IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.3 . No.1, February 2026
DOI : https://doi.org/10.62872/1w6a2t71

Privacy, Surveillance, and Constitutional Rights in the Digital State

Marudut Hasugian[1], Anis Noviya[2], Third Author[3]
[1]Universitas Cendrawasih, Indonesia
[2]Universitas Jambi,

Received: December 25, 2025
Revised: January 22, 2026
Accepted: February 02, 2026
Published: February 12, 2026

Corresponding Author:
Author Name*: Marudut Hasugian
Email*: onggol84@gmail.com

***Abstrak*:** *The transformation of Indonesia into a digital state has intensified the use of digital surveillance technologies, including big data analytics, biometric systems, and algorithmic monitoring, in the name of public administration, security, and governance efficiency. While these developments promise administrative effectiveness, they simultaneously pose serious constitutional challenges to the protection of privacy as a fundamental right. This article examines the normative position of privacy within Indonesia's constitutional framework and analyzes the problem of normative ambiguity surrounding state surveillance in the digital era. Employing normative juridical research with statute, conceptual, and case approaches, this study identifies the absence of clear constitutional limits on surveillance authority, vague standards for public interest and national security justifications, and weak mechanisms of accountability and oversight. The findings demonstrate that such ambiguity risks legitimizing an over-surveillance state and undermines legal certainty and substantive constitutional protection. This article argues that privacy in the digital state must be reconstructed as a core constitutional safeguard through clear legal bases, proportionality requirements, mandatory judicial authorization, and independent supervisory mechanisms, ensuring a balanced relationship between state power and fundamental rights.*

Keywords : privacy, digital surveillance, constitutional rights, digital state, data protection

INTRODUCTION

The transformation toward a digital state has fundamentally altered the relationship between state power and constitutional rights, particularly the right to privacy. The extensive use of big data, artificial intelligence, biometric identification, and digital surveillance systems by the state is no longer limited to national security purposes but increasingly embedded in public service delivery, administrative governance, and social regulation. In this context, privacy ceases to function merely as an individual interest and emerges as a constitutional guarantee that structures the legitimacy of state action in the digital sphere.[1]

Within the Indonesian constitutional framework, the protection of privacy is implicitly embedded in the guarantees of personal security, freedom from arbitrary interference, and the right to communicate and obtain information. However, the digitalization of governance has expanded the state's capacity to collect,

[1] Syahwami Syahwami and Hamirul Hamirul, "The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia," *Enigma in Law* 2, no. 2 (2024), https://doi.org/10.61996/law.v2i2.56

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.3 . No.1, February 2026
DOI : https://doi.org/10.62872/1w6a2t71

process, and monitor personal data on an unprecedented scale, often without clear procedural safeguards or effective oversight mechanisms. This expansion raises a fundamental constitutional tension between efficiency-driven digital governance and the protection of fundamental rights.[2]

A critical legal issue arises from the normative ambiguity surrounding the constitutional limits of state surveillance in Indonesia. Positive law does not clearly define the scope of permissible digital surveillance, the criteria of necessity and proportionality, nor the procedural requirements that must be fulfilled before surveillance measures may lawfully restrict privacy rights. This ambiguity is evident in the fragmented regulation of surveillance powers across sectoral legislation, which tends to prioritize administrative convenience and security objectives over constitutional rights protection.[3]

The absence of a coherent constitutional framework governing digital surveillance generates serious legal consequences. First, it weakens legal certainty by allowing discretionary expansion of surveillance practices without clear normative boundaries. Second, it increases the risk of transforming digital governance into a form of over-surveillance state, where privacy protection becomes contingent rather than guaranteed. Third, it undermines accountability by obscuring responsibility for rights violations arising from unlawful or excessive data processing.[4]

This article argues that the core problem lies not in the existence of surveillance technologies themselves, but in the lack of a constitutionally grounded normative structure governing their use. Existing regulations, including the Personal Data Protection Act and amendments to the Electronic Information and Transactions Law, have not yet fully articulated surveillance as a constitutional issue subject to strict limitations, judicial control, and effective remedies. As a result, the protection of privacy remains normatively vulnerable in the digital state framework.[5]

Based on these concerns, this research formulates three central questions. First, how does normative ambiguity manifest in the regulation of privacy and state surveillance within Indonesia's constitutional order? Second, what are the juridical implications of such ambiguity for the protection of constitutional rights in the digital state? Third, how should a normative framework be reconstructed to ensure that digital surveillance operates within clear constitutional limits while maintaining legitimate state interests in security and governance?

METHOD

This research employs a normative juridical method with a prescriptive and critical orientation. The study focuses on examining legal norms governing privacy and state surveillance within Indonesia's constitutional framework, rather than empirical measurement of technological practices. The normative

[2] Naeem Allahrakha, "Constitutional Safeguards for Digital Rights and Privacy," *International Journal of Law and Policy* (2024), https://doi.org/10.59022/ijlp.172

[3] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28G ayat (1), Pasal 28F, dan Pasal 28J.

[4] Tereza Svobodová, "Recalibrating Liberty and Security: Human Rights Challenges in the Age of Mass Surveillance," *Congress Proceedings* (2025), https://doi.org/10.55843/icl2025cong117s

[5] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.3 . No.1, February 2026
DOI : https://doi.org/10.62872/1w6a2t71

approach is essential to evaluate whether existing legal instruments adequately protect constitutional rights in the context of digital governance.[6]

The statute approach is used to analyze constitutional provisions and statutory regulations relevant to digital surveillance and privacy protection, including the 1945 Constitution, the Personal Data Protection Act, the Electronic Information and Transactions Law, and administrative governance regulations. This approach aims to identify inconsistencies, gaps, and ambiguities that weaken constitutional safeguards.[7]

The conceptual approach draws upon theories of constitutionalism, digital rights, and surveillance state doctrine to assess the legitimacy of state intervention in private digital spaces. Through this approach, privacy is conceptualized not merely as an individual entitlement but as a structural limitation on state power that preserves democratic accountability in the digital era.[8] In addition, the case approach is applied by examining judicial decisions related to privacy, interception, data protection, and administrative surveillance. These cases are analyzed to evaluate how courts interpret constitutional protections in the absence of explicit surveillance standards and to assess whether judicial reasoning contributes to or mitigates normative uncertainty.[9]

Legal materials used in this research consist of primary legal materials in the form of legislation and court decisions, secondary legal materials including scholarly articles and doctrinal works on constitutional law and digital governance, and tertiary materials such as legal dictionaries and encyclopedias. The analysis is conducted through systematic and teleological interpretation to formulate prescriptive recommendations for strengthening constitutional protection in the digital surveillance era.

DISCUSSION

Privacy as a Constitutional Right in the Digital State

Privacy has long been recognized as an inherent component of constitutional rights, even in legal systems that do not explicitly enumerate it as an autonomous right. In the Indonesian constitutional framework, privacy is derived from broader guarantees of personal security, dignity, and freedom from arbitrary interference, as reflected in Article 28G paragraph (1) of the 1945 Constitution. In the digital state context, this derivative protection acquires heightened constitutional relevance because state actions increasingly penetrate personal and informational spheres that were previously inaccessible.[10]

The digitalization of governance fundamentally alters the nature of state interference with private life. Traditional conceptions of privacy focused on physical intrusion or direct coercion, whereas digital surveillance operates through continuous, automated, and often invisible data collection. This shift creates a structural imbalance between the state's technological capacity and the individual's ability to exercise meaningful control over personal information. Consequently, privacy in the digital state must be understood

[6] Peter Mahmud Marzuki, *Legal Research: A Revised Edition* (Jakarta: Kencana, 2017).

[7] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

[8] Lucas Henrique Muniz da Conceição, "Assessing Societal and Digital Constitutionalism in Platform Governance," *Global Constitutionalism* (2024), https://doi.org/10.1017/s2045381723000394

[9] Elena Ionescu, "Privacy and Digital Surveillance in Contemporary Conflicts," *Congress Proceedings* (2025),

[10] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28G ayat (1)

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.3 . No.1, February 2026
DOI : https://doi.org/10.62872/1w6a2t71

not merely as freedom from intrusion, but as a constitutional safeguard against asymmetric informational power exercised by public authorities.[11]

Within Indonesian positive law, the enactment of the Personal Data Protection Act represents a significant step toward recognizing privacy as a legally protected interest. However, the Act primarily frames privacy as a matter of data processing compliance rather than as a constitutional limitation on state power. While it regulates consent, purpose limitation, and data security, it does not comprehensively articulate how privacy functions as a constitutional right capable of restricting surveillance measures justified by administrative efficiency or national security.[12]

This regulatory orientation reflects a deeper normative problem: the absence of a clear constitutional doctrine governing privacy in the digital state. Existing legislation tends to treat privacy protection as a technical or administrative obligation, rather than as a substantive constitutional principle that requires strict justification, necessity, and proportionality. As a result, surveillance practices embedded in public administration, electronic governance systems, and security policies may comply with statutory procedures while still undermining the essence of constitutional rights.[13]

Judicial practice further illustrates this normative ambiguity. Courts have generally addressed privacy-related disputes indirectly, often framing them as matters of administrative legality or procedural compliance rather than constitutional rights violations. The lack of a consistent constitutional test for assessing digital surveillance allows judicial reasoning to defer excessively to legislative or executive discretion. This weakens the judiciary's role as a guardian of constitutional rights in the digital environment and reinforces the perception of privacy as a secondary interest.[14]

From a constitutional perspective, privacy in the digital state should function as a structural limitation on governance rather than a negotiable policy consideration. This requires repositioning privacy as a core element of constitutionalism that constrains how the state designs, implements, and justifies digital surveillance systems. Without such repositioning, the expansion of digital governance risks normalizing intrusive practices under the guise of modernization, thereby eroding constitutional protections incrementally but systematically.[15]

Accordingly, the normative position of privacy must be reconstructed as a constitutional right that imposes substantive obligations on the state. These obligations include clearly defined legal bases for surveillance, strict necessity and proportionality standards, and effective judicial oversight. Only by embedding these requirements within the constitutional understanding of privacy can the digital state maintain legitimacy while safeguarding fundamental rights in an era of pervasive surveillance.

[11] Anri Nishnianidze, "Surveillance in the Digital Age," *European Scientific Journal* 20, no. 37 (2024),
[12] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
[13] Naeem Allahrakha, "Constitutional Safeguards for Digital Rights and Privacy," *International Journal of Law and Policy* (2024)
[14] Syahwami Syahwami and Hamirul Hamirul, "The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia," *Enigma in Law* 2, no. 2 (2024)
[15] Lucas Henrique Muniz da Conceição, "Assessing Societal and Digital Constitutionalism in Platform Governance," *Global Constitutionalism* (2024)

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.3 . No.1, February 2026
DOI : https://doi.org/10.62872/1w6a2t71

Normative Ambiguity in State Surveillance and Digital Governance

The expansion of state surveillance in the digital era reveals a fundamental **normative ambiguity** within Indonesia's legal framework regarding the constitutional limits of governmental power. While digital surveillance is justified on grounds of national security, public order, and administrative efficiency, positive law fails to articulate clear criteria defining when and how such measures may lawfully restrict the right to privacy. This absence of explicit constitutional thresholds blurs the distinction between legitimate governance and excessive intrusion.[16]

One primary source of ambiguity lies in the fragmentation of surveillance authority across multiple sectoral regulations. Surveillance powers are embedded within laws governing electronic information, administrative governance, cybersecurity, and public services, yet these laws rarely provide a unified definition of surveillance or a consistent standard for its constitutional justification. As a result, surveillance practices are regulated procedurally rather than substantively, allowing broad discretionary interpretation by executive authorities.[17]

The lack of normative clarity is further exacerbated by the vague formulation of public interest and national security as justificatory grounds. Indonesian legislation frequently invokes these concepts without providing measurable criteria or procedural safeguards to ensure proportionality. In practice, this enables surveillance measures to be normalized as routine administrative tools rather than treated as exceptional actions requiring strict justification. Such normalization undermines the constitutional requirement that any limitation of fundamental rights must be necessary and proportionate.[18]

Another critical dimension of normative ambiguity concerns the absence of effective oversight mechanisms. Although certain surveillance-related actions may require internal authorization, the law does not consistently mandate prior judicial approval or independent review. This weakens accountability and reduces the possibility of meaningful constitutional control over surveillance practices. Consequently, individuals affected by unlawful or excessive surveillance face significant barriers in accessing remedies and enforcing their constitutional rights.[19]

Judicial practice has not sufficiently mitigated these ambiguities. Courts tend to assess surveillance-related disputes through administrative legality or statutory compliance rather than constitutional proportionality analysis. This approach reinforces executive dominance in defining surveillance boundaries and limits the judiciary's role as a constitutional counterbalance. Without a clear constitutional doctrine, judicial deference risks legitimizing expansive surveillance practices that gradually erode privacy protections.[20]

To clarify these normative uncertainties, it is essential to map the existing regulatory framework and identify where constitutional safeguards are absent or insufficient. The following table illustrates the key

[16] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28J.

[17] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

[18] Amina Sethi, Hafiz Haseeb Ullah, and Rana Muhammad Shahid Naseem, "Surveillance, National Security and the Right to Privacy in the Digital Era," *The Critical Review of Social Sciences Studies* (2025).

[19] Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan.

[20] Syahwami Syahwami and Hamirul Hamirul, "The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia," *Enigma in Law* 2, no. 2 (2024)

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.3 . No.1, February 2026
DOI : https://doi.org/10.62872/1w6a2t71

areas of normative ambiguity in Indonesian digital surveillance governance and their constitutional implications.

Table 1. Normative Ambiguity in State Surveillance Regulation and Constitutional Implications

Regulatory Aspect	Existing Legal Regulation	Identified Normative Ambiguity	Constitutional Implication
Scope of surveillance authority	Sectoral laws (UU ITE, UU PDP, SPBE regulations)	No unified definition or clear limitation of surveillance powers	Risk of excessive state discretion and privacy erosion
Justification grounds	Public interest and national security clauses	Vague and non-measurable criteria	Weak proportionality control
Authorization mechanism	Predominantly administrative approval	Absence of mandatory judicial authorization	Reduced accountability
Oversight and accountability	Internal supervision mechanisms	Lack of independent oversight bodies	Limited remedies for rights violations
Judicial review	Case-by-case administrative review	No consistent constitutional test	Inconsistent protection of privacy rights

The table demonstrates that normative ambiguity is systemic rather than incidental. It affects the foundational elements of surveillance regulation, from authorization to oversight, and directly weakens constitutional guarantees. Without a coherent constitutional framework, surveillance governance risks evolving into a self-legitimizing system driven by efficiency and security narratives rather than rights-based limitations.[21]

Therefore, resolving normative ambiguity is not merely a matter of legislative refinement but a constitutional necessity. Clear standards grounded in legality, necessity, proportionality, and accountability must be articulated to ensure that digital governance does not undermine the constitutional order it purports to strengthen.

Reconstructing Constitutional Protection in the Digital Surveillance Era

The persistence of normative ambiguity in digital surveillance governance necessitates a constitutional reconstruction of privacy protection within the digital state. Rather than treating surveillance as a purely administrative or technical matter, constitutional law must reassert its function as a limiting framework that disciplines state power. In this sense, the digital state should not expand constitutional authority but instead intensify constitutional control due to the heightened risks posed by technologically mediated surveillance.[22]

A core element of this reconstruction is the reaffirmation of the principle of legality in digital surveillance. Surveillance measures must be explicitly grounded in law that clearly defines their scope, objectives, and limits. Vague statutory mandates or open-ended delegations of authority are constitutionally insufficient

[21] Tereza Svobodová, "Recalibrating Liberty and Security: Human Rights Challenges in the Age of Mass Surveillance," *Congress Proceedings* (2025),

[22] O. Gstrein, "Mapping Power and Jurisdiction on the Internet through the Lens of Government-Led Surveillance," *Internet Policy Review* 9 (2020)

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.3 . No.1, February 2026
DOI : https://doi.org/10.62872/1w6a2t71

when fundamental rights are at stake. Legal certainty, as guaranteed by Article 28D paragraph (1) of the 1945 Constitution, requires that individuals be able to foresee the legal consequences of state surveillance practices.[23]

Beyond legality, the principle of proportionality must operate as a substantive constitutional test. Surveillance should only be permitted when it pursues a legitimate aim, is strictly necessary, and constitutes the least intrusive means available. In the digital context, proportionality serves as a critical safeguard against the normalization of mass or preventive surveillance that treats all citizens as potential subjects of control. Without proportionality, surveillance risks becoming structurally incompatible with constitutional democracy.[24]

Judicial authorization constitutes another indispensable pillar of constitutional reconstruction. Surveillance measures that intrude upon privacy must be subject to prior judicial review rather than solely administrative approval. Judicial oversight functions not merely as a procedural formality but as an institutional mechanism that balances executive efficiency against constitutional rights protection. The absence of mandatory judicial authorization significantly weakens accountability and facilitates unchecked expansion of surveillance powers.[25]

In addition, the digital state requires independent oversight mechanisms to ensure ongoing accountability. Given the technical complexity and opacity of surveillance technologies, traditional forms of administrative supervision are insufficient. Independent supervisory bodies with investigatory and corrective powers are necessary to monitor compliance, address violations, and provide effective remedies for affected individuals. Such mechanisms reinforce the constitutional principle that state power, even when technologically advanced, remains subject to control.[26]

Ultimately, constitutional reconstruction must reposition privacy as a structural component of democratic governance rather than an exception that yields to security or efficiency claims. This repositioning does not deny the legitimacy of state surveillance but subjects it to constitutional discipline. Only through a coherent framework integrating legality, proportionality, judicial oversight, and independent accountability can the digital state maintain constitutional legitimacy while safeguarding fundamental rights.[27]

CONCLUSIONS

The emergence of the digital state has fundamentally transformed the relationship between state authority and constitutional rights, particularly the right to privacy. Digital surveillance technologies amplify the state's capacity to monitor, collect, and process personal data, thereby intensifying the constitutional stakes of governance in the digital era. This study demonstrates that Indonesia's legal framework suffers from normative ambiguity regarding the constitutional limits of state surveillance. Fragmented regulation, vague justificatory standards, and weak oversight mechanisms collectively undermine legal certainty and increase the risk of an over-surveillance state. Privacy protection, as currently regulated, remains insufficiently

[23] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28D ayat (1)

[24] Tereza Svobodová, "Recalibrating Liberty and Security: Human Rights Challenges in the Age of Mass Surveillance," *Congress Proceedings* (2025)

[25] Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan.

[26] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

[27] Naeem Allahrakha, "Constitutional Safeguards for Digital Rights and Privacy," *International Journal of Law and Policy* (2024).

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.3 . No.1, February 2026
DOI : https://doi.org/10.62872/1w6a2t71

anchored in constitutional doctrine. Accordingly, this article concludes that effective protection of privacy in the digital state requires a normative reconstruction grounded in constitutional principles. Surveillance must be governed by clear legal bases, subjected to strict proportionality, authorized through judicial control, and monitored by independent oversight institutions. Without such reconstruction, digital governance risks eroding constitutional rights under the guise of modernization and security.

REFERENCES

Book

Marzuki, P. M. (2017). Penelitian hukum (Edisi revisi). Kencana.

Journal Article

Allahrakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. International Journal of Law and Policy. https://doi.org/10.59022/ijlp.172.

Allahrakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. International Journal of Law and Policy. https://doi.org/10.59022/ijlp.172.

Chan, H., & Lo, N. (2025). A Study on Human Rights Impact with the Advancement of Artificial Intelligence. Journal of Posthumanism. https://doi.org/10.63332/joph.v5i2.490.

Da Conceição, L. (2024). A constitutional reflector? Assessing societal and digital constitutionalism in Meta's Oversight Board. Global Constitutionalism. https://doi.org/10.1017/s2045381723000394

Fussey, P., & Sandhu, A. (2020). Surveillance arbitration in the era of digital policing. Theoretical Criminology, 26, 3 - 22. https://doi.org/10.1177/1362480620967020.

Gstrein, O. (2020). Mapping power and jurisdiction on the internet through the lens of government-led surveillance. Internet Policy Rev., 9. https://doi.org/10.14763/2020.3.1497.

Imam, M., Manimekalai, N., & Suba, S. (2025). From Data to Discrimination: Gender, Privacy, and the Politics of Digital Surveillance. Synergy: International Journal of Multidisciplinary Studies. https://doi.org/10.63960/sijmds-2025-2262.

Ionescu, E. (2025). Privacy And Digital Surveillance In Contemporary Conflicts: Assessing The Legality Of Mass Data Collection Under International Law. Congress Proceedings. https://doi.org/10.55843/icl2025cong60i.

Joshi, F. (2025). Digital Privacy vs. State Surveillance: Balancing Fundamental Rights in Cyber Investigations. International Journal For Multidisciplinary Research. https://doi.org/10.36948/ijfmr.2025.v07i05.59306.

Nishnianidze, A. (2024). Surveillance in the Digital Age. European Scientific Journal, ESJ. https://doi.org/10.19044/esj.2024.v20n37p1.

Reis, O., Eneh, N., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. (2024). Privacy Law Challenges In The Digital Age: A Global Review Of Legislation And Enforcement. International Journal of Applied Research in Social Sciences. https://doi.org/10.51594/ijarss.v6i1.733.

Sethi, A., Ullah, H., & Naseem, R. (2025). Surveillance, National Security and the Right to Privacy in the Digital Era. The Critical Review of Social Sciences Studies. https://doi.org/10.59075/gf564d60

Svobodová, T. (2025). Recalibrating Liberty And Security: Human Rights Challenges In The Age Of Mass Surveillance. Congress Proceedings. https://doi.org/10.55843/icl2025cong117s.

Syahwami, S., & Hamirul, H. (2024). The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia. Enigma in Law. https://doi.org/10.61996/law.v2i2.56.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.3 . No.1, February 2026
DOI : https://doi.org/10.62872/1w6a2t71

Legal Documents

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, khususnya Pasal 28G ayat (1), Pasal 28F, dan Pasal 28J.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan.

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Peraturan perundang-undangan terkait keamanan siber dan perlindungan sistem elektronik.