

Digital Surveillance and the Right to Privacy in Indonesia: Assessing the Human Rights Implications of State Use of Digital Identification Systems

Reza Kurniawan Akbar*
Universitas Airlangga, Surabaya, Indonesia
rezakurniawanakbar@students.unair.ac.id

DOI: <https://doi.org/10.65815/Obj8yt13>

Submitted: 28-07-2025

Revised: 29-09-2025, 15-12-2025

Accepted: 15-01-2026

*Corresponding Author

Abstract

The expansion of digital identification and data-driven public administration has created opportunities to improve government services while raising significant concerns concerning privacy and state surveillance. In Indonesia, increasingly extensive collection and processing of personal data by public institutions require effective safeguards against unauthorized access, excessive monitoring, and misuse. This article examines the human rights implications of state use of digital identification systems in Indonesia. Using normative juridical research and policy analysis, the study evaluates privacy rights, personal data protection, government data governance, and oversight mechanisms. The article argues that digital transformation should not undermine the principle of informational self-determination or permit disproportionate state interference with private life. Particular attention is given to data minimization, purpose limitation, transparency, independent oversight, and effective remedies for individuals affected by data misuse. The study proposes a rights-based governance framework requiring clear legal authority, proportionality assessments, security safeguards, independent supervision, and accessible complaint mechanisms. The article concludes that digital identification can support efficient public administration only when technological capacity is accompanied by strong institutional accountability and meaningful protection of privacy rights.

[Perluasan identifikasi digital dan administrasi publik berbasis data telah menciptakan peluang untuk meningkatkan layanan pemerintah sekaligus menimbulkan kekhawatiran signifikan terkait privasi dan pengawasan negara. Di Indonesia, pengumpulan dan pengolahan data pribadi yang semakin luas oleh lembaga publik memerlukan perlindungan yang efektif terhadap akses tanpa izin, pengawasan berlebihan, dan penyalahgunaan. Artikel ini mengkaji implikasi hak asasi manusia dari penggunaan sistem identifikasi digital oleh negara di Indonesia. Dengan menggunakan penelitian yuridis normatif dan analisis kebijakan, studi ini mengevaluasi hak privasi,

perlindungan data pribadi, tata kelola data pemerintah, dan mekanisme pengawasan. Artikel ini berpendapat bahwa transformasi digital tidak boleh merusak prinsip penentuan nasib sendiri informasional atau mengizinkan campur tangan negara yang tidak proporsional terhadap kehidupan pribadi. Perhatian khusus diberikan pada minimalisasi data, pembatasan tujuan, transparansi, pengawasan independen, dan solusi efektif bagi individu yang terkena dampak penyalahgunaan data. Studi ini mengusulkan kerangka kerja tata kelola berbasis hak yang membutuhkan otoritas hukum yang jelas, penilaian proporsionalitas, perlindungan keamanan, pengawasan independen, dan mekanisme pengaduan yang mudah diakses. Artikel ini menyimpulkan bahwa identifikasi digital dapat mendukung administrasi publik yang efisien hanya jika kapasitas teknologi disertai dengan akuntabilitas kelembagaan yang kuat dan perlindungan hak privasi yang bermakna.]

Keywords: Right to privacy, digital identification, surveillance, data protection, Indonesia

Introduction

Digital transformation has become a central feature of contemporary public administration in Indonesia. Government institutions increasingly rely on digital databases, electronic identification, interoperable information systems, online public services, and automated forms of verification to improve administrative efficiency and expand access to public services. Digital identification is particularly significant because it enables the state to authenticate individuals and connect personal information across different governmental functions. In principle, these developments can reduce administrative duplication, improve the delivery of social assistance, strengthen the accuracy of public records, and make public services more accessible. However, the same technological infrastructure can also expand the capacity of public institutions to collect, combine, analyze, and retain information about individuals. Privacy concerns therefore arise not only from isolated data breaches but also from the structural consequences of data aggregation. When digital identity systems become integrated across multiple sectors, information that was originally collected for one administrative purpose may become technically available for another, thereby creating conditions in which public administration gradually acquires surveillance capacities that exceed its original mandate (Lyon 2018; Richards 2013; Nissenbaum 2010).

The right to privacy has consequently become inseparable from questions concerning the distribution and exercise of state power in digital environments. Privacy should not be understood narrowly as an individual's interest in secrecy or the concealment of wrongdoing. Rather, it protects personal autonomy, dignity, freedom of communication, and the ability of individuals to develop social and

political relationships without unjustified observation. In Indonesia, these concerns have become increasingly relevant following the expansion of electronic government and the enactment of Law No. 27 of 2022 concerning Personal Data Protection. While the legislation represents an important step in recognizing data protection as part of the broader protection of individual rights, its effectiveness depends on institutional capacity, enforcement, and the extent to which public authorities are willing to subject their own data-processing practices to meaningful legal constraints. As Fauzy and Shandy (2023) argue, the right to privacy occupies a constitutional position that cannot be reduced to a purely administrative interest, while recent studies continue to identify institutional fragmentation and weak enforcement as persistent challenges in Indonesian data governance (Krisetya and Rachman 2025; Briantama and Yopan 2025).

This study employs normative juridical research combined with policy analysis. The normative approach examines the legal foundations governing privacy, personal data, digital identification, electronic systems, and state responsibility in Indonesia. The principal legal materials include the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 concerning Personal Data Protection, Law No. 23 of 2006 concerning Population Administration as amended, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System. The study also uses international human rights standards, particularly the International Covenant on Civil and Political Rights and relevant United Nations principles concerning privacy in the digital age. Conceptually, the analysis is informed by the principles of legality, necessity, proportionality, informational self-determination, data minimization, purpose limitation, transparency, and accountability. The policy analysis examines how the increasing integration of government databases can affect the relationship between administrative efficiency and individual rights. Rather than evaluating a single digital identification program, the article identifies broader structural risks arising from the state's expanding technological capacity to identify, classify, and monitor individuals.

Digital Identification and the Expansion of State Informational Power

Digital identification systems fundamentally alter the nature of administrative governance because they transform identity into data that can be collected, stored, authenticated, transmitted, and compared across institutional boundaries. Traditional identification systems generally required physical interaction and were often limited to specific administrative contexts. Digital systems, by contrast, enable identification to occur across time and space, potentially connecting information from different sectors of public administration. This creates significant benefits, including improved verification, reduced identity fraud, and more efficient access to government services. However, digital identification also increases the possibility

that the state can construct increasingly comprehensive profiles of individuals through the aggregation of demographic, biometric, transactional, and behavioral information. The human rights concern is therefore not simply that the government possesses personal data, but that technological interoperability may enable the reconstruction of individual lives in ways that were previously impractical or impossible. Privacy protection must consequently address the architecture of data governance rather than focusing exclusively on unauthorized disclosure or cyberattacks (Solove 2006; Richards 2013; Greenleaf 2019).

The concept of surveillance is particularly relevant because surveillance does not require continuous physical observation by government officials. Digital surveillance can emerge through the routine collection and analysis of information for administrative purposes when those practices allow institutions to identify patterns, track behavior, or infer personal characteristics. Lyon (2018) describes contemporary surveillance as increasingly embedded within ordinary social and institutional processes, meaning that monitoring can become normalized precisely because it is presented as necessary for efficiency or security. In Indonesia, the expansion of digital government creates similar risks when large volumes of data are collected without sufficiently clear limits regarding secondary use, inter-agency sharing, or retention. The existence of a legitimate administrative objective does not automatically justify unlimited data processing. A system created to verify eligibility for public services should not automatically become a general infrastructure for monitoring individuals. The distinction between administration and surveillance may gradually disappear when technological capacity expands faster than the legal principles intended to constrain state power (Putra 2022; Paripurna, Lafrance, and Indriani 2025).

The growing importance of biometric information further intensifies these concerns because biometric data are closely connected to the physical and biological identity of an individual. Unlike passwords or other forms of authentication, many biometric characteristics cannot easily be changed once compromised. The processing of facial, fingerprint, or other biometric information therefore requires heightened protection. Lim (2024) argues that Southeast Asian legal frameworks, including Indonesia's, have developed broader protections for biometric information through omnibus data protection legislation, but significant regulatory challenges remain regarding contemporary uses of such data. Indonesian scholarship similarly emphasizes that facial recognition and other biometric technologies may produce serious privacy risks when deployed without sufficiently clear safeguards concerning legal authority, data security, retention, and accountability (Simanjuntak et al. 2023; Asokawati 2024). The human rights issue is consequently not whether the state may ever use biometric technology, but whether its use is governed by strict conditions that prevent function creep, excessive collection, discriminatory application, and irreversible harm arising from the misuse of sensitive personal information.

Privacy as a Constitutional and Human Rights Limitation on Surveillance

The right to privacy should operate as a substantive limitation on state power rather than merely as a procedural requirement concerning data management. The 1945 Constitution protects personal security, dignity, and the right of individuals to protection over themselves and their property, providing a constitutional foundation for the protection of privacy. Article 17 of the International Covenant on Civil and Political Rights also prohibits arbitrary or unlawful interference with privacy, family, home, or correspondence. These principles require that state interference with private life be governed by law and must not become arbitrary merely because it is technologically possible. Digital identification systems therefore need to be assessed according to the legality and proportionality of each form of data collection and processing. The fact that information may assist administrative decision-making does not establish that every collection practice is necessary. As Wisanjaya (2023) observes, privacy protection in Indonesia must increasingly be understood as part of the broader protection of human rights within an environment characterized by rapidly expanding technological capacity.

A rights-based approach requires the application of at least four interrelated standards: legality, legitimate purpose, necessity, and proportionality. First, intrusive data processing must have a sufficiently clear legal basis. Broad administrative authority should not be interpreted as unlimited permission to collect personal information. Second, the objective of data processing must be legitimate and sufficiently specific. Third, the measure must be necessary, meaning that less intrusive alternatives should be considered. Finally, the overall interference with privacy must be proportionate to the importance of the public objective being pursued. These requirements are particularly important when public authorities process sensitive or biometric information because the potential consequences of misuse are substantial and often difficult to reverse. Recent Indonesian scholarship has identified the absence or weakness of effective oversight as a major obstacle to ensuring that the implementation of personal data protection corresponds with constitutional standards (Simanjuntak 2024; Roselin and Putra 2025). Without independent mechanisms capable of reviewing state practices, proportionality may remain an abstract principle rather than an enforceable legal constraint.

Privacy also protects democratic freedom because individuals may alter their behavior when they believe that communications, movements, or associations are subject to constant observation. Richards (2013) describes surveillance as a threat to intellectual privacy because persistent monitoring can discourage individuals from exploring ideas, communicating freely, or participating in political life. This concern is relevant in the context of digital identification because identification infrastructure can potentially link individuals to multiple domains of social activity. The danger is not limited to the misuse of a single database. It lies in the cumulative effect of interconnected systems that permit different forms of information to

become mutually revealing. A democratic legal system should therefore distinguish between targeted and justified information processing and indiscriminate forms of monitoring. The normalization of broad surveillance powers can undermine privacy even when data are not immediately used for punitive purposes. Accordingly, digital identification governance should incorporate strict access controls, documented decision-making, and independent review to ensure that administrative modernization does not gradually create a system of routine and disproportionate observation (Lyon 2018; Putra 2022).

Personal Data Protection and the Problem of Institutional Accountability

Law No. 27 of 2022 concerning Personal Data Protection represents an important legal development because it establishes a comprehensive framework for the processing and protection of personal data in Indonesia. The law recognizes principles that are consistent with international data protection standards, including limitations on data processing and responsibilities for data controllers. Nevertheless, the adoption of legal principles does not automatically guarantee effective protection. The principal challenge concerns institutional implementation, particularly where public authorities exercise extensive data-processing powers while simultaneously participating in the broader administrative structure responsible for digital transformation. A strong privacy regime requires that government institutions be treated as accountable data controllers rather than presumed to be compliant simply because their activities are carried out in the name of public administration. Research on Indonesia's data protection framework repeatedly identifies institutional readiness and enforcement capacity as critical weaknesses that may limit the practical effectiveness of legal protection (Budiman 2023; Budiarta, Dharsana, and Kresnadjaja 2023; Briantama and Yopan 2025).

Independent oversight is particularly important because privacy violations involving state institutions may not be adequately addressed through internal administrative mechanisms alone. Public institutions possess significant informational and institutional advantages over individual data subjects, who may not know which agency collected their information, how the information was processed, or with whom it was shared. Effective oversight should therefore include the authority to investigate complaints, audit data-processing practices, require corrective measures, and impose meaningful consequences for violations. Comparative research concerning the Indonesian Personal Data Protection Law has similarly emphasized that the effectiveness of rights protection depends on institutional structures capable of providing independent supervision and enforcement (Roselin and Putra 2025). The constitutional responsibility of the state is consequently not limited to protecting citizens from private-sector misuse. As Wiredarme (2025) argues, government institutions themselves must recognize personal data as part of constitutional rights connected to dignity, security, and

individual autonomy. A state that requires citizens to provide information for public services must accept a corresponding obligation to protect that information against excessive collection, misuse, and unauthorized disclosure.

Data security constitutes another essential dimension of institutional accountability because weak cybersecurity can convert administrative databases into sources of vulnerability for the individuals whose information they contain. The consequences of a data breach may include identity theft, discrimination, financial harm, reputational damage, and other forms of long-term risk. Yet a human rights perspective requires more than technical security. It also requires governance structures that reduce unnecessary exposure by limiting collection and retention. The principle of data minimization is therefore particularly important. Government institutions should not collect information merely because technological systems make collection convenient or because the information might become useful in the future. Purpose limitation should also prevent agencies from repurposing information for unrelated objectives without an adequate legal basis. Studies of data processing risks in Indonesia demonstrate that excessive collection, inadequate transparency, and unauthorized access remain significant problems even within sectors that have adopted increasingly sophisticated digital technologies (Safitri and Mahfud 2023; Simanjuntak 2024). Privacy protection is consequently inseparable from the institutional discipline of collecting less, retaining less, and sharing only what is legally necessary.

Toward a Human Rights-Based Governance Framework

A rights-based governance framework for digital identification should begin with the recognition that technological capacity cannot determine the scope of lawful state power. The ability to identify individuals more accurately or process large volumes of information more rapidly does not itself justify the collection of additional data. Every intrusive practice should therefore be connected to a specific legal purpose and subjected to a necessity and proportionality assessment. Before implementing new identification technologies, government institutions should conduct human rights and data protection impact assessments that examine the categories of information collected, the sensitivity of the data, the affected population, the likelihood of misuse, the availability of less intrusive alternatives, and the potential consequences of data breaches. These assessments should not be treated as purely technical documents. Their function is to identify whether the proposed system creates an unjustified interference with privacy before the technology becomes embedded in public administration. Such an approach is consistent with broader arguments that digital governance must balance efficiency with accountability and individual rights (Aminah and Saksono 2021; Greenleaf 2019; Fauzy and Shandy 2023).

Transparency must also be understood as a substantive requirement of democratic accountability. Individuals should receive clear information concerning

what data are collected, why they are collected, how long they are retained, which institutions may access them, and what procedures exist for correction or objection. However, transparency alone is insufficient if individuals have no meaningful ability to challenge harmful decisions. A rights-based system should therefore provide accessible mechanisms for data subjects to obtain information, correct inaccurate records, contest unlawful processing, and seek remedies for harm. These mechanisms should be designed to address the asymmetry between citizens and government institutions. Complex bureaucratic procedures, high costs, or inaccessible complaint systems can effectively prevent individuals from exercising their rights even when those rights are formally recognized. Research on Indonesian digital governance increasingly demonstrates that legal awareness, institutional capacity, and public accessibility remain essential to the practical realization of privacy rights (Darnela and Rusdiana 2025; Krisetya and Rachman 2025; Wiredarme 2025).

The governance of digital identification should further recognize the particular dangers associated with sensitive and biometric information. These categories of data should be subject to heightened requirements concerning collection, storage, access, and sharing. Governments should adopt technical measures such as encryption, access logging, role-based authorization, and regular security audits, but technical safeguards must be combined with institutional accountability. Every access to sensitive databases should be traceable, every inter-agency transfer should have a documented legal basis, and every significant automated process should be subject to review. Where algorithmic systems are used to assess eligibility or detect identity irregularities, individuals should not be denied meaningful human review merely because the decision was generated through an automated system. The growing use of artificial intelligence in public governance also creates additional risks concerning bias, opacity, and accountability, making it increasingly necessary to connect data protection with broader human rights principles (Agustian et al. 2025). Efficient administration should therefore remain subordinate to the constitutional requirement that individuals retain legal protection against unjustified and opaque exercises of state power.

Conclusion

Digital identification can provide substantial benefits for public administration in Indonesia by improving the accuracy, accessibility, and efficiency of government services. However, the expansion of digital identification simultaneously increases the state's capacity to collect, integrate, and analyze information concerning individuals. The principal human rights concern is therefore not limited to unauthorized data breaches. It also concerns the gradual transformation of administrative data systems into broader infrastructures of surveillance when data collection, interoperability, and secondary use are not subject to clear legal limitations. Indonesian constitutional guarantees, international human rights

principles, and Law No. 27 of 2022 concerning Personal Data Protection provide an important normative foundation for protecting privacy, but the effectiveness of these protections depends on implementation. Legal authority must be specific, data processing must serve legitimate purposes, and intrusive measures must satisfy requirements of necessity and proportionality. Without meaningful institutional constraints, technological convenience may gradually replace legal justification as the practical basis for expanding state access to personal information.

Indonesia should therefore adopt a more explicit human rights-based framework for the governance of digital identification and state data processing. Such a framework should require data minimization, purpose limitation, heightened protection for biometric information, human rights impact assessments, transparent processing, strong cybersecurity, independent supervision, and accessible remedies. Public institutions should be treated as accountable data controllers and should not be exempt from rigorous oversight merely because their activities pursue administrative or security objectives. Digital transformation will be compatible with human rights only when efficiency is accompanied by institutional responsibility and when individuals retain meaningful control over how their personal information is collected and used. The future legitimacy of Indonesia's digital state will consequently depend not only on technological sophistication but also on its ability to ensure that digital identification strengthens public services without normalizing disproportionate surveillance or weakening the constitutional right to privacy.

References

- Agustian, Dimas, S. Y. Regif, Hendrikus Hironimus Botha, Andre Pattipeilohy, and Samsul Ode. 2025. "Artificial Intelligence in the Implementation of Public Governance: Public Data Security Vulnerabilities in Indonesia." *Jurnal Kebijakan Publik* 16 (1).
- Aminah, Siti, and Herie Saksono. 2021. "Digital Transformation of the Government: A Case Study in Indonesia." *Jurnal Komunikasi: Malaysian Journal of Communication* 37 (2): 272–88. <https://doi.org/10.17576/JKMJC-2021-3702-17>.
- Asokawati, Ainunnisa Rezky. 2024. "Perlindungan Data Biometrik dalam Sektor Perbankan di Indonesia dan Amerika Serikat." *Legal Standing: Jurnal Ilmu Hukum* 8 (3). <https://doi.org/10.24269/lis.v8i3a.10775>.
- Briantama, Abednego, and Muhamad Yopan. 2025. "An Analysis of Digital Institutional Capacity and Personal Data Protection Policy Implementation in Indonesia: A Systematic Literature Review." *Journal of Law, Politic and Humanities* 6 (4). <https://doi.org/10.38035/jlph.v6i4.3253>.
- Budiarta, I Nyoman Putu, I Made Pria Dharsana, and Indrasari Kresnadjaja. 2023. "Penguatan Konstruksi Hukum Perihal Perlindungan Data Pribadi." *Jurnal*

- Magister Hukum Udayana* 12 (1).
<https://doi.org/10.24843/JMHU.2023.v12.i01.p05>.
- Budiman, Risky. 2023. "The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022." *Jurnal Smart Hukum* 2 (1): 24–36.
<https://doi.org/10.55299/jsh.v2i1.1352>.
- Darnela, Lindra, and Erma Rusdiana. 2025. "Public Legal Awareness and the Effectiveness of Indonesia's Personal Data Protection Law: Bridging Normative Framework and Privacy Paradox." *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*.
- Fauzy, Elfian, and Nabila Alif Radika Shandy. 2023. "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." *Lex Renaissance* 7 (3). <https://doi.org/10.20885/JLR.vol7.iss3.art1>.
- Greenleaf, Graham. 2019. "Global Data Privacy Laws 2019: 132 National Laws and Many Bills." *Privacy Laws & Business International Report* 157: 10–13.
- Krisetya, Beltsazar A., and Rifqi Rachman. 2025. "Indonesia's Information Governance: New Nomenclatures, Same Old Problems?" *Indonesian Quarterly* 52 (4): 337–56.
- Lim, Abigail Chiu Mei. 2024. "Biometric Data Landscape in Southeast Asia: Challenges and Opportunities for Effective Regulation." *Computer Law & Security Review* 55. <https://doi.org/10.1016/j.clsr.2024.106056>.
- Lyon, David. 2018. "The Culture of Surveillance: Watching as a Way of Life." *Surveillance & Society* 16 (3): 363–67.
- Nissenbaum, Helen. 2010. "Privacy as Contextual Integrity." *Washington Law Review* 79: 119–57.
- Paripurna, Amira, S̄bastien Lafrance, and Masitoh Indriani. 2025. "Intelligence Surveillance, Counterterrorism, and the Right to Privacy in Indonesia and Canada." *Journal of Southeast Asian Human Rights* 9 (2).
<https://doi.org/10.19184/jseahr.v9i2.41171>.
- Priyantiwi, Rizky Dwi, and Hufron. 2025. "Ensuring Legal Protection of Personal Data in Indonesia's Digital Identity System." *Justitia Jurnal Hukum* 9 (2).
<https://doi.org/10.30651/justitia.v9i2.27113>.
- Putra, Gilang Rizki Aji. 2022. "Hak Privasi vs Kepentingan Negara dalam Pengawasan Siber: Menemukan Keseimbangan Konstitusional di Era Digital Panopticon." *ADALAH: Buletin Hukum dan Keadilan* 6 (7).
<https://doi.org/10.15408/adalah.v6i7.51169>.
- Richards, Neil M. 2013. "The Dangers of Surveillance." *Harvard Law Review* 126 (7): 1934–65.
- Roselin, Sofia, and Moody Rizqy Syailendra Putra. 2025. "Personal Data Subject Rights Protection: A Comparative Study between Indonesian PDP Law and the UK Data Protection Act." *Jurnal USM Law Review* 8 (2).
<https://doi.org/10.26623/julr.v8i2.12076>.

- Safitri, Merlita Yuli, and Mahfud Mahfud. 2023. "The ASEAN Cross-Border Personal Data Transfer Instrument: Has Indonesia's Personal Data Protection Law Followed It?" *Jurnal Magister Hukum Udayana* 12 (3): 553–64. <https://doi.org/10.24843/JMHU.2023.v12.i03.p06>.
- Simanjuntak, Predderics Hockop. 2024. "Perlindungan Hukum terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation." *Esensi Hukum* 6 (2). <https://doi.org/10.35586/esensihukum.v6i2.412>.
- Simanjuntak, Yonatan Kornelius, Daffa Triakhsan Putra, Gragela L. Panjaitan, Christopher Geraldo Siregar, and Natasya Sabatini Putri Pangaribuan. 2023. "Privacy Protection and the Use of Facial Recognition Technology in Public Surveillance: Legal Perspectives and Policy Implementation in the Digital Era." *Problematika Hukum* 9 (1). <https://doi.org/10.33021/ph.v9i1.5200>.
- Solove, Daniel J. 2006. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 (3): 477–560.
- Suhardi, Muhammad. 2025. "State Responsibility in Personal Data Protection within the Electronic-Based Government System." *Jurnal Kecerdasan Buatan dan Teknologi Informasi* 4 (3). <https://doi.org/10.69916/jkbt.v4i3.458>.
- Tarumanagara, Sofia Roselin, and Moody Rizqy Syailendra Putra. 2025. "Personal Data Subject Rights Protection: A Comparative Study between Indonesian PDP Law and the UK Data Protection Act." *Jurnal USM Law Review* 8 (2).
- Wiredarme. 2025. "Tanggung Jawab Konstitusional Negara terhadap Perlindungan Data Pribadi Warga dalam Penyelenggaraan Pemerintahan Digital." *Jurnal Perlindungan Masyarakat: Bestuur Praesidium* 2 (1): 17–30.
- Wisanjaya, I Gede Pasek Eka. 2023. "Perlindungan Hak Privasi sebagai Bagian dari Hak Asasi Manusia dalam Sistem Hukum Nasional Indonesia." *Jurnal Magister Hukum Udayana* 12 (4). <https://doi.org/10.24843/JMHU.2023.v12.i04.p08>.
- Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75–89.

Legal Sources

- Constitution of the Republic of Indonesia of 1945.
- Indonesia. 2006. *Law No. 23 of 2006 concerning Population Administration*, as amended.
- Indonesia. 2019. *Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions*.
- Indonesia. 2018. *Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System*.
- Indonesia. 2022. *Law No. 27 of 2022 concerning Personal Data Protection*.

United Nations. 1966. *International Covenant on Civil and Political Rights*.

Acknowledgment

None

Funding Information

None

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement

N/A