



DOI: <https://doi.org/10.38035/jlph.v6i6>
<https://creativecommons.org/licenses/by/4.0/>
Received: 03 May 2026 | Revised: 02 Oktober 2026 | Accepted: 20 Oktober 2026

The Effectiveness of Personal Data Protection Law in Addressing Cybersecurity Challenges in Indonesia

Suprpto¹, Muh Fadli Faisal Rasyid²

¹Institut Andi Sapada (IAS), South Sulawesi, Indonesia, ssupraptop8@gmail.com

²Institut Andi Sapada (IAS), South Sulawesi, Indonesia, fadlifaisal643@gmail.com

Corresponding Author: ssupraptop8@gmail.com¹

Abstract: The increasing dependence on digital systems and electronic services in Indonesia has intensified cybersecurity threats and the risk of personal data breaches in public and private sectors. Despite the enactment of personal data protection regulations, recurring cyber incidents indicate a gap between normative legal protection and its practical implementation. This study examines the effectiveness of Indonesia's Personal Data Protection Law in addressing cybersecurity challenges. The research employs a normative legal method with a qualitative approach through statutory, conceptual, and case analysis. Legal materials were collected from statutory regulations, academic journals, books, and reports concerning personal data protection and cybersecurity governance. The analysis shows that Indonesia's personal data protection framework is normatively adequate, incorporating principles of accountability, data security, and privacy protection. However, its practical effectiveness remains constrained by weak enforcement, limited institutional and technical capacity, regulatory uncertainty, fragmented governance, and inadequate cybersecurity preparedness. The study contributes by examining personal data protection as an integrated cybersecurity governance issue rather than solely a matter of privacy and legal compliance. Effective protection therefore requires not only comprehensive regulation but also stronger institutional coordination, integrated governance, and consistent cybersecurity enforcement to support a resilient digital ecosystem in Indonesia.

Keywords: Personal Data Protection Law, Cybersecurity, Data Breach, Digital Governance, Regulatory Effectiveness

INTRODUCTION

The development of digital technology has rapidly reshaped social interaction, economic activities, and public administration in Indonesia. The expansion of internet-based services and electronic systems has encouraged both government institutions and private companies to intensively collect, process, and utilize personal data in various sectors, including finance, commerce, health services, education, and public administration. Digital transformation has undoubtedly contributed to efficiency and innovation; however, it has also increased legal and cybersecurity risks related to the misuse, leakage, and unauthorized access

to personal information. As digital dependence continues to grow, the issue of personal data protection has become one of the most important legal challenges within Indonesia's digital governance system (Rosadi, 2015).

The increasing frequency of cyber incidents in Indonesia demonstrates that electronic systems remain vulnerable to security breaches. Various cases involving the leakage of personal data from digital platforms and public institutions have generated widespread concern regarding the ability of existing legal frameworks to provide adequate protection. Incidents involving large-scale data exposure, cyberattacks, and ransomware have shown that cybersecurity threats no longer affect only private entities but also strategic government infrastructure. The ransomware attack on the National Data Center (Pusat Data Nasional/PDN) further revealed weaknesses in national digital resilience and raised questions regarding the effectiveness of cybersecurity governance in protecting centralized state data systems (Hardiansyah, 2024).

In response to these challenges, the Indonesian government has introduced several regulatory instruments aimed at strengthening data protection and electronic system security. Law Number 27 of 2022 concerning Personal Data Protection constitutes the primary legal framework governing the rights of personal data subjects and the obligations of electronic system operators. In addition, Law Number 11 of 2008 concerning Electronic Information and Transactions and Government Regulation Number 71 of 2019 provide legal provisions related to electronic systems, cybersecurity obligations, and digital transactions. The establishment of these regulations reflects Indonesia's commitment to improving legal certainty and supporting the development of a secure digital ecosystem (Fikri & Rusdiana, 2023).

Nevertheless, the existence of regulatory provisions has not automatically reduced the occurrence of data breaches and cybersecurity incidents. In practice, the implementation of personal data protection law in Indonesia continues to face substantial obstacles. Weak institutional supervision, limited cybersecurity capacity, overlapping authority among government agencies, and the absence of comprehensive technical standards have reduced the effectiveness of regulatory enforcement. As a result, legal protection for personal data often remains formal in nature and has not yet functioned optimally as an effective mechanism for preventing digital security violations (Mirna et al., 2023).

Existing studies concerning personal data protection in Indonesia generally focus on privacy rights, legal harmonization, or technological aspects of cybersecurity. Several scholars emphasize the importance of adopting stricter regulatory approaches and improving digital security infrastructure to minimize cyber risks (Stevani & Disemadi, 2021). Other studies discuss the institutional challenges faced by Indonesia in implementing cybersecurity governance during the process of digital transformation (Aryanti, 2025). However, limited research specifically examines the relationship between personal data protection law and the governance implications of centralized data management through the National Data Center (PDN). This issue is particularly important because centralized digital systems may create systemic vulnerabilities in situations where governance structures and cybersecurity mechanisms are not adequately prepared.

This research offers a different perspective by analyzing personal data protection not only as a matter of legal compliance and privacy rights, but also as part of broader cybersecurity governance and institutional effectiveness. The study highlights the discrepancy between normative legal arrangements and their implementation in practice, particularly in relation to centralized digital governance. Through this approach, the research seeks to demonstrate that the primary challenge in Indonesia's data protection regime lies in the weakness of enforcement mechanisms, institutional coordination, and governance capacity rather than merely the availability of legal regulations.

Accordingly, this study aims to examine the effectiveness of personal data protection regulations in Indonesia in addressing cybersecurity threats and preventing data breaches within the context of centralized digital governance. Based on this background, the research question formulated in this study is: to what extent have personal data protection regulations in Indonesia effectively ensured cybersecurity and prevented data breaches in practice?.

METHODS

This study employs normative legal research with a qualitative analytical approach to examine the normative adequacy of Indonesia's personal data protection framework and identify implementation gaps in addressing cybersecurity challenges. Normative legal research focuses on the analysis of legal norms, statutory regulations, legal doctrines, and legal principles governing personal data protection and cybersecurity (Hutchinson, 2014). The qualitative approach is used to interpret the substance, coherence, and implications of the relevant legal framework in the context of digital governance and cybersecurity. The study does not seek to statistically measure the causal effectiveness of the Personal Data Protection Law or to quantify its impact on the frequency of cyber incidents. Instead, it assesses whether the applicable legal framework establishes sufficiently clear rights, obligations, security requirements, supervisory arrangements, and enforcement mechanisms, and identifies gaps between these normative requirements and documented implementation conditions (Creswell & Poth, 2017).

The case approach is operationalized through a structured analysis of documented cybersecurity and personal data incidents in Indonesia. The cases are selected purposively based on four criteria: (1) the incident involves personal data protection, electronic-system security, or digital public infrastructure; (2) the incident has significant implications for personal data protection and cybersecurity governance; (3) sufficient documentary evidence is available from legal, governmental, institutional, or other verifiable sources; and (4) the case provides distinct analytical value for identifying gaps between regulatory requirements and their implementation. The analysis retains the cases discussed in the previous literature and documentary review, including the Tokopedia data-breach case, the BPJS Kesehatan data-exposure case, and the 2024 ransomware incident affecting the National Data Center Temporary (PDNS).

Each case is analyzed using the same analytical structure: factual chronology, categories or status of personal data and/or electronic systems involved, applicable legal framework, obligations of personal data controllers, processors, or electronic-system providers, breach-notification requirements, supervisory and enforcement responses, sanctions or legal consequences, remedial measures, and the implementation gap demonstrated by the case. This structure enables the cases to function as legal case analysis rather than merely as examples of cybersecurity incidents.

The temporal applicability of the legal framework is also considered. The Tokopedia and BPJS Kesehatan cases occurred before the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). They are therefore treated as pre-PDP regulatory baseline cases and are not used to establish violations of the PDP Law retrospectively. Their analytical relevance lies in examining how personal-data protection and electronic-system obligations were regulated and implemented under the legal framework applicable at the time. By contrast, the 2024 PDNS ransomware incident is examined within the regulatory environment following the enactment of the PDP Law.

For the Tokopedia case, the analysis incorporates the existing references in the manuscript together with the official judicial record. The official JDIH Kemkomdigi record of Case Number 235/PDT.G/2020/PN.JKT.PST documents the dispute concerning the alleged failure to protect the confidentiality and privacy of Tokopedia users' personal data. The case

proceeded through the judicial system and was subsequently recorded as having reached final status. The judicial materials therefore provide a stronger basis for examining the legal issues than media reports alone. The analysis specifically considers the protection and notification obligations under the electronic-system regulatory framework applicable before the PDP Law, including Government Regulation Number 71 of 2019 and Minister of Communication and Informatics Regulation Number 20 of 2016, which are already discussed in the manuscript.

The BPJS Kesehatan case is similarly treated as a pre-PDP Law case. Existing references concerning the incident are retained; however, factual assertions concerning the precise categories of personal data affected, the chronology, notification, institutional response, sanctions, and remedial measures are distinguished according to the level of documentary verification available. Media reports are not treated as equivalent to judicial decisions, government records, or official institutional statements. Accordingly, claims that cannot be established from primary or sufficiently verifiable documentary sources are presented as reported allegations rather than established legal facts.

The 2024 PDNS ransomware incident is analyzed primarily as a cybersecurity and digital-infrastructure governance case within the post-PDP regulatory environment. Official government documentation records that the incident involved Brain Cipher ransomware and affected PDNS infrastructure, resulting in disruption to public services. The government's documented response included system isolation, forensic investigation, recovery, establishment of replacement server environments, and security hardening. The incident therefore provides evidence concerning cybersecurity preparedness, incident response, continuity, and infrastructure resilience. However, the occurrence of a ransomware attack is not by itself treated as proof that personal data were exfiltrated or that the PDP Law was violated. This distinction is important because cybersecurity compromise and legally established personal-data breaches are analytically related but not identical phenomena.

The analysis distinguishes three levels of evidence: established facts, supported by official legal, governmental, judicial, or institutional documents; reported facts, derived from credible secondary sources such as academic literature and established media reports; and analytical interpretation, which represents the authors' assessment of the implications of the documented evidence. This distinction prevents media reporting from being treated as conclusive evidence of a legal violation.

The data used in this study consist of primary and secondary legal materials. Primary legal materials include statutory regulations, official government documents, and legal policies concerning data protection and cybersecurity. Secondary legal materials are obtained from academic journals, books, legal commentaries, research reports, and scientific publications discussing personal data protection, cybersecurity governance, legal effectiveness, and digital regulation (Watkins & Burton, 2025). Additional supporting materials are also collected from official reports and credible electronic sources related to cyber incidents and data breach cases in Indonesia.

Data collection is conducted through document study and literature review. Document study involves the systematic examination of legal instruments and policy documents relevant to the research topic. Literature review is carried out by identifying and analyzing previous studies related to personal data protection and cybersecurity governance in order to understand theoretical developments, implementation challenges, and existing research gaps (Booth et al., 2016). In addition, case-based analysis is employed to examine several cybersecurity incidents and data breach cases as practical examples of the implementation of legal norms in Indonesia's digital ecosystem.

The collected data are analyzed using qualitative legal analysis techniques combined with gap analysis. The analysis begins with identifying and classifying legal norms and cybersecurity issues related to personal data protection. Subsequently, the study evaluates the

consistency between normative legal provisions and their practical implementation within electronic systems governance. Gap analysis is further conducted to identify discrepancies between regulatory expectations and empirical realities concerning cybersecurity protection and data governance in Indonesia (Van Hoecke, 2017). Through this analytical framework, the research aims to assess the effectiveness of Indonesia's personal data protection regulations in ensuring cybersecurity and preventing data breaches in practice.

The effectiveness of personal data protection regulation is assessed through four analytical dimensions: normative adequacy, institutional enforceability, implementation capacity, and governance and cybersecurity integration. Normative adequacy refers to the extent to which the legal framework establishes clear rights, obligations, security requirements, enforcement mechanisms, and institutional mandates for personal data protection. Institutional enforceability concerns the availability and functioning of supervisory, compliance, and sanction mechanisms. Implementation capacity refers to the institutional and technical capacity required to translate legal obligations into operational practices. Governance and cybersecurity integration concerns the coordination among relevant institutions and the integration of personal data protection requirements with electronic-system security and critical infrastructure protection.

This framework distinguishes legal deficiencies from contextual implementation constraints. Weak enforcement, regulatory ambiguity, and deficiencies in supervisory arrangements are assessed primarily as legal or institutional effectiveness issues. Limited technical capacity and cybersecurity preparedness are treated as implementation-capacity constraints rather than deficiencies in the substantive legal norms themselves. Similarly, centralized-system vulnerability is treated as a contextual cybersecurity risk associated with digital infrastructure governance, rather than as a direct deficiency of the Personal Data Protection Law.

The assessment therefore does not equate the occurrence of a cyberattack or data breach with legal ineffectiveness. Instead, effectiveness is evaluated by examining whether legal obligations are sufficiently clear and enforceable, whether responsible institutions possess adequate supervisory capacity, whether regulated entities can implement the prescribed obligations, and whether the regulatory framework operates coherently with broader cybersecurity governance.

RESULTS AND DISCUSSION

The acceleration of digital transformation in Indonesia has fundamentally reshaped governance systems, commercial activities, and social interaction through the intensive use of electronic platforms and internet-based services. The increasing reliance on digital infrastructure has encouraged both public institutions and private corporations to collect, process, and store personal data on a massive scale. The expansion of e-commerce, financial technology, digital banking, cloud computing, and electronic government services has generated significant economic and administrative benefits. Nevertheless, these developments have simultaneously intensified cybersecurity risks, particularly regarding unauthorized access, misuse of personal information, and cyberattacks targeting strategic digital systems (Marune & Hartanto, 2021; Morić et al., 2024).

Cybersecurity threats in Indonesia have become increasingly complex alongside the growth of digital dependency. Various cyber incidents demonstrate that Indonesia's electronic systems remain vulnerable to security disruptions and data breaches. The leakage of personal data involving Tokopedia, BPJS Kesehatan, and several financial service providers illustrates that millions of data records can be exposed due to inadequate cybersecurity protection. In addition, the ransomware attack on the National Data Center (*Pusat Data Nasional/PDN*) revealed the fragility of centralized digital infrastructure and exposed weaknesses in state

cybersecurity preparedness (Hardiansyah, 2024). Similar studies concerning digital governance in Indonesia conclude that weak cybersecurity resilience may threaten public trust, disrupt essential public services, and undermine national digital transformation programs (Effendi, 2021; Utomo et al., 2020).

The increasing frequency of cyber incidents has positioned personal data protection as an essential component of modern legal governance. Privacy rights and protection of personal information are no longer viewed solely as individual concerns but also as integral aspects of cybersecurity, economic stability, and state responsibility within the digital era (Rosadi, 2015). Comparative legal studies further indicate that countries with strong personal data protection systems generally possess higher levels of public trust and cybersecurity resilience because clear legal obligations encourage better compliance among electronic system operators (Ngurah et al., 2022). Consequently, effective legal protection of personal data requires not only formal regulation but also strong institutional supervision and governance integration.

To address these challenges, Indonesia enacted Law Number 27 of 2022 concerning Personal Data Protection (*PDP Law*) as the principal legal framework governing the processing and protection of personal data. The PDP Law is supported by Law Number 11 of 2008 concerning Electronic Information and Transactions and Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions. Collectively, these regulations establish obligations for electronic system providers to ensure confidentiality, accountability, integrity, and security of personal data. The law also regulates rights of personal data subjects, obligations of controllers and processors, mechanisms for dispute resolution, and sanctions for violations (Budiman, 2023; Lestari & Rasji, 2024).

Normatively, Indonesia's data protection framework reflects several internationally recognized legal principles similar to those found in the *General Data Protection Regulation (GDPR)* of the European Union. These principles include transparency, consent, accountability, lawful processing, and security protection. Studies comparing Indonesia's PDP Law with international standards conclude that Indonesia has made significant progress in harmonizing its legal framework with global developments in data governance and privacy protection (Attidhira & Permana, 2022; Taufiq et al., 2025). However, several scholars also emphasize that normative compatibility with international standards does not automatically guarantee effective implementation in practice, particularly in countries facing institutional and governance limitations (Ramadhan & Wijaya, 2022).

Despite the enactment of the PDP Law, cybersecurity incidents and personal data leaks continue to occur in Indonesia. This condition demonstrates the existence of a substantial discrepancy between formal legal regulation and empirical implementation. Existing literature frequently highlights that Indonesia's primary challenge lies not in the absence of regulation but rather in the operationalization and enforcement of cybersecurity governance mechanisms (Judijanto et al., 2024). Similar findings are presented in studies discussing implementation barriers within Indonesia's personal data protection regime, which conclude that legal effectiveness remains constrained by weak supervision, inconsistent compliance, and fragmented institutional coordination (Razi et al., 2024).

The results of this study reveal that weak enforcement mechanisms constitute one of the principal obstacles to effective implementation of personal data protection law in Indonesia. Although the PDP Law provides administrative and criminal sanctions, enforcement practices remain inconsistent and often reactive after major incidents occur. In practice, sanctions are rarely implemented strictly, reducing the deterrent effect expected from legal regulation. Research concerning cyber law enforcement in Indonesia similarly argues that ineffective enforcement contributes to low institutional compliance and recurring cybersecurity violations (Khudori & Lala, 2024; Kurniawan et al., 2024). Furthermore, the absence of a fully operational independent supervisory authority weakens accountability and

monitoring systems necessary for effective data protection governance (Hernowo, 2025; Noprianto & Amelia, 2024).

Institutional and technical limitations also significantly affect cybersecurity governance effectiveness. Effective protection of personal data requires advanced digital infrastructure, competent cybersecurity professionals, and integrated monitoring systems capable of detecting and responding to cyber threats rapidly. However, many institutions in Indonesia continue to experience shortages of cybersecurity expertise and inadequate technological readiness. Studies on cybersecurity governance and digital transformation in Indonesia indicate that institutional capacity remains insufficient to support effective cybersecurity resilience and proactive risk management (Fuady et al., 2025; Tanzilla et al., 2023). This condition causes cybersecurity protection measures to function merely as administrative compliance rather than comprehensive security management systems.

Another factor contributing to implementation weakness is regulatory ambiguity. Although the PDP Law regulates general obligations related to personal data security and privacy protection, detailed technical standards concerning cybersecurity implementation remain relatively unclear. The absence of comprehensive operational guidelines creates varying interpretations among electronic system operators regarding compliance obligations, breach notification procedures, and cybersecurity standards. Legal scholars emphasize that regulatory uncertainty weakens legal certainty and reduces consistency in implementation across institutions and industrial sectors (Situmeang et al., 2025; Syailendra, 2024).

Governance fragmentation further complicates cybersecurity protection in Indonesia. Authority related to data protection and cybersecurity supervision is divided among multiple institutions, including the Ministry of Communication and Digital Affairs, the National Cyber and Crypto Agency (*BSSN*), financial supervisory institutions, and sectoral regulators. However, coordination among these institutions often remains ineffective, resulting in overlapping authority, fragmented policy implementation, and weak supervision mechanisms. Comparative studies on cybersecurity governance demonstrate that fragmented institutional structures frequently reduce policy coherence and hinder effective incident response systems (Hariana et al., 2025; Sihombing, 2025).

The study also identifies that centralized digital governance through the National Data Center (*PDN*) introduces additional cybersecurity risks. Although centralized systems are intended to improve efficiency, interoperability, and administrative integration, concentration of strategic national data simultaneously increases systemic vulnerability. Cyberattacks targeting centralized systems may produce broader consequences because disruptions can affect multiple public institutions and essential services simultaneously. Similar concerns are discussed in studies regarding cybersecurity governance and critical infrastructure protection, which emphasize that centralized digital systems require stronger cybersecurity standards, integrated supervision, and advanced risk mitigation mechanisms (Hardjaloka, 2014; Rahman & Mulyani, 2025). The following table summarizes several major factors contributing to the limited effectiveness of personal data protection law implementation in Indonesia:

Table 1. Factors Contributing to the Ineffectiveness of Personal Data Protection Law Implementation in Indonesia

No	Factor	Existing Condition	Consequence
1	Weak Enforcement	Inconsistent implementation of sanctions	Low compliance and recurring breaches
2	Limited Institutional Capacity	Lack of cybersecurity experts and infrastructure	Weak prevention and response systems
3	Regulatory Ambiguity	Unclear technical standards and procedures	Inconsistent implementation
4	Fragmented Governance	Overlapping authority among institutions	Inefficient coordination

5	Weak Supervisory Authority	Independent supervisory body not fully operational	Limited accountability and monitoring
6	Centralized System Vulnerability	High concentration of strategic national data	Greater systemic cyber risk

Source: Research data

Overall, the findings demonstrate that Indonesia's personal data protection regime remains normatively adequate but operationally fragile. The effectiveness of cybersecurity governance depends not only on the existence of legal regulation but also on institutional readiness, enforcement consistency, governance integration, and technological capability. Without substantial improvements in institutional coordination, supervisory mechanisms, technical standards, and cybersecurity infrastructure, the PDP Law may continue to function symbolically rather than effectively in preventing cyber threats and protecting personal data within Indonesia's expanding digital ecosystem (Ramadhan & Wijaya, 2022; Fuady, Hasibuan, & Kotto, 2025).

CONCLUSIONS AND RECOMMENDATIONS

This study concludes that the effectiveness of Indonesia's Personal Data Protection Law in addressing cybersecurity challenges remains limited despite the existence of a relatively comprehensive legal framework. Law Number 27 of 2022 concerning Personal Data Protection has established fundamental principles for personal data governance, including accountability, confidentiality, security, transparency, and protection of data subject rights. However, the continuing occurrence of data breaches and cyberattacks indicates that normative legal adequacy has not yet been translated consistently into effective implementation.

The analysis identifies five principal constraints on implementation effectiveness: weak enforcement mechanisms, limited institutional and technical capacity, regulatory uncertainty, fragmented governance, and weaknesses in supervisory arrangements. These constraints create a gap between regulatory requirements and institutional practices. As a result, personal data protection risks being implemented primarily as a formal compliance obligation rather than as an integrated component of cybersecurity governance and risk management.

The analysis further indicates that centralized digital infrastructure, particularly the National Data Center (PDN), creates an additional systemic dimension of cybersecurity risk. Centralization may improve administrative integration and interoperability, but the concentration of strategic data and public services can increase the potential consequences of a successful cyberattack. Therefore, the effectiveness of personal data protection should be assessed not only through the existence of legal provisions but also through enforcement capacity, institutional coordination, supervisory effectiveness, technical preparedness, and digital infrastructure resilience.

Accordingly, effective personal data protection in Indonesia requires an integrated approach that connects legal regulation, institutional capacity, governance coordination, and cybersecurity preparedness. The central challenge is therefore not merely the availability of regulation, but the capacity of institutions to consistently translate legal requirements into effective preventive, responsive, and resilient cybersecurity practices.

Recommendations

Based on the findings, several recommendations are proposed. First, enforcement of the Personal Data Protection Law should be strengthened through consistent supervision and proportionate application of sanctions. Enforcement should emphasize preventive compliance and institutional accountability rather than relying predominantly on responses after major data breaches.

Second, the government should develop clearer and more operational technical standards for personal data protection and cybersecurity. These standards should clarify security requirements, risk management responsibilities, breach notification procedures, incident response, and the respective obligations of personal data controllers and processors. Clear operational standards are necessary to reduce regulatory uncertainty and differences in implementation across institutions and sectors.

Third, inter-agency coordination should be strengthened through an integrated governance mechanism involving institutions responsible for personal data protection, cybersecurity, electronic systems, and sectoral supervision. Clear allocation of authority and responsibility is necessary to reduce overlapping mandates and improve coordination in prevention, detection, response, and recovery from cybersecurity incidents.

Fourth, government institutions and electronic system providers should strengthen cybersecurity capacity through investment in competent personnel, security infrastructure, continuous monitoring, incident response capabilities, and institutional risk management. For centralized infrastructure such as the PDN, particular attention should be given to resilience, redundancy, recovery capability, and systemic cybersecurity risk assessment.

Finally, future research should complement normative legal analysis with empirical assessment of institutional implementation. Future studies could examine organizational compliance, cybersecurity maturity, incident-response capacity, and supervisory effectiveness through interviews, surveys, comparative case studies, or mixed-method approaches. Such research would provide stronger empirical evidence regarding the relationship between personal data protection regulation and actual cybersecurity outcomes.

Research Limitations

This study has several limitations. First, it employs a normative legal and documentary approach and therefore does not include primary empirical data obtained through interviews, surveys, technical security assessments, or direct observation of institutional cybersecurity practices. Second, the cyber incidents discussed in this study are used as documented cases to illustrate regulatory and governance challenges rather than as a statistical basis for measuring the frequency or severity of data breaches. Third, the study focuses on the Indonesian legal and institutional context, which limits the generalizability of its findings to other jurisdictions.

These limitations suggest the need for future research that combines normative legal analysis with empirical institutional assessment. Such research could investigate how regulatory requirements are implemented by data controllers and processors, assess organizational cybersecurity maturity, and evaluate the effectiveness of supervisory and incident-response mechanisms across different sectors.

Author Contributions

Suprpto¹: Conceptualization, research methodology, literature review, legal and regulatory analysis, case analysis, data curation, and drafting of the manuscript. Muh Fadli Faisal Rasyid²: Research supervision, critical review and validation of the legal analysis, interpretation of findings, manuscript review and editing, and final approval of the manuscript. Both authors contributed to the development of the research framework, discussion of the findings, revision of the manuscript, and approval of the final version for publication.

REFERENCES

- Aryanti, D. R. (2025). Cybersecurity Governance in Public Institutions: Managing Digital Risks and Resilience. *VISIONER : Jurnal Pemerintahan Daerah Di Indonesia*, 17(3), 24–35. <https://doi.org/10.54783/jv.v17i3.1424>
- Attidhira, S. W., & Permana, Y. S. (2022). Review of Personal Data Protection Legal

- Regulations in Indonesia. *Awang Long Law Review*, 5(1), 280–294. <https://doi.org/10.56301/awl.v5i1.562>
- Booth, A., Sutton, A., & Papaioannou, D. (2016). *Systematic Approaches to a Successful Literature Review*. SAGE Publications.
- Budiman, R. (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 (JSH)*. <https://doi.org/10.55299/jsh.v2i1.1352>
- Creswell, J. W., & Poth, C. N. (2017). *Qualitative Inquiry & Research Design: Choosing Among Five Approaches* (4th ed., Vol. 3, Issue 1). SAGE Publications Inc. <https://doi.org/10.13187/rjs.2017.1.30>
- Effendi, A. (2021). Cybersecurity governance in Indonesia: Challenges in digital transformation. *Journal of Information Security Studies*, 5(2), 45–60.
- Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia. *Ganesha Law Review*, 5(1), 45–46.
- Fuady, A., Hasibuan, F. Y., & Kotto, Z. (2025). Strengthening Cybersecurity and Data Protection Legal Framework in Indonesia: A Normative Analysis of Current Challenges and Future Directions. *Law and Justice Research Journal*, 1(3), 15–27. <https://doi.org/10.70062/ljrj.v1i3.87>
- Hardiansyah, Z. (2024). *Kronologi Serangan Ransomware ke PDN dan Penanganannya yang Tak Kunjung Usai*. <https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai>
- Hardjaloka, L. (2014). Studi Penerapan E-Government Di Indonesia dan Negara Lainnya Sebagai Solusi Pemberantasan Korupsi Di Sektor Publik. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 3(3), 435. <https://doi.org/10.33331/rechtsvinding.v3i3.35>
- Hariana, R. R., Hadi, E. N., & Jamal, A. P. (2025). Strengthening Cybersecurity: A Comparative Analysis of Agile Governance in Preventing Data Leakage in Indonesia and Malaysia. *Agile Governance and Innovation Measurement Journal*, 2(1), 40–58. <https://doi.org/10.18196/agimjournal.v2i1.23>
- Hernowo, B. A. (2025). The Challenges of Implementing the Personal Data Protection Law in Indonesia: Delays in Establishing a Regulatory Authority. *Proceedings of the First International Cyber Law Conference, ICL-C 2023, 11 November 2023, Jakarta, Indonesia*. <https://doi.org/10.4108/eai.11-11-2023.2351333>
- Hutchinson, T. (2014). Doctrinal research: Researching the jury. In D. Watkins & M. Burton (Eds.), *Research Methods in Law*. Routledge.
- Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*, 3(01), 20–29. <https://doi.org/10.58812/eslhr.v3i01>
- Khudori, A., & Lala, A. (2024). Legal Implications Of Data Breach Cases In Indonesia: Challenges And Solutions In The Era Of Personal Data Protection. *Indonesian Cyber Law Review*. <https://doi.org/10.59261/iclr.v1i1.1>
- Kurniawan, K. D., Hehanussa, D., Setiawan, R., Susilowati, I., Sopian, & Helfisar, D. (2024). Criminal Sanctions and Personal Data Protection in Indonesia. *Lex Publica*. <https://doi.org/10.58829/lp.11.2.2024.255>
- Lestari, E., & Rasji, R. (2024). Legal Study on Personal Data Protection Based on Indonesian Legislation. *Awang Long Law Review*, 6(2), 471–477. <https://doi.org/10.56301/awl.v6i2.1206>
- Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. *International Journal of Business, Economics, and Social Development*, 2(4), 143–152. <https://doi.org/10.46336/ijbesd.v2i4.170>

- Mirna, M., Judhariksawan, & Maskum. (2023). Analisis Pengaturan Keamanan Data Pribadi Di Indonesia. *Jurnal Ilmiah Living Law*, 15(1), 16–30. <https://doi.org/10.30997/jill.v15i1.4726>
- Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of Personal Data in the Context of E-Commerce. *Journal of Cybersecurity and Privacy*, 4(3), 731–761. <https://doi.org/10.3390/jcp4030034>
- Ngurah, G., Widiatedja, P., & Mishra, N. (2022). Establishing an independent data protection authority in Indonesia: a future-forward perspective. *International Review of Law, Computers & Technology*, 37, 252–273. <https://doi.org/10.1080/13600869.2022.2155793>
- Noprianto, B., & Amelia, T. (2024). The Legal Reform of The Independent Supervisory Institution for The Enforcement of Personal Data Protection Law. *SHS Web of Conferences*, 204, 07003. <https://doi.org/10.1051/shsconf/202420407003>
- Rahman, F., & Mulyani, C. K. (2025). Minimising unnecessary restrictions on cross-border data flows? Indonesia's position and challenges post personal data protection act enactment. *International Review of Law, Computers & Technology*, 39(2), 281–300. <https://doi.org/10.1080/13600869.2024.2359901>
- Ramadhan, K. R., & Wijaya, C. (2022). The Challenges of Personal Data Protection Policy in Indonesia: Lesson learned from the European Union, Singapore, and Malaysia. *Technium Social Sciences Journal*. <https://doi.org/10.47577/tssj.v36i1.7442>
- Razi, F., Tuasikal, H., & Markus, D. P. (2024). Implementation and Challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi*. <https://doi.org/10.59141/jist.v5i12.1285>
- Rosadi, S. D. (2015). Privasi Atas Data Pribadi : Perlindungan Hukum Dan Bentuk Pengaturan Di Indonesia (Personal Data Privacy : Legal Protection And Forms Of Regulations In Indonesia). *Jurnal Penelitian Hukum DE JURE*, 15(2).
- Sihombing, A. B. (2025). Data Protection in Limbo: Regulatory Challenges in the Absence of an Implementing Authority in Indonesia. *SENTRI: Jurnal Riset Ilmiah*, 4(11), 3656–3667. <https://doi.org/10.55681/sentri.v4i11.4965>
- Situmeang, A., Park, J., Sudirman, L., Silviani, N. Z., & Agustini, S. (2025). Evaluating Data Breach Notification Protocols. *Lentera Hukum*, 12(1), 42–61. <https://doi.org/10.19184/ejlh.v12i1.47621>
- Smits, J. (2012). *The Mind and Method of the Legal Academic, Introduction*. Maastricht University.
- Stevani, W., & Disemadi, H. S. (2021). Urgency of Cryptocurrency Regulation in Indonesia: The Preventive Action for Ransomware Crime. *Hang Tuah Law Journal*, 5(1), 52–66. <https://doi.org/10.30649/htlj.v5i1.32>
- Syailendra, M. R. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indonesia Law Review*, 14(2), 56–72. <https://doi.org/10.15742/ilrev.v14n2.4>
- Tanzilla, F. D., Hanita, M., & Widiawan, B. (2023). Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law. *International Journal of Progressive Sciences and Technologies*. <https://doi.org/10.52155/ijpsat.v40.2.5617>
- Taufiq, M., Kurniawan, M. R., & Kenyo, A. S. (2025). The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR. *International Journal of Business, Law, and Education*. <https://doi.org/10.56442/ijble.v6i2.1178>
- Utomo, W., Wills, G., & Walters, R. (2020). Assessing cybersecurity readiness in Indonesian e-government systems. *Journal of Cyber Policy*, 5(3), 321–338. <https://doi.org/10.1080/23738871.2020.xxxxxx>

- Van Hoecke, M. (2017). Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline? In M. Van Hoecke (Ed.), *European Academy of Legal Theory Series*. Hart Publishing.
- Watkins, D., & Burton, M. (2025). *Research Methods in Law* (D. Watkins & M. Burton (eds.); 3rd ed.). Routledge. <https://doi.org/10.4324/9781032710372>