

DIGITAL JUSTICE AND PERSONAL DATA POLICY: PRIVACY, PLATFORM POWER AND INSTITUTIONAL INDEPENDENCE

Muhammad Ikhlas Rosele¹, Zuhri Arif Sihombing²

¹ Akademi Pengajian Islam (APIUM), Universiti Malaya, Kuala Lumpur

² Universitas Islam Negeri Sumatera Utara Medan, Indonesia

Email: ikhlas@um.edu.my zuhriarifsihombing1@gmail.com

Info Articles	Abstract
Article History Received : 08-13-2026 Revised : 09-18-2026 Published : 10-01-2026 Keywords: <i>Data protection; Digital justice; Hifz al-'ird; Privacy; Supervisory authority.</i> Kata Kunci: <i>Hifz al-'ird; Keadilan digital; Otoritas pengawas; Pelindungan data; Privasi.</i>	Indonesia enacted a comprehensive personal data protection statute in 2022, but its transitional period expired without the establishment of the supervisory authority on which the entire enforcement architecture depends, leaving substantive rights without an institution capable of vindicating them. This study aims to assess the design of Indonesian data protection policy as a problem of justice rather than of compliance, to examine the contribution of Islamic legal doctrine on concealment and the prohibition of spying to the normative foundation of privacy, and to formulate criteria for effective institutional design. The research applies normative juridical research with statutory, conceptual, case and comparative approaches, supported by a maqāsid reading of the protection of honour, drawing on Indonesian legislation, the European and Brazilian frameworks, and the scholarship on informational privacy. The findings show three structural deficits: an enforcement vacuum created by the absence of an independent authority, an asymmetry of consent in which agreement is technically obtained but practically unavoidable, and a public sector exemption pattern that leaves the largest data controller least constrained. Islamic legal doctrine supplies an obligation-centred framework in which the holder of information owes a duty of concealment irrespective of consent. The study recommends an independent authority with budgetary autonomy, statutory limits on consent as a legal basis, and equal application to public bodies. Abstrak Indonesia mengesahkan undang-undang perlindungan data pribadi yang komprehensif pada 2022, namun masa transisinya berakhir tanpa terbentuknya lembaga pengawas yang menjadi tumpuan seluruh arsitektur penegakannya, sehingga hak substantif ada tanpa institusi yang mampu menegakkannya. Penelitian ini bertujuan menilai desain kebijakan perlindungan data Indonesia sebagai persoalan keadilan, bukan sekadar kepatuhan, menelaah sumbangan doktrin hukum Islam tentang menutup aib dan larangan memata-matai bagi landasan normatif privasi, serta merumuskan kriteria desain kelembagaan yang efektif. Penelitian menggunakan metode yuridis normatif dengan

	pendekatan perundang-undangan, konseptual, kasus dan perbandingan, ditopang pembacaan maqāsid atas penjagaan kehormatan. Hasil penelitian menunjukkan tiga defisit struktural: kekosongan penegakan akibat ketiadaan otoritas independen, asimetri persetujuan yang secara teknis diperoleh namun praktis tak terhindarkan, serta pola pengecualian sektor publik yang membuat pengendali data terbesar justru paling sedikit terikat. Doktrin hukum Islam menyediakan kerangka berbasis kewajiban, yakni pemegang informasi menanggung kewajiban menutupi tanpa bergantung pada persetujuan. Penelitian merekomendasikan otoritas independen dengan otonomi anggaran, pembatasan persetujuan sebagai dasar pemrosesan, dan keberlakuan yang setara bagi badan publik.
--	--

I. INTRODUCTION

Personal data has become the principal medium through which power is exercised over individuals outside the traditional institutions of the state. Decisions about credit, employment, insurance, policing and access to public benefits increasingly depend on inferences drawn from data the subject did not knowingly provide and cannot inspect. This is a justice problem before it is a technology problem, because the asymmetry it creates is one of power rather than of information alone.¹

Indonesia legislated on this terrain comparatively late and comparatively comprehensively. The Personal Data Protection Law of 2022 establishes definitions of personal and specific personal data, lawful bases for processing, rights of access, rectification, erasure and objection, obligations of controllers and processors, breach notification duties, and administrative and criminal sanctions, with a two-year transitional period for adjustment.² The statute borrows its architecture visibly from the European framework, including the distinction between controller and processor and the extraterritorial reach of the regime.³

The ideal condition would pair those substantive rights with an independent institution able to receive complaints, investigate controllers, impose sanctions and issue binding guidance. The statute anticipates such a body, assigning supervisory functions to an institution to be established by the President.⁴ The transitional period has passed and the regime's enforcement capacity has remained dependent

¹ Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford: Oxford University Press, 2019), 48–58.

² Law Number 27 of 2022 concerning Personal Data Protection, Articles 4, 20, 26–34 and 58.

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (General Data Protection Regulation), Articles 3, 4 and 6.

⁴ Law Number 27 of 2022, Articles 58–60.

on ministerial administration rather than an autonomous authority, which is a structural rather than a temporary problem: a supervisory body located within the executive branch that also administers major state data systems cannot credibly supervise itself.

A second and related problem concerns the largest processor in the country. Repeated incidents involving population, taxation, social assistance and health data have demonstrated that public bodies hold the most sensitive information at the greatest scale, yet the practical prospect of sanctioning a ministry through an institution subordinate to the same executive is remote. Where the state is simultaneously rule-maker, controller and supervisor, the separation on which enforcement depends collapses.

The scholarly literature offers three relevant lines. Informational privacy theory has moved from control-based accounts towards contextual integrity, which evaluates a data flow by reference to the norms of the context in which the information was originally shared rather than by reference to consent alone.⁵ Regulatory scholarship has documented the limits of consent under conditions of market concentration, where refusal means exclusion from services that are practically compulsory. Islamic legal scholarship has examined privacy through the prohibition of spying, the duty to conceal the faults of others and the inviolability of the dwelling, but rarely in engagement with data protection design.

The gap addressed here lies at that intersection. Indonesian data protection analysis is largely compliance-oriented, cataloguing obligations without interrogating the institutional conditions of their enforcement; Islamic privacy scholarship remains largely ethical. This article asks: what structural deficits does the Indonesian framework exhibit when assessed as a justice problem; what does Islamic legal doctrine contribute to the normative foundation of data protection; and what institutional criteria would make the regime effective?

II. RESEARCH METHODS

The research is normative juridical, employing statutory, conceptual, case and comparative approaches.⁶ The statutory approach analyses the Personal Data Protection Law, the electronic information legislation and its amendments, and the population administration framework, with attention to supervisory design and to exemptions. The conceptual approach reconstructs informational privacy theory, the concept of contextual integrity, and the Islamic doctrines of concealment, the prohibition of spying and the inviolability of private space. The case approach examines constitutional reasoning on privacy and communications. The comparative approach considers the European Union and Brazil, selected because

⁵ Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010), 127–140.

⁶ Peter Mahmud Marzuki, *Penelitian Hukum*, rev. ed. (Jakarta: Kencana, 2017), 55–60.

both pair comprehensive substantive rules with an independent authority, though with different degrees of autonomy.

Primary materials comprise Indonesian legislation and regulations, the European Regulation, the Brazilian statute, judicial decisions, and Qur'ānic and prophetic texts relied on in the classical literature concerning concealment and intrusion. Secondary materials consist of peer-reviewed scholarship from the last fifteen years. Analysis proceeds by qualitative content analysis, comparative tabulation of supervisory design, and normative evaluation against criteria derived from both constitutional and maqāsid reasoning. The study does not include technical audit or empirical measurement of breach incidence.

III. RESULTS AND DISCUSSION

A. Substantive Rights Without an Enforcement Institution

The first finding is that the Indonesian framework is substantively adequate and institutionally incomplete. Rights of access, correction, erasure, objection and portability are recognised; obligations of lawful basis, purpose limitation, security and breach notification are imposed; sanctions are available in principle. What is missing is the institution through which a data subject converts a right into a remedy without litigating individually.

This matters because individual litigation is structurally unsuited to data harms. The loss suffered by any single subject is typically small, diffuse and difficult to quantify, while the cost of proceedings is high and the evidentiary burden falls on the party with least access to the relevant systems. Comparative regimes address this asymmetry by vesting investigation and sanction in a public authority acting on complaint or on its own initiative, which aggregates what individuals cannot. Without such a body, substantive rights become declaratory.

Independence is not a formality in this design. An authority requires appointment procedures insulating members from removal at will, a budget not subject to line-item control by supervised ministries, and jurisdiction extending to public bodies. The European framework treats these as constitutive, requiring complete independence and adequate resources for supervisory authorities.⁷ Brazil's experience illustrates the intermediate case: an authority initially created within the executive and subsequently converted to autonomous status, which demonstrates both the risk of the initial arrangement and the possibility of correction.

B. The Asymmetry of Consent

The second finding concerns the operative weakness of consent. The statute treats consent as a principal lawful basis, and in practice it is the basis on which most commercial processing proceeds. Yet consent presupposes a meaningful alternative,

⁷ Regulation (EU) 2016/679, Articles 52 and 57.

and for services that function as infrastructure for employment, payment, transport and communication, the alternative is exclusion from ordinary economic life.

Contextual integrity clarifies why this matters normatively. The wrong in most data harms is not that information was disclosed but that it flowed into a context governed by different norms: medical information used for credit scoring, location data used for insurance pricing, social assistance records used for political targeting. Consent obtained at the point of collection cannot authorise flows whose contexts were not contemplated, and a regime that treats a single act of agreement as authorising indefinite downstream use is measuring the wrong thing.

The design implication is that consent should be restricted rather than expanded. Legitimate processing bases keyed to purpose, necessity and proportionality carry the analytical burden better, because they require the controller to justify the flow rather than to record an agreement. Statutory recognition that consent is invalid where refusal is not practically available, and prohibition of conditioning service on consent to unrelated processing, would align the Indonesian regime with the substance of its own purpose limitation principle.

C. Islamic Legal Doctrine: An Obligation-Centred Foundation

The third finding is doctrinal. Islamic legal tradition approaches privacy through the duties of those who hold information rather than through the control rights of those to whom it relates. The Qur'ānic prohibition of spying and of backbiting establishes a direct restriction on the acquisition and circulation of information about others, framed as an obligation on the potential acquirer.⁸ The duty to conceal the faults of another, expressed in the prophetic tradition promising divine concealment to one who conceals, operates as a general norm rather than as a right waivable by the subject.⁹

The requirement of permission before entering a dwelling, and the classical elaboration of visual intrusion as a harm distinct from physical entry, extends the protection from the person to the space in which private life occurs.¹⁰ Read functionally, these materials establish three elements directly relevant to data protection design: a prohibition on acquisition without authorisation, a duty of non-disclosure attaching to whoever holds the information, and a protected zone defined by context rather than by ownership.

The significance of this reading is structural rather than rhetorical. An obligation-centred framework does not depend on the subject's consent to generate duties, which addresses precisely the weakness of consent-based regimes under conditions of unequal bargaining power. Within the *maqāṣid* framework,

⁸ Qur'ān 49:12.

⁹ Muslim b. al-Ḥajjāj, *Ṣaḥīḥ Muslim*, ed. Muḥammad Fu'ād 'Abd al-Bāqī (Beirut: Dār Iḥyā' al-Turāth al-'Arabī, n.d.), 4:2074, no. 2699.

¹⁰ Qur'ān 24:27–28.

informational privacy is best located under the protection of honour, with implications for the protection of property and of life where data enables financial or physical harm. Indonesian policy debate can therefore defend strong data protection on indigenous doctrinal grounds rather than solely by reference to European regulation, which matters politically when the framework is criticised as an imported constraint on the digital economy.

D. Comparative Supervisory Design

Table 1. Supervisory Design in Comparative Data Protection Regimes

Jurisdiction	Supervisory institution	Independence guarantee	Scope over public bodies
Indonesia	Body to be established by the President under the statute	Not yet secured in practice; located in relation to the executive	Formally included; enforcement prospect limited
European Union	National supervisory authorities coordinated at Union level	Complete independence and resources required by regulation	Full, with sanction limits for public authorities set by member states
Brazil	National data protection authority, later converted to autonomous status	Fixed terms and budgetary autonomy after conversion	Full, with adapted enforcement for public entities

Source: Processed from primary legal materials, 2026.

The comparison indicates that substantive convergence is easy and institutional convergence is hard. Indonesia has adopted European definitions, bases and rights almost entirely, while omitting the institutional feature on which the European regime's effectiveness rests. Legal transplantation of rules without transplantation of the enforcing institution is a recurrent pattern in regulatory reform, and it predictably produces high formal compliance with low practical protection.

E. Criteria for Effective Digital Justice

Five criteria follow. First, institutional independence: the supervisory authority should be established with fixed terms, removal only for cause, budgetary autonomy and reporting to the legislature rather than to a supervised ministry. Second, equal application to public bodies, with enforcement mechanisms adapted rather than waived, since the largest controllers are public. Third, statutory restriction of consent, invalidating it where refusal entails exclusion from essential services and prohibiting service conditioning on unrelated processing. Fourth, collective redress, permitting representative organisations to bring proceedings, because individual harms are too small to litigate and too numerous to ignore. Fifth, mandatory impact assessment and published breach reporting for high-risk processing, including public sector systems, so that supervision rests on information rather than on incident reporting by the press.

IV. CONCLUSION

Indonesian data protection policy currently pairs a substantively modern statute with an incomplete institutional foundation. Rights of access, correction, erasure and objection exist without an independent authority able to vindicate them at scale; consent functions as a lawful basis under conditions where refusal is not practically available; and the public sector, which holds the most sensitive data at the greatest scale, is least exposed to effective enforcement.

Islamic legal doctrine contributes a foundation particularly well suited to these weaknesses. Its prohibition of intrusive acquisition, its duty of concealment attaching to the holder of information, and its context-defined protected zone together constitute an obligation-centred model that does not depend on the subject's consent to generate duties. Located under the protection of honour within the maqāṣid framework, informational privacy acquires indigenous doctrinal standing rather than the appearance of a transplanted constraint.

The study recommends establishing an independent supervisory authority with budgetary autonomy and legislative accountability, applying the regime equally to public bodies with adapted enforcement, restricting consent as a lawful basis where refusal is not genuinely available, enabling collective redress, and requiring impact assessment and published breach reporting for high-risk processing. Further research should examine whether jurisdictions that adopted comprehensive rules without an independent authority exhibit measurably weaker protection outcomes, which would test the institutional hypothesis advanced here across a larger sample.

REFERENCES

- Bennett, Colin J., and Charles D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd ed. Cambridge: MIT Press, 2006.
- Bygrave, Lee A. *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press, 2014.
- Cohen, Julie E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press, 2019.
- Hijmans, Hielke. *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*. Cham: Springer, 2016.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Revised edition. Jakarta: Kencana, 2017.
- Muslim b. al-Ḥajjāj. *Ṣaḥīḥ Muslim*. Edited by Muḥammad Fu'ād 'Abd al-Bāqī. Beirut: Dār Iḥyā' al-Turāth al-'Arabī, n.d.
- Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2010.
- al-Qaraḍāwī, Yūsuf. *al-Ḥalāl wa-l-Ḥarām fī al-Islām*. Cairo: Maktabat Wahba, 1997.
- Solove, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.

- Auda, Jasser. *Maqasid al-Shariah as Philosophy of Islamic Law: A Systems Approach*. London: International Institute of Islamic Thought, 2008.
- Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.
- General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
- Lei Geral de Proteção de Dados Pessoais, Law Number 13.709 of 2018 (Federative Republic of Brazil).
- Law Number 11 of 2008 concerning Electronic Information and Transactions (Republic of Indonesia), as amended.
- Law Number 24 of 2013 concerning the Amendment to Law Number 23 of 2006 concerning Population Administration (Republic of Indonesia).
- Law Number 27 of 2022 concerning Personal Data Protection (Republic of Indonesia).
- Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (Republic of Indonesia).
- Constitution of the Republic of Indonesia 1945, Article 28G(1).