiality of information; it must be understood as protecting the individual's capacity to preserve their autonomy, honor, and social recognition in the digital sphere.

From Administrative Compliance toward Victim-Centered Digital Justice

The preceding discussion showed that a data breach is understood not merely as an event in which one loses control over one's digital identity, but also as an experience that reshapes the individual's relationship with the digital realm.⁴⁵ The informants' accounts, however, reveal that a far more complex problem emerges only after the violation has occurred. The greatest difficulty they faced lay not in discovering that others had used their data, but in identifying who was accountable and obtaining a clear recovery mechanism.⁴⁶ Of the nine victims interviewed with assistance from a legal aid office in Lampung Province, six first attempted to resolve the matter through digital service providers. At the same time, the remaining three chose to report it to law enforcement. Although the avenues they pursued differed, the resulting experiences followed a similar pattern: procedural ambiguity, limited access to information, and uncertainty about which recovery steps were even available.

The responses victims received reveal a tendency to channel resolution toward securing accounts and forestalling further risk rather than toward recovery from the harm already suffered. Indeed, the burden of proof continued to rest on the data owner, who has no access to the data controller's

⁴⁴ Lesya Chesnokova, "Information Privacy: Protecting Freedom and Individual Autonomy," *The Digital Scholar Philosopher s Lab* 4, no. 2 (2021): 145–57, <https://doi.org/10.32326/2618-9267-2021-4-2-145-157>.

⁴⁵ Dennis Gibson and Clive Harfield, "Amplifying Victim Vulnerability: Unanticipated Harm and Consequence in Data Breach Notification Policy," *International Review of Victimology* 29, no. 3 (September 2023): 341–65, <https://doi.org/10.1177/02697580221107683>.

⁴⁶ Nur Chanifah et al., "The Digitalisation of Employment, Fiqh Education and Empowerment of Migrant Workers' Rights," *Justicia Islamica* 23, no. 1 (March 2026): 253–84, <https://doi.org/10.21154/justicia.v23i1.12454>.

digital infrastructure,⁴⁷ taking the form of measures such as changing passwords, updating authentication, severing device access, or heightening vigilance against suspicious digital activity. Such steps are certainly important for limiting risk. Yet they leave unanswered the questions that resurfaced repeatedly throughout the interviews: whether the exposed identity is still in use, who bears responsibility for the misuse, and how to restore a sense of security. As one informant put it, "Even after my account was secured, I still had no idea what my data had been used for, or where I was supposed to turn to demand accountability."⁴⁸ This statement does not stand as an isolated experience; rather, it captures a pattern that recurs across various cases. The victims' experiences show that the problem of data protection lies not only in the weak handling of incidents but also in the very way protection is designed and implemented. Success as it has hitherto been measured—by the restoration of systems and the containment of technical disruptions—is not enough for victims, who continue to face uncertainty over how their identities are being used, the risk of further misuse, and an eroding sense of security in their digital lives. These findings reinforce the work of Syifa Nurul and Wira Atma, Tania Tresna et al., and Mahfud et al., which point to a gap between the formal success of data protection and the recovery victims actually experience. Effective data protection, then, must be assessed not by the recovery of systems alone, but by its capacity to restore a sense of security, certainty, and justice to victims.

Experience across multiple countries shows that the victim-centered approach is increasingly recognized as an essential part of data-protection governance and the response to cybercrime. This awareness springs from the recognition that victims of data breaches suffer not only economic loss or technical disruption, but also psychological shock, panic, a sense of lost control, and even a condition resembling learned helplessness—the state in which individuals feel they no longer have any power to govern what is happening to them. Recovery, accordingly, is not confined to restoring

⁴⁷ Ninuk Triyanti, I. Gusti Ayu Ketut Rachmi Handayani, and Lego Karjoko, "Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration Law," *Hasanuddin Law Review* 11, no. 1 (January 2025): 132, <https://doi.org/10.20956/halrev.v11i1.6177>.

⁴⁸ ST and DW, *Interview*, Lampung, May 18, 2026

systems; it extends to forms of support that help victims regain both a sense of security and the capacity to act.

In the European Union, this development is visible in the integration of the data-protection regime with a victim-protection approach under the Revised EU Victims' Rights Directive.⁴⁹ This approach treats victims as rights-bearing subjects entitled to information, support, and assistance throughout the recovery process, including where the violation occurs in the digital realm.⁵⁰ Protection does not end with the data controller's duty to report incidents or to repair systems; it extends to providing services that help victims understand the risks they face, access complaint mechanisms, and obtain support tailored to their needs.⁵¹

A more operational model can be found in the United Kingdom through its Cyber Helpline. The service offers a one-stop support mechanism for victims of cybercrime, sparing them from having to navigate the various institutions involved on their own.⁵² Support workers help victims carry out technical steps, provide preliminary legal guidance, and connect them with the relevant parties to contain the knock-on effects of data misuse.⁵³ A similar approach has taken shape in South Korea through a state-backed specialized agency that delivers integrated assistance to victims of cybercrime.⁵⁴ This

⁴⁹ "The European Union's Obligations to Safeguard the Fundamental Right to Data Protection Extraterritorially," in *Transatlantic Jurisdictional Conflicts in Data Protection Law* (Cambridge University Press, 2023), 33–56, <https://doi.org/10.1017/9781108784818.003>.

⁵⁰ Mercedes Llorente Sánchez Arjona, "Las Víctimas En El Espacio Judicial Europeo: Estudio de La Directiva 2012/29/UE, de 25 de Octubre de 2012," *Revista de Estudios de La Justicia*, no. 22 (November 2015), <https://doi.org/10.5354/0718-4735.2015.37589>; Maja Nišević and Aleksandra Ivanković, "Secondary Victimization through Data Protection: Balancing Victim Privacy and Support in the EU Legal Framework," *International Review of Victimology* 32, no. 1 (January 2026): 65–82, <https://doi.org/10.1177/02697580251374719>.

⁵¹ Cécile de Terwangne, "Privacy and Data Protection in Europe: Council of Europe's Convention 108 and the European Union's GDPR," in *Research Handbook on Privacy and Data Protection Law* (Edward Elgar Publishing, 2022), 10–35, <https://doi.org/10.4337/9781786438515.00007>.

⁵² Jamie Saunders, "Tackling Cybercrime – the UK Response," *Journal of Cyber Policy* 2, no. 1 (January 2017): 4–15, <https://doi.org/10.1080/23738871.2017.1293117>.

⁵³ Prabha A, Beulah Shekhar, and Ameenul Abdullah K S, "Mapping Cybercrime Victimization: A Review of Psychological, Social and Economic Impacts," *International Journal For Multidisciplinary Research* 7, no. 6 (December 2025), <https://doi.org/10.36948/ijfmr.2025.v07i06.65150>; Shital Harishchandra Ujade, "Role of Social Work in Cybercrime Victim Support," *Gurukul International Multidisciplinary Research Journal*, ahead of print, April 14, 2025, <https://doi.org/10.69758/GIMRJ/250313IIVXIIIP0042>.

⁵⁴ Na-Mi Kang and Sang-Jin Park, "Strategies to Enhance the Effectiveness of One-Stop Solution Centers for Crime Victims," *The Korean Association for Terrorism Studies* 18, no. 2 (June 2025): 74–93, <https://doi.org/10.46350/KATS.2025.18.2.74>.

support spans not only the technical dimension but also psychological services and legal aid, so that victims need not face the recovery process alone.

In practice, the support model operates on the principle that victims are not left to handle every consequence of a violation alone. Support workers can help contact banks to reverse transactions flagged as fraudulent, coordinate with network providers to lock down misused numbers, assist with the reporting process, and, at the same time, provide psychological counseling at no extra cost. This approach marks a fairly fundamental shift in orientation: the success of protection is no longer measured by how quickly systems are restored, but by how far victims can regain control over their own lives.⁵⁵

This situation becomes especially relevant when read alongside the evolution of data-protection regulation in Indonesia. The enactment of Law No. 27 of 2022 was indeed an important step toward reducing the regulatory fragmentation that had previously been scattered across multiple sectors. Yet consolidating these norms has not, in itself, removed the obstacles the public encounters when confronting data violations. The informants' experiences show that the formal recognition of rights is not always matched by the ability to exercise those rights effectively.⁵⁶ Not all victims understand the complaint procedures, have the capacity to trace how their data is used, or can secure adequate legal support. In practice, the responsibility for self-protection is shifted back onto individuals—even though they occupy a far weaker position than the data processors and controllers.

A comparison with several other countries shows that the challenge of data protection in Indonesia lies not merely in strengthening regulation, but also in building a recovery infrastructure that victims can actually access. So long as the available mechanisms continue to cast the individual as the party who must seek out information, contact the various institutions, and shoulder the burden of recovery alone, protection will remain stalled at the administrative level. Protection acquires real meaning only when it can restore a sense of security, repair the victim's social standing, and provide recovery

⁵⁵ An Nisya Nursabilah et al., "Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Scam Serta Dampaknya Bagi Korban Sebagai Bentuk Viktimisasi Sekunder," *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora* 2, no. 3 (June 2025): 168–87, <https://doi.org/10.62383/humif.v2i3.1912>.

⁵⁶ Rengga Kusuma Putra et al., "Institutional Dysfunction in Personal Data Protection: A Legal-Political Analysis Based on New Institutional Theory," *Perkara : Jurnal Ilmu Hukum Dan Politik* 3, no. 2 (June 2025): 938–49, <https://doi.org/10.51903/bkktey52>.

pathways that are equally accessible to all. The shift from administrative compliance to digital justice, then, calls for support services that not only protect data but also restore the human beings harmed by the violation.

Reinterpreting *Hifz al- 'Ird* as a Foundation for Data Protection and Legal Aid for Victims

The two preceding findings reveal an interconnected pattern. At the individual level, a data breach results in the loss of control over one's digital identity and inflicts harm that extends well beyond the economic. At the institutional level, victims encounter limited access to recovery because the protection mechanisms on offer remain oriented toward securing systems and procedural compliance. Taken together, this shows that the problem of data protection in Indonesia cannot be explained through the language of cybersecurity or regulatory effectiveness alone; it touches on a more fundamental question of how the law regards the human person and their dignity in the digital realm.

This finding is further reinforced by the experience of several countries, which shows that modern data protection is increasingly moving away from an information-security paradigm and toward one of rights protection and victim recovery. Through the General Data Protection Regulation (GDPR), the European Union frames data protection as part of citizens' fundamental rights. It broadens the concept of harm to include non-material damage such as psychological distress, loss of control over one's identity, and damage to one's digital reputation.⁵⁷ The judgment of the Court of Justice of the European Union (CJEU) in *Österreichische Post AG v UI* affirmed that non-material damage resulting from a breach of data protection can constitute a basis for legal compensation.⁵⁸ In South Korea, the reform of the Personal Information Protection Act (PIPA) has strengthened compensation mechanisms and expanded post-breach recovery obligations.⁵⁹ India's experience with the

⁵⁷ Jonas Knetsch, "The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases," *Journal of European Tort Law* 13, no. 2 (August 2022): 132–53, <https://doi.org/10.1515/jetl-2022-0008>; Mireille Hildebrandt, "The Fundamental Right of Data Protection," in *Smart Technologies and the End(s) of Law* (Edward Elgar Publishing, 2015), 186–213, <https://doi.org/10.4337/9781849808774.00017>.

⁵⁸ Knetsch, "The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases."

⁵⁹ Ju Seon Yoo, "Personal Information Protection Act Revised in 2023 and My Data Utilization Plan - Focusing on the Insurance Industry -," *Korea Financial Law Association* 20, no. 2 (August 2023): 55–76, <https://doi.org/10.15692/KJFL.20.2.2>.

Digital Personal Data Protection Act 2023, meanwhile, marks an important shift from a digital-economy-development approach toward strengthening data subjects' rights to safeguard constitutional dignity.⁶⁰ Although the institutional contexts of these countries differ from Indonesia's, a consistent pattern holds: data protection is increasingly understood as protecting human beings, not merely systems.

These empirical findings also align with prior research. Solove shows that the harm caused by privacy violations cannot always be measured in economic terms, since it often takes the form of lost control, a sense of insecurity, and long-term shifts in social relationships Cohen.⁶¹ Cohen, Austin, and Becker affirmed that privacy is a prerequisite for the formation of identity and maintain that it is a precondition for individual freedom in a digital society. In the context of data governance, Waldman⁶² demonstrates how the extraction and exploitation of data create asymmetric relations of power among individuals, corporations, and the state, thereby eroding human autonomy.⁶³ In contemporary Islamic law, Auda emphasizes that *maqāṣid* must be read in an open, contextual way if they are to respond to changes in social and technological structures.⁶⁴ Taken together, these findings reinforce the argument that the harm caused by data breaches cannot be reduced to a technical matter; it must be understood as a question of protecting human dignity.

From this point, a reading through *maqāṣid al-sharīa* becomes relevant—not to supplant positive law, but to interrogate the basic assumptions that

⁶⁰ Chea Yun Jung and Hyun Kyong Joo, "Post-'Lee-Luda' Personal Information Protection in Korea: Developer Responsibility and Autonomous AI Governance," *International Data Privacy Law* 13, no. 2 (June 2023): 154–67, <https://doi.org/10.1093/idpl/ipad006>.

⁶¹ Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (January 2006): 477, <https://doi.org/10.2307/40041279>.

⁶² Ari Ezra Waldman, "Privacy's Rights Trap," *SSRN Electronic Journal*, ahead of print, 2022, <https://doi.org/10.2139/ssrn.4182858>.

⁶³ Obioma Adesewa Okonkwo, "Structural Asymmetries in Data Ownership, Access to Information, and Human Rights Enforcement across Global Digital Governance Regimes.," *World Journal of Advanced Research and Reviews* 4, no. 2 (December 2019): 238–55, <https://doi.org/10.30574/wjarr.2019.4.2.0151>.

⁶⁴ Arminsyah Arminsyah, "Maqasid Al-Shariah in Contemporary Legal Systems: An Analysis of Digital Rights and Privacy Protection," *Al-Qadha: Jurnal Hukum Islam Dan Perundang-Undangan* 12, no. 2 (July 2025): 289–308, <https://doi.org/10.32505/qadha.v12i2.11178>; Uthman Mehdad Al-Turabi and Jasser Auda, "Toward a Maqāṣid-Based Legal Reform: Systemic Thinking for Social Transformation in the Modern Muslim World," *Indonesian Journal of Islamic Law* 8, no. 2 (December 2025): 209–28, <https://doi.org/10.35719/fhw10v84>.

underpin it. The reconstruction of *maqāṣid* proposed by Jasser Auda⁶⁵ opens up room to shift the orientation of law from the protection of objects toward the protection of the human being as the central locus of *maṣlaḥah* (welfare). Within this framework, *ḥifẓ al-ʿird* is no longer understood narrowly as the safeguarding of social honor within physical relationships, but is extended to the protection of identity and personal integrity across every sphere of life, including the digital realm⁶⁶ This expansion matters because victims' experiences show that personal data no longer functions as merely administrative information; it has become an instrument that determines how a person is recognized, trusted, and able to participate in social life.⁶⁷

This approach gains further legitimacy from developments in contemporary Islamic legal thought, which has begun to read privacy and data as part of the protection of human honor. Several studies on Islamic digital ethics show that the concept of *ḥifẓ al-ʿird* has the conceptual capacity to be extended into the digital realm, since the core of its protection lies in safeguarding human integrity against acts that demean or exploit.⁶⁸ Digital identity can thus be understood as a new form of the sphere of honor that warrants protection.

A consequence of this shift in perspective is that data protection moves from a supplementary need to a fundamental one. In a digital society, the misuse of data can simultaneously compromise personal security, impair the

⁶⁵ Zaprulkhan Zaprulkhan, "Maqāṣid Al-Shariah in the Contemporary Islamic Legal Discourse: Perspective of Jasser Auda," *Walisono: Jurnal Penelitian Sosial Keagamaan* 26, no. 2 (December 2018): 445, <https://doi.org/10.21580/ws.26.2.3231>; Jasser Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach* (International Institute of Islamic Thought (IIIT), 2008).

⁶⁶ Desy Damayanti, Rahma Hasna Naziha, and Cucu Surahman, "Perspektif Hukum Islam Terhadap Perlindungan Data Pribadi Di Era Digital," *Al-Battar: Jurnal Pamungkas Hukum* 1, no. 3 (December 2024): 151–63, <https://doi.org/10.63142/xzd65n65>; Husnul Fatarib et al., "Progressive Legal Reasoning in Contemporary Islamic Legal Reform: Negotiating the Maqāṣid and Hermeneutic Approaches," *JURIS (Jurnal Ilmiah Syariah)* 24, no. 2 (December 2025): 277–94, <https://doi.org/10.31958/juris.v24i2.16123>.

⁶⁷ Titis Thoriquattyas and Nita Rohmawati, "Maqasid Al-Sharia and the Digital Data Ownership: From al-Shatibi to Jasser Auda," *Journal of Islamic Law on Digital Economy and Business*, February 27, 2026, 168–81, <https://doi.org/10.20885/JILDEB.vol1.iss2.art5>.

⁶⁸ 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 (November 2025): 107–28, <https://doi.org/10.62509/ajis.v2i2.260>; Nina Nurani, Apriwandi Apriwandi, and Hafied Noor Bagja, "Intellectual Property Rights Law Reform Based on Maqāṣid Al-Sharī'ah as a Model for Green Business-Based Creative Industry Protection to Support Sustainable Development," *De Jure: Jurnal Hukum Dan Syar'iah* 18, no. 1 (February 2026): 1–32, <https://doi.org/10.18860/j-fsh.v18i1.40840>.

ability to make free decisions, inflict economic loss, and damage a person's social recognition. Data protection is therefore more aptly placed within the category of primary necessities (*ḍarūriyyāt*),⁶⁹ because its failure produces disruptions that bear directly on the protection of life (*ḥifẓ al-nafs*), intellect (*ḥifẓ al-‘aql*), property (*ḥifẓ al-māl*), and, above all, human honor (*ḥifẓ al-‘ird*).⁷⁰ This argument also finds support in interdisciplinary research demonstrating that the impact of a data breach is multidimensional. These findings further show that data protection has moved from an administrative need to an existential one that shapes the very quality of citizens' lives. The state's inability to provide protection and recovery, then, can no longer be read as merely an administrative matter but as a failure to discharge its legal and moral responsibility to safeguard the welfare of its citizens.

Building on this reading, the present study proposes a model of *Maqāṣid*-Oriented Legal Aid (MOLA) as an operational reinterpretation of *ḥifẓ al-‘ird* in the digital context. The first is a restorative dimension, which makes victim recovery its primary goal through the erasure of leaked data, the rehabilitation of digital identity, the recognition of non-material harm, and social recovery mechanisms that go beyond economic compensation. This approach resembles developments in the European Union, which has begun to recognize the rights to erasure and non-economic recovery as part of efforts to protect digital dignity. From an Islamic legal perspective, this orientation is rooted in *jabr al-ḍarar* (the redress of harm), which emphasizes not only the compensation of material loss but also recovery from acts that damage one's honor. The second is a structural dimension that drives systemic improvement through strategic litigation, policy advocacy, and strengthening institutional accountability, so that similar violations do not recur.⁷¹ South Korea's experience shows that strengthening oversight mechanisms and administrative sanctions, paired with victims' access to recovery, can improve

⁶⁹ Cristine Mailiena and M. Ilham Tanzilulloh, "Normativity of Consumer Protection in the Perspective of *Maqāṣid Shari'ah*," *Invest Journal of Sharia & Economic Law* 4, no. 1 (August 2024): 176–88, <https://doi.org/10.21154/invest.v4i1.9004>.

⁷⁰ Mohammad Farid Fad, "Perlindungan Data Pribadi Dalam Perspektif *Sadd Dzari'ah*," *Muamalatuna* 13, no. 1 (June 2021): 33, <https://doi.org/10.37035/mua.v13i1.4674>.

⁷¹ Arliana Agustin Faridhatul Shima and Lukman Santoso, "Right of Access to Legal Aid for the Poor: Study of Islamic Civil Cases in the PA Ponorogo Legal Area," *Istinbath: Jurnal Hukum* 21, no. 1 (July 2024): 19–39, <https://doi.org/10.32332/3hw8f526>.

institutional compliance with data protection. Within the *maqāṣid* framework, this approach aligns with the principle of *sadd al-dharāʿi*, which closes off avenues that enable recurrent harm.⁷²

The third is a community-based accessibility dimension⁷³ that harnesses networks of legal aid, Islamic universities, *pesantren* (Islamic boarding schools), and philanthropic instruments such as waqf to extend the reach of protection to groups that have long found it difficult to access formal mechanisms. This approach draws inspiration from community-based legal empowerment practices in India and several Global South countries, which show that the success of digital-rights protection depends heavily on the capacity to build social infrastructure beyond the state. The model offers novelty on three levels at once. Conceptually, this study broadens the meaning of *ḥifẓ al-ʿird* by incorporating digital identity and data sovereignty as part of human honor. Methodologically, *maqāṣid* is not treated as an abstract normative legitimation, but is deployed as a tool for evaluating and designing recovery mechanisms. Practically, the proposed model brings Islamic law, legal aid, and digital governance together within a single framework oriented toward the recovery of the human person.

Data protection, then, is no longer understood as a technical matter of information management, but as a legal mandate to ensure that every citizen retains control over their identity and dignity in the digital age. Compared with the positive-law approach, which remains predominantly oriented toward administrative compliance, a *maqāṣid*-based approach allows data protection to be built on the principles of *maṣlaḥah* (welfare), recovery, and respect for human honor as the law's ultimate aim.

⁷² Desy Damayanti, Rahma Hasna Naziha, and Cucu Surahman, "Perspektif Hukum Islam Terhadap Perlindungan Data Pribadi Di Era Digital," *Al-Battar: Jurnal Pamungkas Hukum* 1, no. 3 (2024): 151–63, <https://doi.org/10.63142/xzd65n65>; Teguh Anshori, "Menuju Fiqih Progresif (Fiqih Modern Berdasarkan Maqashid Al Syariah Perspektif Jaser Auda)," *Al-Syakhsiyyah: Journal of Law and Family Studies* 2, no. 1 (June 2020): 168–81, <https://doi.org/10.21154/syakhsiyyah.v2i1.2166>.

⁷³ Arliana Agustin Faridhatul Shima and Lukman Santoso, "Right of Access to Legal Aid for the Poor: Study of Islamic Civil Cases in the PA Ponorogo Legal Area," *Istinbath: Jurnal Hukum* 21, no. 01 (July 2024): 19–39, <https://doi.org/10.32332/istinbath.v21i01.9654>; Fitri Nurulita et al., "Sacred Law in Secular Systems: Shariawiz and Digital Inheritance Fiqh among Muslim Minorities in the United States," *Asy-Syir'ah: Jurnal Ilmu Syari'ah dan Hukum* 59, no. 2 (2025): 252–73, <https://doi.org/10.14421/ajish.v59i2.1642>.

Conclusion

This study shows that personal data breaches in Indonesia cannot be understood merely as technical incidents or administrative violations, but as events that strip individuals of control over their digital identity and, ultimately, undermine human dignity. Empirical findings drawn from victims' experiences reveal that the resulting harm extends beyond economic loss to encompass a sense of insecurity, social uncertainty, and the loss of any ability to determine how one's own identity is used. At the same time, the available protection mechanisms remain oriented toward system recovery and procedural compliance, and have thus yet to deliver effective access to justice for victims.

Against this backdrop, the study affirms the need for a paradigm shift in data protection from an administrative approach toward a human-centered one. Through a reinterpretation of *ḥifẓ al-ʿird* within the framework of contemporary *maqāṣid al-sharīa*, data protection is positioned as part of the protection of honor and digital identity, both of which hold a fundamental place in modern life. On this basis, the study proposes the Maqasid-Oriented Legal Aid (MOLA) model as a framework integrating victim recovery, institutional reform, and the expansion of community-based access to legal aid. Future research is encouraged to test the application of this model in the institutional practice of legal aid and in data-protection governance at both the local and national levels, to assess its effectiveness in strengthening digital justice in Indonesia.

References

- A, Prabha, Beulah Shekhar, and Ameenul Abdullah K S. "Mapping Cybercrime Victimization: A Review of Psychological, Social and Economic Impacts." *International Journal For Multidisciplinary Research* 7, no. 6 (December 2025). <https://doi.org/10.36948/ijfmr.2025.v07i06.65150>.
- Al, muhammad deniardi et al. "criminal law arrangements in indonesia related to judicial review." *Russian Law Journal* 11, no. 3 (April 2023). <https://doi.org/10.52783/rlj.v11i3.1835>.
- Al-Farjani, Saleh Hashem, and Waheed Alazhari. "Bridging Law, Technology, and Justice in the Digital Age." *INDONESIAN JOURNAL OF*

- SUSTAINABILITY 5, no. 1 (February 2026): 37. <https://doi.org/10.30659/ijsunissula.5.1.37-49>.
- Al-Fatih, Sholahuddin, and Zaka Firma Aditya. "The legal protection against terrorism suspects in Indonesia (case study of the arrest process of terrorism suspects by Densus 88)." *Legality : Jurnal Ilmiah Hukum* 27, no. 1 (July 2019): 14–26.
- Al-Fatih, Sholahuddin, Zaka Firma Aditya, Abdul Basid Fuadi, and Muhammad Nur. "Academic Freedom of Expression in Indonesia: A Maqashid Sharia Notes." *El-Mashlahah* 13, no. 2 (December 2023): 203–24. <https://doi.org/10.23971/el-mashlahah.v13i2.7573>.
- Al-Turabi, Uthman Mehdad, and Jasser Auda. "Toward a Maqāṣid-Based Legal Reform: Systemic Thinking for Social Transformation in the Modern Muslim World." *Indonesian Journal of Islamic Law* 8, no. 2 (December 2025): 209–28. <https://doi.org/10.35719/fhw10v84>.
- An Nisya Nursabilah, Nazmi Viranha Khurulani, Anggia Prasanti, Dea Aulia Zuhra, Allyah Alicia Hg, and Nabila Nabanurohmah. "Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Scam Serta Dampaknya Bagi Korban Sebagai Bentuk Viktimisasi Sekunder." *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora* 2, no. 3 (June 2025): 168–87. <https://doi.org/10.62383/humif.v2i3.1912>.
- Anshori, Teguh. "Menuju Fiqih Progresif (Fiqih Modern Berdasarkan Maqashid Al Syariah Perspektif Jaser Auda)." *Al-Syakhsiyyah: Journal of Law and Family Studies* 2, no. 1 (June 2020): 168–81. <https://doi.org/10.21154/syakhsiyyah.v2i1.2166>.
- Arliana Agustin, Faridhatul Shima, and Lukman Santoso. "Right of Access to Legal Aid for the Poor: Study of Islamic Civil Cases in the PA Ponorogo Legal Area." *Istinbath: Jurnal Hukum* 21, no. 1 (July 2024): 19–39. <https://doi.org/10.32332/3hw8f526>.
- Arminsyah, Arminsyah. "Maqasid Al-Shariah in Contemporary Legal Systems: An Analysis of Digital Rights and Privacy Protection." *Al-Qadha : Jurnal Hukum Islam Dan Perundang-Undangan* 12, no. 2 (July 2025): 289–308. <https://doi.org/10.32505/qadha.v12i2.11178>.
- Aryo Putranto. "Kebocoran Data 6 Juta Wajib Pajak Termasuk Jokowi Diklaim Ulah Peretas Bjorka." *Kompas.Com* (Jakarta), 2024.
- Asyari, Haekal Al. "Between Freedom And Protection: A Critical Review Of Indonesia'S Cyberspace Law." *Prophetic Law Review*, July 4, 2023, 79–103. <https://doi.org/10.20885/PLR.vol5.iss1.art5>.
- Azizah, Imroatul, Lisa Aminatul Mukaromah, Khurul Anam, Sanuri Sanuri, and Nafi' Mubarak. "Digitalization and Cyberfeminism: Reinterpreting Islamic

- Criminal Law for Gender Equality and Women's Rights." *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi*, May 17, 2026, 127-43. <https://doi.org/10.24090/volksgeist.v9i1.15378>.
- BBC News. "Aadhaar: 'Leak' in World's Biggest Database Worries Indians." 2018. <https://www.bbc.com/news/world-asia-india-42575443>.
- BBC.News Indonesia. "Pusat Data Nasional Sementara Lumpuh Akibat Ransomware, Mengapa Instansi Pemerintah Masih Rentan Terhadap Serangan Siber?" 2024. <https://www.bbc.com/indonesia/articles/cxee2985jrvo>.
- Buitelaar, J. C. "Post-Mortem Privacy and Informational Self-Determination." *Ethics and Information Technology* 19, no. 2 (June 2017): 129-42. <https://doi.org/10.1007/s10676-017-9421-9>.
- Chanifah, Nur, Fahd bin Mohana bin Salim al-Ahmadi, Abu Samsudin, Nurul Islami, and Muhammad Najih Vargholy. "The Digitalization of Employment, Fiqh Education and Empowerment of Migrant Workers' Rights." *Justicia Islamica* 23, no. 1 (March 2026): 253-84. <https://doi.org/10.21154/justicia.v23i1.12454>.
- Chesnokova, Lesya. "Information Privacy: Protecting Freedom and Individual Autonomy." *The Digital Scholar Philosopher's Lab* 4, no. 2 (2021): 145-57. <https://doi.org/10.32326/2618-9267-2021-4-2-145-157>.
- Damayanti, Desy, Rahma Hasna Naziha, and Cucu Surahman. "Perspektif Hukum Islam Terhadap Perlindungan Data Pribadi Di Era Digital." *Al-Battar: Jurnal Pamungkas Hukum* 1, no. 3 (December 2024): 151-63. <https://doi.org/10.63142/xzd65n65>.
- Darmawan, Fendi, and Henry Arianto. "Upaya Perlindungan Hukum Dan Tanggung Jawab Kemkomdigi Terhadap Korban Kebocoran Data Pribadi Di Indonesia." *Arus Jurnal Sosial dan Humaniora* 5, no. 3 (December 2025): 3678-88. <https://doi.org/10.57250/ajsh.v5i3.1741>.
- Desy Damayanti, Rahma Hasna Naziha, and Cucu Surahman. "Perspektif Hukum Islam Terhadap Perlindungan Data Pribadi Di Era Digital." *Al-Battar: Jurnal Pamungkas Hukum* 1, no. 3 (2024): 151-63. <https://doi.org/10.63142/xzd65n65>.
- Devayani Nighoskar. "Are Our Aadhaar Identities Available On WhatsApp For Just Rs. 500?" *Homegrown*, 2021. <https://homegrown.co.in/homegrown-explore/are-our-aadhaar-identities-available-on-whatsapp-for-just-rs-500>.
- Evans, Mark, Ying He, Leandros Maglaras, Iryna Yevseyeva, and Helge Janicke. "Evaluating Information Security Core Human Error Causes (IS-CHEC) Technique in Public Sector and Comparison with the Private Sector."

- International Journal of Medical Informatics* 127 (July 2019): 109–19.
<https://doi.org/10.1016/j.ijmedinf.2019.04.019>.
- Fad, Mohammad Farid. “Perlindungan Data Pribadi Dalam Perspektif Sadd Dzari’ah.” *Muamalatuna* 13, no. 1 (June 2021): 33.
<https://doi.org/10.37035/mua.v13i1.4674>.
- Fatarib, Husnul, Zezen Zainul Ali, Nur Aziz Arifin, Abdul Najib, and Muhammad Nur Fathoni. “Progressive Legal Reasoning in Contemporary Islamic Legal Reform: Negotiating the Maqāsid and Hermeneutic Approaches.” *JURIS (Jurnal Ilmiah Syariah)* 24, no. 2 (December 2025): 277–94.
<https://doi.org/10.31958/juris.v24i2.16123>.
- Ghafur, Saira, Emilia Grass, Nick R. Jennings, and Ara Darzi. “The Challenges of Cybersecurity in Health Care: The UK National Health Service as a Case Study.” *The Lancet Digital Health* 1, no. 1 (May 2019): e10–12.
[https://doi.org/10.1016/S2589-7500\(19\)30005-6](https://doi.org/10.1016/S2589-7500(19)30005-6).
- Gibson, Dennis, and Clive Harfield. “Amplifying Victim Vulnerability: Unanticipated Harm and Consequence in Data Breach Notification Policy.” *International Review of Victimology* 29, no. 3 (September 2023): 341–65. <https://doi.org/10.1177/02697580221107683>.
- Goldfus, Yuval. “Tell Me Who Your Friends Are, and I’ll Tell You Who You Are: Privacy and the Social Self.” *SSRN Electronic Journal*, ahead of print, 2023.
<https://doi.org/10.2139/ssrn.4539608>.
- Gstrein, Oskar J., and Anne Beaulieu. “How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches.” *Philosophy & Technology* 35, no. 1 (March 2022): 3.
<https://doi.org/10.1007/s13347-022-00497-4>.
- Hildebrandt, Mireille. “The Fundamental Right of Data Protection.” In *Smart Technologies and the End(s) of Law*, 186–213. Edward Elgar Publishing, 2015. <https://doi.org/10.4337/9781849808774.00017>.
- Huda, Uu Nurul, Dian Rachmat Gumelar, and Alwi Al Hadad. “Fortifying Democracy: Deploying Electoral Justice for Robust Personal Data Protection in the Indonesian Election.” *Khazanah Hukum* 6, no. 1 (March 2024): 24–33. <https://doi.org/10.15575/kh.v6i1.30734>.
- Iskandar. “Data Pemerintah Dominasi 58 Persen Kebocoran Di Dark Web, Platform Baru Ini Tawarkan Deteksi Dini.” *Liputan6.com* (Jakarta), 2025.
- Jasser Auda. *Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach*. International Institute of Islamic Thought (IIIT), 2008.
- Jung, Chea Yun, and Hyun Kyong Joo. “Post-‘Lee-Luda’ Personal Information Protection in Korea: Developer Responsibility and Autonomous AI

- Governance.” *International Data Privacy Law* 13, no. 2 (June 2023): 154–67. <https://doi.org/10.1093/idpl/ipad006>.
- Kang, Na-Mi, and Sang-Jin Park. “Strategies to Enhance the Effectiveness of One-Stop Solution Centers for Crime Victims.” *The Korean Association for Terrorism Studies* 18, no. 2 (June 2025): 74–93. <https://doi.org/10.46350/KATS.2025.18.2.74>.
- Knetsch, Jonas. “The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases.” *Journal of European Tort Law* 13, no. 2 (August 2022): 132–53. <https://doi.org/10.1515/jetl-2022-0008>.
- Kurdi, Kurdi, and Joko Cahyono. “Perlindungan Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022.” *JUNCTO: Jurnal Ilmiah Hukum* 6, no. 2 (December 2024): 330–39. <https://doi.org/10.31289/juncto.v6i2.5443>.
- Maharani, Rista, and Andria Luhur Prakoso. “Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital.” *JURNAL USM LAW REVIEW* 7, no. 1 (March 2024): 333–47. <https://doi.org/10.26623/julr.v7i1.8705>.
- Mailiena, Cristine, and M. Ilham Tanzilulloh. “Normativity of Consumer Protection in the Perspective of Maqāṣid Sharī‘ah.” *Invest Journal of Sharia & Economic Law* 4, no. 1 (August 2024): 176–88. <https://doi.org/10.21154/invest.v4i1.9004>.
- Muzakkie, Shohiban Azkaa, and Eka Juarsa. “Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Pada Aplikasi Pinjaman Online Ilegal Menurut Undang-Undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi.” *Bandung Conference Series: Law Studies* 3, no. 2 (August 2023): 984–87. <https://doi.org/10.29313/bcsls.v3i2.7284>.
- Najlaa Flayyih, Mohammed Hasson Ali, Ahmad Fadii, and Khaled Aljasmi. “The Right to Informational Self-Determination between Legislation and Implementation.” *Access to Justice in Eastern Europe* 8, no. 3 (2025): 362–89. <https://doi.org/10.33327/AJEE-18-8.3-a000116>.
- 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 (November 2025): 107–28. <https://doi.org/10.62509/ajis.v2i2.260>.
- Nišević, Maja, and Aleksandra Ivanković. “Secondary Victimization through Data Protection: Balancing Victim Privacy and Support in the EU Legal Framework.” *International Review of Victimology* 32, no. 1 (January 2026): 65–82. <https://doi.org/10.1177/02697580251374719>.

- Nurani, Nina, Apriwandi Apriwandi, and Hafied Noor Bagja. "Intellectual Property Rights Law Reform Based on Maqāṣid Al-Sharī'ah as a Model for Green Business-Based Creative Industry Protection to Support Sustainable Development." *De Jure: Jurnal Hukum Dan Syar'iah* 18, no. 1 (February 2026): 1–32. <https://doi.org/10.18860/j-fsh.v18i1.40840>.
- Nurulita, Fitri, Neilta Melikiati, Maulana Achsan Al Farisi, and Muhamad Alvian. "Sacred Law in Secular Systems: Shariawiz and Digital Inheritance Fiqh among Muslim Minorities in the United States." *Asy-Syir'ah: Jurnal Ilmu Syari'ah dan Hukum* 59, no. 2 (2025): 252–73. <https://doi.org/10.14421/ajish.v59i2.1642>.
- Okonkwo, Obioma Adesewa. "Structural Asymmetries in Data Ownership, Access to Information, and Human Rights Enforcement across Global Digital Governance Regimes." *World Journal of Advanced Research and Reviews* 4, no. 2 (December 2019): 238–55. <https://doi.org/10.30574/wjarr.2019.4.2.0151>.
- Putra, Rengga Kusuma, Yulia Agustin, Latif Nurul Ihsan, and Zaki Ahmad Dafiqi. "Institutional Dysfunction in Personal Data Protection: A Legal-Political Analysis Based on New Institutional Theory." *Perkara : Jurnal Ilmu Hukum Dan Politik* 3, no. 2 (June 2025): 938–49. <https://doi.org/10.51903/bkktey52>.
- Rahmadani, Siti, and Rina Arum Prastyanti. "Human Rights and Cybersecurity: Reinforcing Legal Protections for Personal Data." *International Journal of Law Dynamics Review* 3, no. 1 (May 2025): 20–29. <https://doi.org/10.62039/ijldr.v3i1.80>.
- Sabina Tiffani and Faisal. "Analisis Hukum Terhadap Perlindungan Data Pribadi (Studi Kasus @farida.Nurhan Dan @codebluuuu)." *Jurnal Ilmu Hukum, Humaniora Dan Politik* 4, no. 3 (April 2024): 291–300. <https://doi.org/10.38035/jihhp.v4i3.1915>.
- Sánchez Arjona, Mercedes Llorente. "Las Víctimas En El Espacio Judicial Europeo: Estudio de La Directiva 2012/29/UE, de 25 de Octubre de 2012." *Revista de Estudios de La Justicia*, no. 22 (November 2015). <https://doi.org/10.5354/0718-4735.2015.37589>.
- Sandika, Arabin, Cholidi Zainuddin, and Arief Wisnu Wardhana. "Legal Protection For Victims Of Misuse Of Personal Data When Making Online Loans." *Jurnal Ilmiah Advokasi* 12, no. 2 (August 2024): 305–16. <https://doi.org/10.36987/jiad.v12i2.5503>.
- Saunders, Jamie. "Tackling Cybercrime – the UK Response." *Journal of Cyber Policy* 2, no. 1 (January 2017): 4–15. <https://doi.org/10.1080/23738871.2017.1293117>.

- Shima, Arliana Agustin Faridhatul, and Lukman Santoso. "Right of Access to Legal Aid for the Poor: Study of Islamic Civil Cases in the PA Ponorogo Legal Area." *Istinbath: Jurnal Hukum* 21, no. 01 (July 2024): 19–39. <https://doi.org/10.32332/istinbath.v21i01.9654>.
- Situmeang, Ampuan, Jihyun Park, Lu Sudirman, Ninne Zahara Silviani, and Shenti Agustini. "Evaluating Data Breach Notification Protocols." *Lentera Hukum* 12, no. 1 (April 2025): 42–61. <https://doi.org/10.19184/ejhl.v12i1.47621>.
- Solove, Daniel J. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154, no. 3 (January 2006): 477. <https://doi.org/10.2307/40041279>.
- Terwangne, Cécile de. "Privacy and Data Protection in Europe: Council of Europe's Convention 108 and the European Union's GDPR." In *Research Handbook on Privacy and Data Protection Law*, 10–35. Edward Elgar Publishing, 2022. <https://doi.org/10.4337/9781786438515.00007>.
- "The European Union's Obligations to Safeguard the Fundamental Right to Data Protection Extraterritorially." In *Transatlantic Jurisdictional Conflicts in Data Protection Law*, 33–56. Cambridge University Press, 2023. <https://doi.org/10.1017/9781108784818.003>.
- Thoriquttyas, Titis, and Nita Rohmawati. "Maqasid Al-Sharia and the Digital Data Ownership: From al-Shatibi to Jasser Auda." *Journal of Islamic Law on Digital Economy and Business*, February 27, 2026, 168–81. <https://doi.org/10.20885/JILDEB.vol1.iss2.art5>.
- Triyanti, Ninuk, I. Gusti Ayu Ketut Rachmi Handayani, and Lego Karjoko. "Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration Law." *Hasanuddin Law Review* 11, no. 1 (January 2025): 132. <https://doi.org/10.20956/halrev.v11i1.6177>.
- Ujade, Shital Harishchandra. "Role of Social Work in Cybercrime Victim Support." *Gurukul International Multidisciplinary Research Journal*, ahead of print, April 14, 2025. <https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0042>.
- Vardanyan, Lusine, Václav Stehlík, and Hovsep Kocharyan. "Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity." *TalTech Journal of European Studies* 12, no. 1 (May 2022): 159–85. <https://doi.org/10.2478/bjes-2022-0008>.
- verihubs. "Statistik Cybercrime Indonesia 2025–2026: Data Dan Tren Terbaru." Accessed April 17, 2026. <https://verihubs.com/blog/statistik-cybercrime-indonesia>.
- Wairimu, Samuel, and Lothar Fritsch. "Modeling Privacy Harms of Compromised Personal Medical Data – beyond Data Breach." *Proceedings*

- of the 17th International Conference on Availability, Reliability and Security (New York, NY, USA), August 23, 2022, 1–9. <https://doi.org/10.1145/3538969.3544462>.
- Waldman, Ari Ezra. “Privacy’s Rights Trap.” *SSRN Electronic Journal*, ahead of print, 2022. <https://doi.org/10.2139/ssrn.4182858>.
- Yoo, Ju Seon. “Personal Information Protection Act Revised in 2023 and My Data Utilization Plan - Focusing on the Insurance Industry -.” *Korea Financial Law Association* 20, no. 2 (August 2023): 55–76. <https://doi.org/10.15692/KJFL.20.2.2>.
- Zaprul Khan, Zaprul Khan. “Maqāṣid Al-Shariah in the Contemporary Islamic Legal Discourse: Perspective of Jasser Auda.” *Walisongo: Jurnal Penelitian Sosial Keagamaan* 26, no. 2 (December 2018): 445. <https://doi.org/10.21580/ws.26.2.3231>.