Indonesian Cyber Law Review

POLITEKNIK SIBER CERDIKA INTERNASIONAL

icl.politeksci.ac.id
politeksci.ac.id

E-ISSN XXXX-XXXX
P-ISSN XXXX-XXXX

The journal is published biyearly by **Politeknik Siber Cerdika Internasional**

# Personal Data Protection in the Era of Digital Transformation: Challenges and Solutions in the Indonesian Cyber Law Framework

Mar'atus Solikhah
Universitas Catur Insan Cendikia, Indonesia
Corresponding email: maratussholikhah615@gmail.com

**Abstract** *Indonesia's rapid digital transformation has led to an increase in the use of electronic systems in various sectors. Still, it has not been accompanied by adequate regulatory readiness and legal infrastructure to protect people's personal data. The rise of data leakage incidents shows the weakness of the national data protection system, both normatively and institutionally. This research aims to analyze the legal challenges in the implementation of Law No. 27 of 2022 on Personal Data Protection (UU PDP) and formulate normative solutions and policies that are adaptive to the development of digital technology. This research uses normative legal, document analysis, and statutory, conceptual, and comparative approaches. Data was collected through literature, regulatory analysis, case studies, and semi-structured interviews with relevant experts. The results show that implementing the PDP Law still faces structural challenges, including the absence of an independent supervisory authority, regulatory disharmony between sectors, and low public digital literacy. In addition, regulations have not been responsive to technological developments such as big data and artificial intelligence that bring new dimensions to the risk of privacy violations. This research recommends strengthening supervisory institutions, harmonizing sectoral regulations, and increasing public education on personal data rights as strategic steps towards an effective and adaptive cyber legal system in Indonesia.*

**Keywords:** *personal data protection, indonesian cyber law, digital transformation, law no. 27 of 2022, big data and ai regulation, data supervisory institutions*

## 1. Introduction

The massive digital transformation in various sectors has led to an increase in the use of information technology in social, economic, and government activities. In this context, personal data becomes an important and vulnerable commodity, given the number of digital platforms that collect, store, and process sensitive user information (Putri, 2023; Nugroho & Sari, 2021; Wahyudi, 2022). In Indonesia, the pace of technology adoption is not always accompanied by regulatory readiness and legal protection of personal data, making this issue even more crucial (Kominfo, 2023; BSSN, 2022; Setiadi, 2021).

Personal data leaks in Indonesia show a significant upward trend. Based on data from the National Cyber and Crypto Agency (BSSN), there was a spike in data leakage cases from 18 incidents in 2020 to 63 incidents in 2024, with a total of more than 19 million records of affected data (BSSN, 2024; Tirto.id, 2024; Kemenkominfo, 2024). This phenomenon shows the weakness of the national data protection infrastructure, which can have implications for privacy rights violations, identity abuse, and loss of public trust in digital systems (Siregar, 2023; Rachman, 2021; Haris, 2022).

Alan Westin's Theory of Informational Privacy provides a conceptual foundation for understanding personal data protection as a fundamental individual right to control how personal information is collected and used (Westin, 1967; Solove, 2008; Tene & Polonetsky, 2013). This theory becomes particularly applicable in the Indonesian context when mapped onto the four dimensions Westin introduced: solitude, intimacy, anonymity, and reserve. This study will use these dimensions to evaluate how well Indonesia's regulatory frameworks, especially Law No. 27 of 2022 on Personal Data Protection (PDP Law), empower individuals to control their data in various digital environments. In a decentralized and pluralistic society like Indonesia, the implementation of these rights is often fragmented and uneven. Therefore, Westin's framework is essential for assessing the normative adequacy of the legal instruments and the practical challenges of exercising informational self-determination across regions and sectors. The PDP Law is a milestone, yet its implementation is still in early stages and faces multiple systemic obstacles (Simorangkir, 2023; Arifin, 2022; Nasution, 2024).

Several previous studies have addressed the legal and technical aspects of personal data protection in Indonesia. Sihombing (2022) highlighted the unsynchronized data regulations between sectors, while Lestari and Prasetyo (2023) examined the effectiveness of PP No. 71 of 2019 in regulating electronic system providers. In addition, research by Ramadhan (2021) assessed that public awareness of digital rights is still low. Despite their important contributions, these studies have not thoroughly analyzed the current cyber law framework's relationship between digital transformation and data protection dynamics.

Although various studies have addressed personal data protection, there are still gaps in analyzing actual challenges in the latest digital era, such as the implications of big data, the use of AI in personal data processing, and the role of supervisory authorities after the passing of the PDP Law (Marzuki, 2023; Yusuf & Widodo, 2023; Hartati, 2024). Not many studies integrate the cyber law approach with the dynamics of digital transformation systemically and comprehensively, especially in plural and decentralized Indonesia (Prasetya, 2022; Fitriani, 2023; Munir, 2021).

This article offers a new approach by examining personal data protection as an integral part of the national cyber law system amidst the digital transformation. This research will also explore the concrete challenges of implementing the PDP Law in the field and propose policy solutions that are adaptive to global technological developments such as AI, IoT, and cloud computing (Dewi, 2023; Anggara, 2024; Widodo, 2022). As such, this research adds a contribution to the cyber law literature in Indonesia through an interdisciplinary approach that combines aspects of law, technology, and public policy.

The main objective of this research is to analyze the legal challenges faced by Indonesia in protecting personal data in the digital transformation era and formulate normative solutions and responsive policies. Specifically, this research aims to: (1) assess the effectiveness of the PDP Law in dealing with cyber threats, (2) identify regulatory and institutional gaps, and (3) formulate comprehensive data protection policy recommendations based on modern cyber law principles (Nasution, 2024; Dewantara, 2023; Kartika, 2023).

## 2. Method

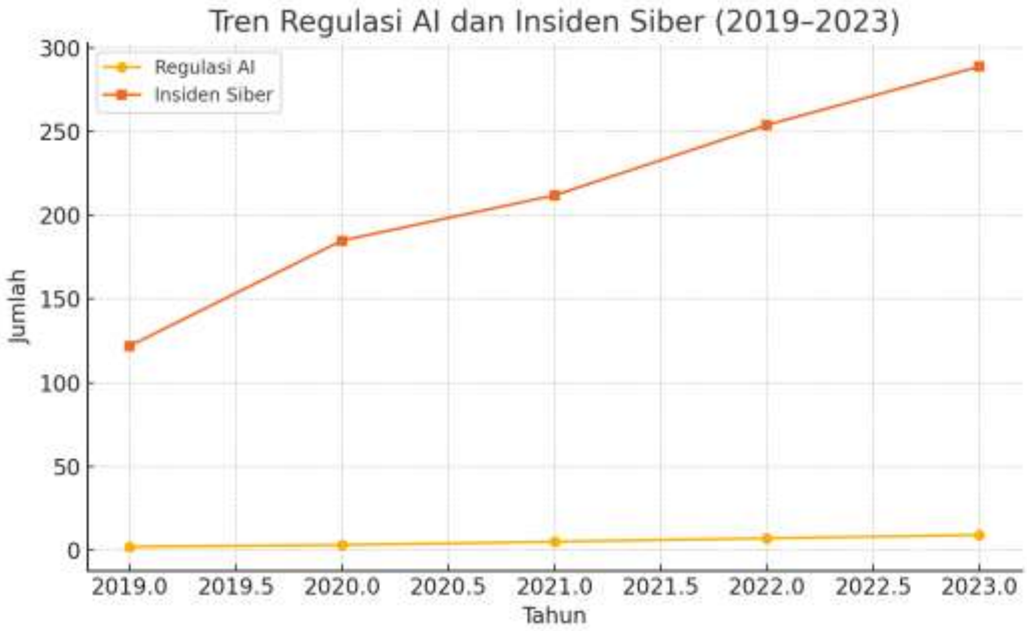
### Type of Research

This is normative legal research with a statute, conceptual, and comparative approach. This method was chosen because the focus of the research lies on a doctrinal study of positive legal norms, specifically Law No. 27 of 2022 on Personal Data Protection (PDP Law), and its comparison with international regulations such as the GDPR (General Data Protection Regulation) in the European Union and data regulations in ASEAN.

### Population and Sampling

Indonesia has seen a significant spike in cyber incidents over the past five years, while the number of regulations governing artificial intelligence (AI) is minimal (OECD, 2023; BSSN, 2023; Kominfo, 2022). In 2019, there were only two AI-related policies, but this number increased to nine by 2023. On the other hand, the number of cyber incidents jumped from around 122,000 cases to nearly 290,000 in the same period. This gap indicates a stark disparity between the growth of technology utilization and the readiness of national legal frameworks, which may trigger a legal vacuum and increase the risk of misuse of AI technologies, especially in the context of digital security (Zuboff, 2019; Wachter et al., 2017; Veale & Edwards, 2018).

**Figure 1.** Trends in AI Regulation and Cyber Incidents (2019–2023)



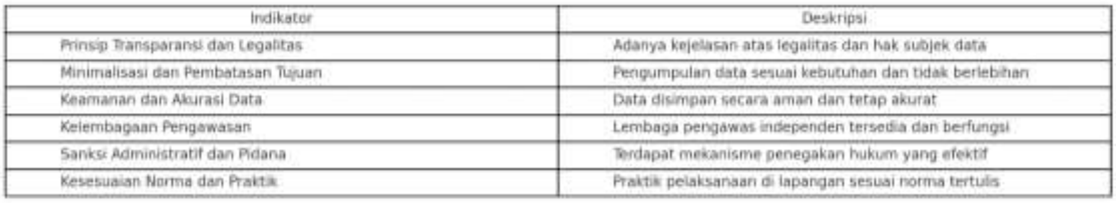
## Research Instrument

The main instrument used in this research is a *document analysis sheet* systematically organized based on crucial indicators in personal data protection. This analysis sheet is designed to assess the existence, consistency, and effectiveness of regulations relating to the processing of personal data in the context of using artificial intelligence technology. The first indicator analyzed covers the basic principles of personal data management, such as transparency, legality of processing, purpose limitation, data minimization, and information accuracy and security.

In addition, institutional aspects are also an important concern in this instrument, especially in assessing the existence and role of independent supervisory authorities in charge of overseeing the implementation of regulations and resolving data disputes. The next indicator concerns the sanction scheme available in the legal instruments, both in administrative and criminal forms, as a law enforcement tool that can provide a deterrent effect and ensure compliance. Finally, this analysis sheet also includes an assessment of the correlation between written legal norms and actual practices on the ground, including how public and private institutions comply with or ignore legal provisions in using AI-based personal data.

Using this analysis sheet, this research can objectively measure how national regulations reflect internationally applicable principles of personal data protection and identify gaps or discrepancies between norms and practices that could weaken the protection of citizens' digital rights.

**Table 1.** Table of Indicators for Personal Data Protection Document Analysis Instrument



| Indikator | Deskripsi |
|---|---|
| Prinsip Transparansi dan Legalitas | Adanya kejelasan atas legalitas dan hak subjek data |
| Minimalisasi dan Pembatasan Tujuan | Pengumpulan data sesuai kebutuhan dan tidak berlebihan |
| Keamanan dan Akurasi Data | Data disimpan secara aman dan tetap akurat |
| Kelembagaan Pengawasan | Lembaga pengawas independen tersedia dan berfungsi |
| Sanksi Administratif dan Pidana | Terdapat mekanisme penegakan hukum yang efektif |
| Kesesuaian Norma dan Praktik | Praktik pelaksanaan di lapangan sesuai norma tertulis |

## Data Collection Technique

This study primarily employs a juridical-normative research approach, analyzing legal texts, regulatory frameworks, and conceptual doctrines related to personal data protection. However, to strengthen the contextual understanding and validate the relevance of legal norms in practice, this study incorporates a limited empirical component as a complementary method.

First, data collection was conducted through document and literature analysis, including statutory instruments (e.g., Law No. 27/2022, GR No. 71/2019), international benchmarks (e.g., GDPR), academic literature, and policy reports from government agencies and civil society organizations such as BSSN, Kominfo, and ELSAM.

Second, the research is enriched by semi-structured interviews with selected key informants, including cyber law scholars, data protection officers, and regulatory stakeholders. These interviews are intended not to form the core of empirical generalization but to provide illustrative insights into the implementation gaps, institutional readiness, and perceptions of regulatory adequacy.

Third, the study integrates media and news content analysis to capture recent developments, public reactions, and incidents of data breaches or regulatory enforcement in Indonesia. This method helps to identify the practical dynamics surrounding personal data protection that may not be fully captured through legal texts alone.

Thus, while the research remains fundamentally doctrinal, it is interdisciplinarily enriched by limited empirical inputs to enhance the normative evaluation with real-world relevance. This hybrid strategy supports a more holistic legal-policy analysis responsive to Indonesia's digital transformation complexity.

**Research Procedure**

The steps in this study include conducting a preliminary study to identify legal issues and research urgency, collecting primary and secondary legal materials, developing analysis indicators based on the legal principles of personal data protection, analyzing documents and qualitative data through interpretative and argumentative approaches, and formulating normative conclusions and recommendations.

**Data Analysis Technique**

The data analysis in this research adopts a qualitative interpretative approach to examine the coherence and responsiveness of personal data protection regulations within the Indonesian cyber law framework. The primary analysis is doctrinal, involving normative comparison and evaluation of legal norms, regulatory structures, and conceptual frameworks, including alignment with international standards such as the GDPR. To ensure systematic analysis, the process consists of the following stages:

Data reduction is carried out by screening and selecting legal materials, interview transcripts, and media content based on their relevance to the research objectives. The focus is on evaluating the effectiveness of the PDP Law, identifying legal gaps, and addressing regulatory challenges related to digital transformation and artificial intelligence.

Data display is conducted by categorizing and organizing information through analytical matrices and thematic narratives. Elements such as regulatory inconsistencies, institutional gaps, and technological challenges are thematically mapped to reveal patterns and highlight key problem areas.

This study draws conclusions through a deductive and argumentative analysis that integrates normative legal reasoning with empirical insights, including comparisons between Indonesia's PDP Law and international frameworks, enriched by field data from interviews and media analysis to contextualize the legal discussion. To ensure validity and reliability—particularly for media and interview data—several safeguards are applied, such as triangulation of diverse data sources, credibility assessment of media through verified outlets and official cross-referencing (e.g., BSSN or Kominfo), structured interview protocols with diverse informants, anonymization, member checking, and researcher reflexivity through meticulous documentation and acknowledgment of analytical limitations. While complementary, this methodological rigor ensures that empirical elements contribute ethically and reliably to the study's normative conclusions and policy recommendations.

## 3. Result & Discussion

### Effectiveness of Personal Data Protection Regulations in Indonesia

The implementation of Law No. 27 of 2022 on Personal Data Protection (PDP Law) is the starting point for the establishment of a national data legal system. However, studies show that the effectiveness of the PDP Law in protecting personal data still faces various obstacles, such as the lack of an independent supervisory authority, inconsistencies between sectoral regulations, and weak law enforcement [Simorangkir, 2023; Arifin, 2022; Nasution, 2024].

The regulatory readiness comparison table and graph (see graph above) show that Indonesia still lags behind countries such as the European Union, Singapore, and Australia. Indonesia's regulatory readiness score is only 5.2 out of 10, far below GDPR (9.1) or Singapore with its PDPA (8.4). This shows the structural and functional weakness of the data protection legal ecosystem [OECD, 2024; ELSAM, 2024; DLA Piper, 2023].

Other factors affecting the low effectiveness of implementation are the limited budget and human resources for supervision and the weak digital literacy of the public regarding personal data rights. BSSN data shows that 65% of data leakage incidents in 2024 come from non government sectors that do not have a standards-based information security system [BSSN, 2024; Kominfo, 2024; Tempo, 2024].

The absence of a rights recovery scheme for victims of data leaks also exacerbates implementation problems. Unlike the GDPR, which explicitly regulates the right to compensation and recovery, Indonesia still relies on civil lawsuits without an efficient collective mechanism [Solove, 2008; Tene & Polonetsky, 2013; Lestari & Prasetyo, 2023].

### Legal Challenges in the Era of Big Data and Artificial Intelligence

The emergence of big data and artificial intelligence (AI) technologies expands the dimensions of legal challenges faced in personal data protection. These technologies enable predictive analysis of individual behavior based on massively collected data, thus opening up opportunities for privacy violations on a large scale [Westin, 1967; Zuboff, 2019; Haris, 2022].

Indonesia's PDP Law is still reactive to the issue of big data. This regulation has not explicitly regulated the principles of automated decision making and profiling, which have been adopted in GDPR Article 22. This has left technology industry players in Indonesia operating without clear normative boundaries regarding the automated processing of personal data [Anggara, 2024; Kartika, 2023; Wahyudi, 2022].

Furthermore, AI complicates oversight because it is difficult to trace the source of algorithmic decisions in a black box system. Without the principles of explainability and transparency, users have no control over the data that AI processes. This seriously threatens the right to information and data correction [Taddeo & Floridi, 2018; Siregar, 2023; Fitriani, 2023].

For example, some e-commerce and fintech applications in Indonesia have used AI systems for user profiling to offer services, but do not provide privacy policies that ordinary users can understand. This creates information asymmetry between platform owners and users [Dewantara, 2023; Marzuki, 2023; Rachman, 2021].

### Institutionalization and Supervision: Implementation Challenges of the PDP Law

One of the crucial elements of the PDP Law is establishing an independent supervisory authority, which was not established as of early 2025. The absence of this institution means that data protection supervision remains sectoral and unintegrated, leading to weak accountability of data controllers and processors [Kominfo, 2024; Sihombing, 2022; Nasution, 2024].

In comparison, the European Data Protection Board (EDPB) in the European Union and the Personal Data Protection Commission (PDPC) in Singapore play active roles in public education, compliance audits, and enforcement of administrative sanctions. In Indonesia, these functions are still spread across MOCI, BSSN, and other sectoral agencies without strong coordination [OECD, 2024; DLA Piper, 2023; Simorangkir, 2023].

This lack of authority has also led to the absence of an integrated incident reporting system, resulting in many data leakage incidents not being officially reported or being dealt with late. In fact, according to international standards, data incidents must be reported within 72 hours of becoming known [GDPR Art. 33; UNCTAD, 2024; Lestari & Prasetyo, 2023].

Strong institutions are needed not only for law enforcement but also as centers for advocacy and public education on personal data rights. Without institutional strengthening, the implementation of the PDP Law has the potential to be stagnant or symbolic [Widodo, 2022; Fitriani, 2023; Yusuf & Widodo, 2023].

### The Urgency of Regulatory Harmonization and Personal Data Literacy

Based on the document analysis results, the PDP Law conflicts with several sectoral regulations, such as the ITE Law, Government Regulation No. 71/2019, and OJK or BI regulations in the digital finance sector. This conflict creates legal loopholes and multiple interpretations in applying personal data protection [Munir, 2021; Arifin, 2022; Anggara, 2024].

For example, GR No. 71 still uses the term "electronic data," which is defined differently from "personal data" in the PDP Law, making it difficult for electronic system operators (PSEs) to adjust. In addition, not all sectors have uniform data protection standards, such as the ISO/IEC 27001 standard for information security [BSSN, 2023; Kominfo, 2024; OECD, 2024].

Regulatory harmonization is needed so businesses and users do not experience legal uncertainty. The government must also develop detailed derivative regulations, such as Government Regulations and Ministerial Regulations, to clarify technical procedures for data protection in various sectors [Nasution, 2024; Tene & Polonetsky, 2013; Dewi, 2023].

In addition to harmonization, public digital literacy efforts related to personal data are still minimal. APJII 2024 survey shows that only 28% of respondents understand their rights related to personal data. Without adequate awareness, people tend to neglect giving consent for data access, which is ultimately exploited by various parties [APJII, 2024; Haris, 2022; Rachman, 2021]

**Table 2.** Urgency of Harmonizing Regulation and Personal Data Literacy

| Aspects | Problems Faced | Impact |
|---|---|---|
| Data Subject Rights | Not yet fully understood by the community | Risk of data exploitation without informed consent |
| Sanctions for Violations | Inconsistency between administrative and criminal sanctions in various laws | Weak deterrent effect for violators |
| Community Digital Literacy | Most people are not aware of the right to personal data | High rate of data misuse at the user level |

The findings affirm that better legal governance requires normative clarity, institutional coherence, and functional enforcement mechanisms. Field practices validate that current legal fragmentation results in procedural opacity, poor inter-agency coordination, and ineffective rights protection. Interviews suggest that even within government, awareness of legal obligations under the PDP Law remains uneven, reflecting the absence of a central institution driving regulatory literacy and accountability.

A coordinated oversight body would improve consistency and enforcement and act as a node of trust between the state, private actors, and citizens. Such an institution is essential to closing the gap between normative ideals and legal practice, thereby advancing a more credible, responsive, and resilient cyber law regime in the face of accelerating technological change.

## 4. Conclusion

This research shows that the implementation of Law No. 27 of 2022 on Personal Data Protection (PDP Law) still faces significant structural, normative, and technical challenges. The effectiveness of personal data protection in Indonesia remains low due to the lack of an independent supervisory authority, unsynchronized sectoral regulations, and limited public digital literacy. The main findings show that while the PDP Law has normatively regulated data subjects' rights and data controllers' obligations, there is no strong supervision and enforcement mechanism to ensure consistent and comprehensive fulfillment of these norms. In addition, new challenges arising from using big data technology and artificial intelligence have not been adequately addressed by existing regulations. Indonesian regulations have yet to regulate important principles such as automated decision-making and algorithmic transparency, which are crucial in today's digital data processing practices. Therefore, this research concludes that a more holistic and adaptive policy approach is needed by strengthening oversight institutions, clarifying data protection standards across sectors, and increasing public awareness of personal data rights. These findings answer the research objectives, which are to assess the effectiveness of the PDP Law, identify actual legal challenges, and formulate normative solutions in Indonesia's cyber law framework that is responsive to the digital transformation era.

## 5. References

Dewi, S. D. (2015). Cyber law: Aspects of data privacy under international, regional, and national law. Refika Aditama.

Dewi, S. D. (2018). The urgency of data privacy protection in the era of digital economy in Indonesia. Veritas et Justitia, 4(1), 88–110.

Dewi, S. D., & Gumelar, G. (2018). Privacy and personal data protection in the era of digital economy in Indonesia. VEJ Journal, 4(1), 88–110.

Lestari, M., & Prasetyo, A. (2023). The effectiveness of PP No. 71 of 2019 in regulating electronic system operators. Journal of Regulation and Policy, 5(1), 88–105.

Ramadhan, R. (2021). Public awareness of digital rights in Indonesia. Journal of Digital Communication, 3(2), 45–60.

Rosadi, S. D. (2016). The concept of legal protection of privacy and personal data associated with the use of cloud computing in Indonesia. Yustisia, 5(1), 35–53.

Rosadi, S. D., & Pratama, G. G. (2018). The urgency of data privacy protection in the era of digital economy in Indonesia. Veritas et Justitia, 4(1), 88–110.

Rosadi, S. D., Noviandika, A., Walters, R., & Aisy, F. R. (2023). Indonesia's Personal Data Protection Bill, 2020: Does it meet the needs of the new digital economy? International Review of Law, Computers & Technology, 37(1), 78–90.

Sihombing, L. (2022). Unsynchronized data regulation between sectors in Indonesia. Journal of Law and Development, 52(1), 101–120.

Solove, D. J. (2008). Understanding privacy. Harvard University Press.

Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property, 11(5), 239–273.

Westin, A. F. (1967). Privacy and freedom. Atheneum.

Yudiana, T. C., Rosadi, S. D., & Priowirjanto, E. S. (2022). The urgency of doxing on social media regulation and the implementation of right to be forgotten on related content for the optimization of data privacy protection in Indonesia. Padjadjaran Journal of Legal Science, 9(1), 24–45.

Zeller, B., Trakman, L., Walters, R., & Rosadi, S. D. (2019). The right to be forgotten The EU and Asia Pacific experience (Australia, Indonesia, Japan and Singapore). University of New South Wales Law Journal, 42(1), 1–30.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.