JAMBURA LAW REVIEW
JALREV 8 (1) 2026 VOLUME 8 ISSUE 01
ISSN PRINT: 2654-9266
ISSN ONLINE: 2656-0461

Legal Protection for Personal Data Leaks and Its Implications for Citizens' Privacy Rights Within The Framework of The Indonesian Legal State

1st Uu Nurul Huda
2nd Tatang Astarudin
3rd Muhammad Irsan Nasution
4th Ahmad Abdul Khozin
5th Muhammad Irsan

[1,2,3,4]Sunan Gunung Djati State Islamic University Bandung, Indonesia.
[5] University of Melbourne, Australia.

✉ *Correspondence Email: uunurulhuda@uinsgd.ac.id*

Article Info

Submitted: *June 14, 2025*
Revised: December 8, 2025
Accepted: January 29, 2026

Keywords:
Data Breach; Legal Protection; Protection Privacy.

How to cite *[Chicago Manual of Style 17th edition (full note)]*: Uu Nurul Huda, Tatang Astarudin, Muhammad Irsan Nasution, Ahmad Abdul Khozin, Muhammad Irsan. "Legal Protection for Personal Data Leaks and Its Implications for Citizens' Privacy Rights Within The Framework of The Indonesian Legal State" *Jambura Law Review* 8, no. 1 (2026): 144–159.

Abstract

This study aims to examine the problem of personal data leakage in Indonesia, with a focus on the factors causing the leakage, its impact on citizens' privacy rights, and legal protection measures taken by authorized institutions and electronic system organizers (ESE) within the framework of the Indonesian rule of law. This study uses a qualitative descriptive-analytical approach, combining empirical data from field interviews with legal analysis. Key stakeholders from government institutions responsible for the management and protection of personal data were interviewed, and existing regulations, such as the Personal Data Protection Law and Permendagri No. 17/2020, were analyzed to understand the effectiveness of existing legal protection. Research findings show that data breaches in Indonesia are caused by inadequate data security infrastructure, limited expertise at the local level, and inconsistent implementation of national regulations. Although regulatory frameworks such as ISO 27001 certification are in place, a lack of resources and training in local governments hampers effective data protection. Coordination between central and local governments is essential, but faces challenges in ensuring uniform data management practices and protecting personal data from external threats.

@2026 – Uu Nurul Huda, Tatang Astarudin, Muhammad Irsan Nasution, Ahmad Abdul Khozin, Muhammad Irsan.
Under the license CC BY-SA 4.

Introduction

In the era of globalization and rapid advancements in information technology.[1] The protection of personal data has become increasingly critical. In this context, the present study aims to contribute to strengthening legal protections against personal data breaches and their implications for citizens' privacy rights, particularly within the framework of a rule-of-law state.[2]

Despite efforts to legislate personal data protection in Indonesia, data breaches remain a significant threat. Addressing this issue requires a thorough understanding of the current legal framework and improvements in its enforcement to ensure the security and integrity of personal data[3].

In recent years, persistent allegations of personal data breaches have raised concerns about public trust in the use of information technology in Indonesia. The Ministry of Communication and Information Technology, the National Cyber and Crypto Agency, and the Directorate General of Civil Registration (DUKCAPIL) [4], part of the Ministry of Home Affairs, have been called upon to investigate alleged data breaches. For instance, in 2023, the personal data of 34,900,867 Indonesian passport holders was reportedly leaked [5]. Similarly, the National Identification Number (NIK) data of 337 million citizens, managed by the Directorate General of DUKCAPIL under the Ministry of Home Affairs, was also compromised [6].

Additionally, further allegations of data breaches have emerged, such as an account named "Jimbo" offering to sell 252 million voter records for the 2024 elections, allegedly sourced from the General Elections Commission (KPU) website, on the online forum BreachForum [7]. The account shared 500,000 records as a sample and posted screenshots

---

[1] Alla S. Ivanova et al., "The Strategic Management in Terms of an Enterprise's Technological Development," *Journal of Competitiveness* 11, no. 4 (2019): 40–56, https://doi.org/10.7441/joc.2019.04.03.

[2] Anjar Sri Ciptorukmi and Adalia Safira Rahma, "Urgensi Pembentukan Pengadilan Keluarga: Refleksi Perlindungan Hak Anak Dalam Kasus Perceraian Di Indonesia," *LITIGASI* 25, no. 2 (2024): 130–49, https://doi.org/10.23969/litigasi.v25i2.18009; Miftahus Sholehudin et al., "Cancellation of Marriage Due to Apostasy in Islamic Law and Human Rights: A Comparative Analysis of Indonesia and Malaysia," *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 1 (2025): 33–51, https://doi.org/10.18860/j-fsh.v17i1.31465; Musa Taklima et al., "Consumer Protection as an Instrument for Fulfilling Human Rights in the Economic Sector and Its Constitutionalizing Efforts in the 1945 Constitution," *JURISDICTIE* 14, no. 1 (2023): 75–105, https://doi.org/10.18860/j.v14i1.20844.

[3] Akhmad Satori and Subhan Agung, "Personal Data Protecion in Indonesia: Legal Perspective," *International Journal of Multicultural and Multireligious Understanding* 7, no. 7 (2020): 183–89, http://dx.doi.org/10.18415/ijmmu.v7i7.177.

[4] Jonathan Brilliannata et al., "Protection of Personal Data as Confidential Information in Criminal Proceedings," *Legal Brief* 11, no. 4 (2022): 2263–67, https://doi.org/10.47643/1815-1329_2022_6_125.

[5] Biro Humas Kementerian Kominfo, "Siaran Pers No. 132/HM/KOMINFO/07/2023 Tentang Kominfo Telusuri Dugaan Kebocoran Data Paspor 34 Juta Warga Indonesia," Kominfo, 2023, https://www.kominfo.go.id/berita/siaran-pers/detail/siaran-pers-no-132-hm-kominfo-07-2023-tentang-kominfo-telusuri-dugaan-kebocoran-data-paspor-34-juta-warga-indonesia.

[6] BBC News Indonesia, "Ratusan Juta Data Dukcapil Kemendagri Diduga Bocor, Pakar Siber: 'Ini Peretasan Paling Parah,'" BBC News Indonesia, 2023, https://www.bbc.com/indonesia/articles/c51v25916zlo.

[7] Launa et al., "Tendensi Politik Kejahatan Dunia Maya," *JIKA (Jurnal Ilmu Komunikasi Andalan)* 7, no. 1 (2024): 26–51, https://doi.org/10.31949/jika.v7i1.8762.

from https://cekdptonline.kpu.go.id/ to verify the authenticity of the data. The asking price for the database was 74,000 USD, equivalent to 1.1 billion rupiah [8].

Moreover, the impact of personal data breaches on citizens' privacy rights must be thoroughly examined and analyzed [9]. The potential misuse of personal data and threats to private life [10] could erode public trust in the Indonesian legal system. Therefore, this research seeks to strengthen legal protections against personal data breaches and understand their implications for citizens' privacy rights within the framework of Indonesia's legal system.

Problem Statement

Despite Indonesia's efforts to legislate the protection of personal data, data breaches continue to occur frequently, highlighting significant weaknesses in the enforcement and oversight of digital information security. High-profile incidents—such as the leak of passport data belonging to 34.9 million individuals, the exposure of 337 million national identification numbers (NIK), and the alleged sale of 252 million voter records—demonstrate the inadequacy of the current legal framework in safeguarding citizens' privacy rights in the digital age. These breaches not only jeopardize individual privacy but also risk eroding public trust in the rule of law and the credibility of state institutions. Consequently, there is an urgent need for a comprehensive analysis to strengthen legal protections against personal data breaches and to examine their implications for citizens' privacy rights within the context of Indonesia's legal system.

Methods

This study employs a descriptive-analytical method with a juridical-empirical approach to explore legal protection against personal data breaches and their implications for citizens' privacy rights within the framework of the Indonesian legal system. The descriptive-analytical method aims to provide a comprehensive overview of the phenomenon of personal data breaches in Indonesia and analyze it in light of the applicable legal framework. The juridical-empirical approach focuses on understanding how personal data protection laws are implemented in practice and how legal norms function within society.

To grasp the complexity of this issue, the study utilizes several complementary approaches. A legal approach is adopted to examine the laws and regulations governing personal data protection in Indonesia, including Law No. 27 of 2022 on Personal Data Protection, as well as other relevant regulations. This analysis will assess how current

[8] Sintya Dewi Rahma et al., "Analysis of the Indonesian Government ' S Efforts in Overcoming Public Data Leak Cases," *Proceeding: The Sunan Ampel International Conference of Political and Social Sciences (SAICoPSS),* 1 (2023): 254–66, https://doi.org/10.15642/saicopss.2023.1..254-266.
[9] Jacob Leon Kröger et al., *How Data Can Be Used Against People: A Classification of Personal Data Misuses*, 2021.
[10] Judy Watson et al., "Understanding the Effects of Compromise and Misuse of Personal Details on Older People," *Australasian Journal of Information Systems* 23 (2019): 1–29, https://doi.org/10.3127/ajis.v23i0.1721.

legal norms protect individuals from data breaches and evaluate whether these regulations are sufficiently effective in safeguarding citizens' privacy rights.

An empirical approach is applied by collecting field data to observe how these regulations are implemented by law enforcement agencies and relevant parties. The research involves in-depth interviews with various stakeholders, including officials from the Ministry of Communication and Information, non-governmental organizations working in digital rights, and companies managing personal data. This primary data is expected to provide insights into the challenges encountered in enforcing the law and public perceptions regarding personal data protection.

Additionally, a conceptual approach is utilized to examine foundational concepts such as privacy, data security, and the right to information, which form the theoretical basis for personal data protection. This approach will explain the importance of personal data protection in the context of human rights and how it is regulated within the Indonesian legal system. A case study approach is also employed, analyzing several instances of personal data breaches in Indonesia. This case analysis will help identify patterns, challenges, and best practices in addressing data breaches, and evaluate whether law enforcement aligns with principles of justice and the protection of individual rights.

The data used in this study consists of primary data obtained through in-depth interviews, as well as secondary data, including legal materials such as laws, government regulations, scientific journals, articles, and books relevant to the research topic. Additionally, tertiary data is utilized, such as legal encyclopedias, legal dictionaries, and other supporting materials to enrich the analysis. Data collection techniques include interviews with key informants to gain a deeper understanding of the issues surrounding the implementation of personal data protection laws, documentation studies involving the review of legal documents, official reports, and court decisions related to personal data protection, as well as literature studies to explore relevant theories and concepts and understand the international context of personal data protection.

Data analysis is conducted qualitatively with a legal approach. The analysis involves identifying relevant legal themes, evaluating the consistency of legal application, and interpreting the findings in the context of legal theory and principles of justice. This analysis focuses on three key aspects: the positive aspect, which refers to the alignment with existing legal norms; coherence, which examines the relationship between legal norms and practices in the field; and justice, which assesses the impact of law enforcement on the protection of individual rights. By using this method, the study aims to make a significant contribution to understanding the effectiveness of legal protection against personal data breaches in Indonesia and their implications for citizens' privacy rights within the legal framework.

1. Data Leaks Problem In Indonesia

The use of digital technology in Indonesia has been on the rise, both among the general public and institutions. According to data from the Ministry of Communication and Informatics (KOMINFO), the Indonesian Digital Society Index (IMDI) in 2022 scored 37.8 out of 100, based on four key pillars: Infrastructure and Ecosystem, Digital Skills, Empowerment, and Employment.[11] This indicates that while progress has been made, improvement is still needed, especially in empowering the digital society. Additionally, telecommunications statistics report that in 2022, around 66.48% of Indonesia's population accessed the Internet, and 67.88% owned a mobile phone. These figures demonstrate an increase from the previous year and reflect the growing acceptance of digital technology by the public.[12]

By 2024, an internet penetration survey released by the Indonesian Internet Service Providers Association (APJII) revealed that 221.6 million Indonesians, or about 79.5% of the total population of 278.7 million, had access to the Internet. This represents a 1.4% increase from the previous year. Since 2018, Indonesia's internet penetration has grown from 64.8% to 73.7% in 2020, 77.01% in 2022, and 78.19% in 2023. The majority of these internet users belong to Generation Z and millennials, who account for more than 60% of all internet users in the country.[13]

While the increasing use of digital technology in Indonesia brings many benefits, it also heightens the risk of personal data leaks. With more digital activities, more personal data, such as identity information, transaction histories, and health records, is stored online.[14] Low digital literacy further exacerbates this issue, as many users are unaware of the risks involved in sharing information online. For instance, weak passwords or ignoring privacy policies of digital services are common practices.[15]

The issue of personal data protection in Indonesia has become a significant concern, particularly after several large-scale data leaks involving government agencies and private sector organizations.[16] Notable incidents include the leak of 6.8 million voter

[11] Kominfo, "Indeks Masyarakat Digital Indonesia (IMDI) Tahun 2022-2023," Kominfo, 2024, https://data.kominfo.go.id/opendata/dataset/indeks-masyarakat-digital-indonesia-imdi.
[12] Badan Pusat Statistik (BPS), "Statistik Telekomunikasi Indonesia 2022," Badan Pusat Statistik (BPS), 2023, https://www.bps.go.id/id/publication/2023/08/31/131385d0253c6aae7c7a59fa/statistik-telekomunikasi-indonesia-2022.html.
[13] APJII, "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," APJII, 2024, https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.
[14] Sumartini Dewi and Sri Wulandari, *Corporate Criminal Liability Telecommunication Company Against Consumer Personal Information Data Leakage in Indonesia* (Atlantis Press SARL, 2023), https://doi.org/10.2991/978-2-38476-024-4_23.
[15] Diana Setiawati et al., "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (2020): 95–109, https://doi.org/10.18196/iclr.2219.
[16] Setiawati et al., "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore."

records from the 2017 Jakarta gubernatorial election, which contained sensitive information such as Family Card Numbers, National Identity Numbers, and personal details. Another infamous case involved the hacker "Bjorka," who leaked 34 million Indonesian passports and 18.5 million BPJS Ketenagakerjaan participant records. Bjorka was also suspected of leaking data from 1.3 billion SIM cards in 2022.[17]

In 2024, another significant data leak was attributed to an unidentified individual known as "Jimbo," who reportedly leaked 252,327,304 records and sold the database for $74,000, equivalent to 2 bitcoins. This dataset contained personally identifiable information (PII), including passport details.[18] Additionally, in September 2024, a tax data leak affected 6 million citizens, including President Joko Widodo and his ministers. The social media platform X reported that the data, consisting of tax identification numbers, was sold on the "BreachForums" site for Rp. 150,000,000.00 (RM 41,565 or US $10,000).[19]

These incidents reveal significant weaknesses in Indonesia's cybersecurity policies, ranging from insufficient regulations to inadequate information technology infrastructure within many institutions, both governmental and private.[20] The lack of public awareness and understanding of the importance of personal data protection worsens the situation, with many citizens unaware of the risks of data leaks. Additionally, there is limited oversight and law enforcement in addressing violations related to data protection.[21] Repeated data breaches without strict sanctions against responsible parties have led to a growing distrust in the government's ability to safeguard citizens' data.[22]

The ongoing data breaches in Indonesia highlight the country's struggle to protect its citizens' privacy rights in the digital age.[23] A comprehensive approach is needed to address these challenges, including strengthening technology systems and improving human resource capacity. Although there have been no major internal data leaks, the potential for external breaches, such as those involving service providers, remains high due to weak security systems.[24] While ISO 27001 certification, the international standard

---

[17] Agus Ahadi Deradjat et al., "Data Protection & Privacy 2024," Chamber and Partners, 2024, https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2024/indonesia/trends-and-developments.

[18] Resecurity, "Vast Voter Data Leaks Cast Shadow Over Indonesia's 2024 Presidential Election Cyber Threat Intelligence," Resecurity, 2024, https://www.resecurity.com/blog/article/vast-voter-data-leaks-cast-shadow-over-indonesias-2024-presidential-election.

[19] Chandra Asmara, "Indonesia Probes Alleged Hack of Jokowi, Six Million Taxpayers," The Star, 2024, https://www.thestar.com.my/tech/tech-news/2024/09/19/indonesia-probes-alleged-hack-of-jokowi-six-million-taxpayers.

[20] Muhammad Firdaus, *A Review of Personal Data Protection Law in Indonesia*, no. 1 (2020): 1–7.

[21] E. Rosmaini et al., "Study to the Current Protection of Personal Data in the Educational Sector in Indonesia," *Journal of Physics: Conference Series* 978, no. 1 (2018): 1–7, https://doi.org/10.1088/1742-6596/978/1/012037.

[22] Yovita Arie Mangesti et al., "Ethico-Legal Aspects Of Personal Data Protection In Indonesia," *International Journal of Educational Research & Social Sciences* 2, no. 5 (2021): 1030–37.

[23] Charisma Septi and Jayanti Suraji, "The Issues of Data Protection Against Leaking of Personal Data in Social Security Health Services (a Comparison Between Indonesia and Other Countries Regulations)," *International Journal of Business, Economics and Law* 26, no. 1 (2022): 103–6.

[24] Muh Akbar et al., "Personal Data Leaks Ahead of 2024 Elections : Threats to Integrity and Public Trust," *Jurnal Litigasi Amsir* 7, no. 2023 (2024): 103–8.

for information security, has been introduced,[25] its implementation has been hindered by cost and infrastructure limitations. This illustrates the structural challenges faced by many regions in Indonesia, where security standards set by the central government have not been uniformly adopted.

As a nation governed by the rule of law, Indonesia has a clear obligation to protect its citizens' fundamental rights, including the right to privacy, as guaranteed by the constitution.[26] Article 28G of the 1945 Constitution acknowledges the right to personal and family protection, providing a constitutional basis for safeguarding personal data.[27] The Personal Data Protection Law (PDP Law), enacted in 2022, offers a strong legal framework for protecting personal data in the digital era. This law responds to the rapid development of technology and the increased use of the internet, which poses significant privacy risks, especially in data-driven sectors.

However, despite the passage of the PDP Law, its implementation faces several significant challenges. One of the primary issues is the digital infrastructure gap between urban and rural areas. In many rural regions, limited technological infrastructure hampers the effective implementation of data protection measures. Consequently, there is an imbalance in data management, with more developed areas having better systems while less developed regions remain vulnerable to data breaches. Furthermore, local officials often lack the necessary knowledge and training on secure digital data governance, contributing to weak data protection practices at the regional level. The lack of coordination between central and regional governments in enforcing regulations complicates the development of a cohesive national system.

2. Factors Causing Data Leaks And Its Implications On Citizens Privacy Rights

Data leaks in Indonesia stem from various complex and interrelated factors, including negligence in data management and weak information technology security systems across both government and private sectors. One of the most prominent causes is the lack of strict and consistent security standards. At the government level, both central and regional, there is often insufficient awareness and understanding of the importance of protecting personal and sensitive data.[28] Many agencies have not prioritized budget and human resources for managing secure information technology infrastructure, increasing the risk of data leaks.

Existing security systems frequently fail to keep pace with the latest technological advancements, making them vulnerable to cyberattacks, such as malware, ransomware,

[25] Robertus Nanda Christiadi and Rudi Sutomo, "Measurement of IT Security Governance Capabilities Using COBIT 2019 at Indonesian Business Sector," *G-Tech: Jurnal Teknologi Terapan* 7, no. 4 (2023): 1498–508, https://doi.org/10.33379/gtech.v7i4.3170.
[26] Sinta Rosadi, "Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia," *Brawijaya Law Journal* 5, no. 2 (2018): 143–57, https://doi.org/10.21776/ub.blj.2018.005.01.09.
[27] Septi and Suraji, "The Issues of Data Protection Against Leaking of Personal Data in Social Security Health Services (a Comparison Between Indonesia and Other Countries Regulations)."
[28] Andrew Shandy Utama et al., *Problematika Penegakan Hukum* (INSAN CENDEKIA MANDIRI, 2021).

and data theft through phishing.[29] For instance, many government information technology systems still rely on outdated software that no longer receives security updates, leaving gaps that can be exploited. Moreover, many institutions do not implement sufficient encryption to protect critical data.

Human error also plays a significant role in data breaches in Indonesia. Some breaches occur due to employee carelessness, such as using weak passwords, accessing public networks for important work, or sharing sensitive information through unsecured communication channels.[30] The lack of awareness and training on data security further exacerbates the situation.

Similar issues exist in the private sector. Many companies fail to comply with data protection regulations, such as the newly enacted Personal Data Protection Act (UU PDP). Companies often prioritize business profits over the security of customer data, leading to breaches of consumers' personal information, such as phone numbers, addresses, and financial details, which fall into the hands of irresponsible third parties.

The problem of data leaks in Indonesian government institutions is growing increasingly complex and urgent. Government-managed data includes sensitive information, such as population data, financial records, and other strategic information critical to national security. The challenge is exacerbated by outdated and poorly integrated security systems,[31] Many government agencies, especially at the regional level, continue to use outdated technology that no longer receives security updates, rendering them vulnerable to cyberattacks.[32] Additionally, a lack of strict security standards, particularly in terms of data encryption and access control, further contributes to the problem. Low employee awareness of data security practices, such as using weak passwords and sharing account access, is also prevalent.

Budget constraints significantly hinder efforts to maintain robust data security within government institutions. Limited budgets tend to prioritize essential public services over enhancing cybersecurity infrastructure, leaving many agencies without the necessary security technologies. Although regulations like the Personal Data Protection Law (UU PDP) exist, their enforcement is weak, resulting in a lack of consequences for institutions that fail to protect data, fostering a culture of indifference.

The threat of cyberattacks on government agencies continues to rise, as these institutions are often targeted by hackers seeking high-value data.[33] Unfortunately, many agencies

[29] Chih-Chieh Chiu et al., "Using an Efficient Detection Method to Prevent Personal Data Leakage for Web-Based Smart City Platforms," *Wireless Communications and Mobile Computing* 2023 (2023): 1–10, https://doi.org/10.1155/2023/5303329.
[30] Yudo Arhuma Binardy, "Legal Protection Arrangements in Indonesia for Privacy Rights in Cases of Personal Data Leakage," *International Journal of Social Science and Human Research* 04, no. 12 (2021): 3870–74, https://doi.org/10.47191/ijsshr/v4-i12-56.
[31] Akbari Amarul Zaman et al., "Pertanggung Jawaban Pidana Kebocoran Data Bpjs Dalam Perspektif Uu Ite," *De Juncto Delicti: Journal of Law* 1, no. 2 (2021): 146–57, https://doi.org/10.35706/djd.v1i2.5732.
[32] Nelson Novaes Neto et al., "Developing a Global Data Breach Database and the Challenges Encountered," *Journal of Data and Information Quality* 13, no. 1 (2021): 1–33, https://doi.org/10.1145/3439873.
[33] Yitong Ji et al., "A Critical Study on Data Leakage in Recommender System Offline Evaluation," *ACM Transactions on Information Systems* 41, no. 3 (2023), https://doi.org/10.1145/3569930.

lack effective mitigation or response strategies to handle these threats. The situation is worsened by the absence of cooperation between government agencies, where some may have adequate security systems while others remain highly vulnerable. Moreover, implementing government digitalization programs, such as e-government, faces significant security challenges. Many of these new systems are developed without sufficient consideration of security, leading to vulnerabilities that can result in data leaks.[34]

A real-life example highlighting the urgency of this issue can be seen in West Nusa Tenggara (NTB), where many local government institutions do not meet international standards for information security management, such as ISO 27001 certification. ISO 27001 is a global standard specifying requirements for an information security management system aimed at safeguarding data confidentiality, integrity, and availability. Without this certification, institutions in NTB are highly vulnerable to significant risks, including data leaks caused by weak information security systems.

In NTB, government agencies, from population services to public service sectors, often rely on outdated or insufficiently secured information technology systems. This situation is further worsened by the lack of attention to comprehensive data security management. These institutions are uncertified under ISO 27001 and fail to implement basic practices outlined in the standard, such as security risk management, access control to sensitive information, and regular monitoring and evaluation of potential cyber threats. This lack of standards makes these systems vulnerable to cyberattacks, both domestic and international, leading to large-scale data breaches.

In some cases, efforts to improve data security are hindered by budget constraints, as local governments prioritize physical infrastructure projects over strengthening information technology security systems. Beyond financial limitations, a shortage of qualified cybersecurity professionals also aggravates the situation. In NTB, for instance, many government employees responsible for data management lack specialized training in information security. As a result, human errors such as using weak passwords, sharing account access, and mishandling of sensitive data are widespread. Additionally, these institutions often do not have clear policies limiting access to authorized personnel only.

The absence of ISO 27001 certification and proper security practices creates vulnerabilities that external actors can exploit. In an era of increasingly sophisticated cyberattacks, local governments in NTB face significant threats from hackers who can exploit system weaknesses to steal or corrupt data.

The leakage of personal data directly threatens the core principles of the rule of law, particularly protecting citizens' privacy rights.[35] In a state governed by the rule of law,

[34] Neto et al., "Developing a Global Data Breach Database and the Challenges Encountered."
[35] Yenny Eta Widyanti, "Human Rights and Indonesian Legal Protection of Traditional Cultural Expressions: A Comparative Study in Kenya and South Africa," *Jurisdictie: Jurnal Hukum Dan Syariah* 14, no. 2 (2024): 315–34, https://doi.org/10.18860/j.v14i2.24318; M. Yazid Fathoni et al., "Reformulation of Sale And Purchase Agreement Regulations in Creating Legal Certainty and Justice in The Transfer of Land Rights in Indonesia," *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 1 (2024): 55–67, https://doi.org/10.29303/ius.v12i1.1351.

everyone has the right to privacy, protected by the Constitution and other legal frameworks. This right guarantees that citizens will not be subject to unauthorized intrusions by government or private entities. However, personal data leaks violate this right, undermining the state's authority to safeguard its citizens.

When personal data is leaked, citizens become vulnerable to the misuse of their information, including identity theft, fraud, and manipulation for commercial or political purposes.[36] In this context, data leaks represent not just a technical failure but a violation of fundamental rights, imposing on the state the responsibility to guarantee its citizens' rights. The rule of law mandates clear and effective protection of individual privacy, including through strict legal regulations governing personal data collection, storage, and use.

Data leaks also indicate failures in law enforcement and oversight, which are fundamental pillars of the rule of law. A state governed by the rule of law ensures that laws are somewhat and consistently applied and protects against human rights violations, including the right to privacy. However, when personal data is easily leaked or misused, it is evident that the legal system is not functioning effectively. This reveals a gap between what should happen and what occurs, where existing regulations fail to be implemented effectively.

The state's inability to address data leaks threatens the integrity of the rule of law. An ideal rule of law system would not only create regulations for data protection but also ensure their proper enforcement and implementation. Failure to protect personal data can erode public trust in state institutions, weaken the credibility of the law, and widen the gap between public expectations and reality.

In an ideal scenario, a state governed by the rule of law would provide protection and redress for victims of data breaches, including imposing strict sanctions on those responsible for the violations. However, personal data leaks will persist without a solid and effective system, further endangering citizens' privacy rights.

3. Legal Protection Measures Against Personal Data Leaks Taken By Authorized Institutions And Pse From The Perspective Of The Indonesian Legal System

The Indonesian government has taken significant legal steps to protect citizens' data by enacting the Personal Data Protection Law (UU PDP). This law marks a major milestone in safeguarding privacy rights in Indonesia, particularly given the rise in data breaches alongside the rapid growth of digital technology and online platforms. The law is designed to provide legal assurances that personal data is managed securely and not misused by unauthorized parties, whether in the public or private sectors.

The PDP Law passed in 2022, regulates various aspects of data collection, processing, and storage, setting security standards for entities handling personal data. It grants

[36] Akila Victor et al., "Survey on Effective Disposal of E-Waste to Prevent Data Leakage," *Computer Assisted Methods in Engineering and Science* 31, no. 2 (2024): 187–212, https://doi.org/10.24423/cames.2024.492.

individuals new rights regarding their data, such as access, amend, and even request the deletion of irrelevant data. Furthermore, the PDP Law requires data controllers in the public and private sectors to obtain explicit consent from individuals before processing their data. This gives citizens greater control over their personal information and ensures it is used only for legitimate and transparent purposes.

In addition to the PDP Law, the government has introduced several supporting regulations to strengthen personal data protection across various sectors. One such regulation is Permendagri No. 17 of 2020, which governs local governments' management of population data. This regulation ensures that local government agencies' handling of population data, such as identity numbers and addresses, complies with high-security standards. It serves as a crucial framework for protecting citizen data at the local level, especially considering the vast amount of data managed for public administration. Regular audits are also mandated to ensure the continued security of population data management systems and to guard against potential leaks.

In West Nusa Tenggara (NTB), personal data protection has become a priority as awareness of the importance of privacy rights grows. A concrete step taken by the NTB regional government includes a procedure for requesting the use of data through a recommendation from the provincial government to the central authority. This process ensures that every request to use citizens' data follows a controlled mechanism, with central authority approval required as part of stricter oversight. This measure aims to prevent unauthorized parties from misusing data and ensures that personal data is used only for legitimate purposes in accordance with applicable laws.

The NTB government also mandates that entities collaborating in data utilization obtain ISO 27001 certification, an international standard governing information security management systems. ISO 27001 provides a comprehensive framework for protecting data against hacking, data theft, or information leaks. Implementing this certification underscores NTB’s commitment to maintaining data integrity and security, not just as a legal obligation but also as a proactive effort to prevent data breaches that could harm citizens.

Although the implementation of personal data protection at the regional level, as demonstrated in NTB, shows good intentions to secure citizens' information, significant challenges remain. A key obstacle is the limited technological infrastructure needed to support the secure management of personal data. In regions like NTB and other remote, frontier, and underdeveloped (3T) areas, digital infrastructure, such as secure servers, updated software, and reliable networks, is often inadequate to meet the security standards required, including those set by ISO 27001.

Human resource limitations are also a major challenge. Many regions lack skilled personnel in cybersecurity and data management, and staff at the regional level often lack the expertise to manage data breach risks or conduct effective security audits. Training and competency development in data protection are often under-prioritized in budget and strategic planning. Consequently, implementing security standards, such as ISO 27001, is often ineffective due to the shortage of qualified experts.

The high costs of obtaining ISO 27001 certification present another significant barrier, particularly for regional institutions. The certification process requires substantial time, human, and financial resources. Many local governments or organizations lack sufficient budgets to pursue certification despite it being a critical requirement to safeguard data from external threats like hacking or unauthorized data use. Local budgets often prioritize immediate physical infrastructure or public service needs, leaving data protection efforts underfunded.

Moreover, maintaining ISO 27001 certification requires ongoing commitment, including continuous monitoring and periodic audits. Institutions that obtain certification must ensure compliance with established standards, which also demands additional resources. As a result, some institutions struggle to maintain their certification, leading to inconsistent data protection reliability.

These challenges illustrate that while legal frameworks have been well-established, their successful implementation at the regional level depends heavily on improvements in technical capacity and human resources. The central government plays a crucial role in providing support through adequate budget allocations, training for regional officers, or strict supervision. Investments in digital infrastructure and personnel training are essential to enhance information security management systems across the regions.

Additionally, the central government could consider providing subsidies or other assistance to alleviate the financial burden of ISO 27001 certification for regional institutions seeking to improve security standards. This could be achieved through economic incentives, facilitating partnerships with more affordable certification providers, or developing a certification system tailored to local conditions. Such measures could encourage more institutions at the local level to adopt international standards without facing excessive financial obstacles.

More substantial supervision from the central government is crucial to ensure that legal frameworks are implemented effectively on paper. Regular audits, monitoring, and evaluation of regional implementation should be conducted to ensure that citizens' data is protected from leaks or misuse. Effective oversight should include strict sanctions for institutions or entities that violate data protection regulations, reinforcing the seriousness of protecting citizens' privacy rights.

Conclusion

The issue of personal data leakage in Indonesia reflects significant challenges in safeguarding citizens' privacy rights, particularly with the increasing use of information technology in both the public and private sectors. Data leakage is caused by various factors, including the lack of strict enforcement of security standards, insufficiently trained human resources, and weak infrastructure, especially in regional areas. Although the government has introduced regulations such as the Personal Data Protection Law and Permendagri 17/2020, their implementation at the regional level remains far from optimal, particularly for ISO 27001 certification. This undermines the principle of a rule-of-law state that guarantees human rights, including the right to privacy, which the state must effectively protect.

References

Ahadi Deradjat, Agus, Mahiswara Timur, Nina Cornelia Santoso, and Dhan Partap Kaur. "Data Protection & Privacy 2024." Chamber and Partners, 2024. https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2024/indonesia/trends-and-developments.

Akbar, Muh, Fhad Syahril, Dina Maliah, and Hasan Nurhaedah. "Personal Data Leaks Ahead of 2024 Elections : Threats to Integrity and Public Trust." *Jurnal Litigasi Amsir* 7, no. 2023 (2024): 103–8.

APJII. "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang." APJII, 2024. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.

Asmara, Chandra. "Indonesia Probes Alleged Hack of Jokowi, Six Million Taxpayers." The Star, 2024. https://www.thestar.com.my/tech/tech-news/2024/09/19/indonesia-probes-alleged-hack-of-jokowi-six-million-taxpayers.

Badan Pusat Statistik (BPS). "Statistik Telekomunikasi Indonesia 2022." Badan Pusat Statistik (BPS), 2023. https://www.bps.go.id/id/publication/2023/08/31/131385d0253c6aae7c7a59fa/statistik-telekomunikasi-indonesia-2022.html.

BBC News Indonesia. "Ratusan Juta Data Dukcapil Kemendagri Diduga Bocor, Pakar Siber: 'Ini Peretasan Paling Parah.'" BBC News Indonesia, 2023. https://www.bbc.com/indonesia/articles/c51v25916zlo.

Binardy, Yudo Arhuma. "Legal Protection Arrangements in Indonesia for Privacy Rights in Cases of Personal Data Leakage." *International Journal of Social Science and Human Research* 04, no. 12 (2021): 3870–74. https://doi.org/10.47191/ijsshr/v4-i12-56.

Biro Humas Kementerian Kominfo. "Siaran Pers No. 132/HM/KOMINFO/07/2023 Tentang Kominfo Telusuri Dugaan Kebocoran Data Paspor 34 Juta Warga Indonesia." Kominfo, 2023. https://www.kominfo.go.id/berita/siaran-pers/detail/siaran-pers-no-132-hm-kominfo-07-2023-tentang-kominfo-telusuri-dugaan-kebocoran-data-paspor-34-juta-warga-indonesia.

Brilliannata, Jonathan, Rofikotul Jamiilah, and Haidar Talib. "Protection of Personal Data as Confidential Information in Criminal Proceedings." *Legal Brief* 11, no. 4 (2022): 2263–67. https://doi.org/10.47643/1815-1329_2022_6_125.

Chiu, Chih-Chieh, Pang-Wei Tsai, and Chu-Sing Yang. "Using an Efficient Detection Method to Prevent Personal Data Leakage for Web-Based Smart City Platforms." *Wireless Communications and Mobile Computing* 2023 (2023): 1–10. https://doi.org/10.1155/2023/5303329.

Christiadi, Robertus Nanda, and Rudi Sutomo. "Measurement of IT Security Governance Capabilities Using COBIT 2019 at Indonesian Business Sector." *G-Tech: Jurnal Teknologi Terapan* 7, no. 4 (2023): 1498–508. https://doi.org/10.33379/gtech.v7i4.3170.

Dewi, Sumartini, and Sri Wulandari. *Corporate Criminal Liability Telecommunication Company Against Consumer Personal Information Data Leakage in Indonesia*. Atlantis Press SARL, 2023. https://doi.org/10.2991/978-2-38476-024-4_23.

Fathoni, M. Yazid, Adi Sulistiyono, and Lego Karjoko. "Reformulation of Sale And Purchase Agreement Regulations in Creating Legal Certainty and Justice in The Transfer of Land Rights in Indonesia." *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 1 (2024): 55–67. https://doi.org/10.29303/ius.v12i1.1351.

Firdaus, Muhammad. *A Review of Personal Data Protection Law in Indonesia*. no. 1 (2020): 1–7.

Ivanova, Alla S., Nataliia G. Holionko, Tetiana B. Tverdushka, Tadeusz Olejarz, and Alina Y. Yakymchuk. "The Strategic Management in Terms of an Enterprise's Technological Development." *Journal of Competitiveness* 11, no. 4 (2019): 40–56. https://doi.org/10.7441/joc.2019.04.03.

Ji, Yitong, Aixin Sun, Jie Zhang, and Chenliang Li. "A Critical Study on Data Leakage in Recommender System Offline Evaluation." *ACM Transactions on Information Systems* 41, no. 3 (2023). https://doi.org/10.1145/3569930.

Kominfo. "Indeks Masyarakat Digital Indonesia (IMDI) Tahun 2022-2023." Kominfo, 2024. https://data.kominfo.go.id/opendata/dataset/indeks-masyarakat-digital-indonesia-imdi.

Kröger, Jacob Leon, Florian Müller, and Milagros Miceli. *How Data Can Be Used Against People: A Classification of Personal Data Misuses*. 2021.

Launa, Bambang Mudjiyanto, and Franky P. Roring. "Tendensi Politik Kejahatan Dunia Maya." *JIKA (Jurnal Ilmu Komunikasi Andalan)* 7, no. 1 (2024): 26–51. https://doi.org/10.31949/jika.v7i1.8762.

Mangesti, Yovita Arie, Slamet Suhartono, and Ahmad Mahyani. "Ethico-Legal Aspects Of Personal Data Protection In Indonesia." *International Journal of Educational Research & Social Sciences* 2, no. 5 (2021): 1030–37.

Neto, Nelson Novaes, Stuart Madnick, Anchises Moraes G.De Paula, and Natasha Malara Borges. "Developing a Global Data Breach Database and the Challenges Encountered." *Journal of Data and Information Quality* 13, no. 1 (2021): 1–33. https://doi.org/10.1145/3439873.

Rahma, Sintya Dewi, Bonifasius Ananda Putra, and Lukman Fahmi Djarwadit. "Analysis of the Indonesian Government ' S Efforts in Overcoming Public Data Leak Cases." *Proceeding: The Sunan Ampel International Conference of Political and Social*

Sciences (SAICoPSS), 1 (2023): 254–66. https://doi.org/10.15642/saicopss.2023.1..254-266.

Resecurity. "Vast Voter Data Leaks Cast Shadow Over Indonesia's 2024 Presidential Election Cyber Threat Intelligence." Resecurity, 2024. https://www.resecurity.com/blog/article/vast-voter-data-leaks-cast-shadow-over-indonesias-2024-presidential-election.

Rosadi, Sinta. "Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia." *Brawijaya Law Journal* 5, no. 2 (2018): 143–57. https://doi.org/10.21776/ub.blj.2018.005.01.09.

Rosmaini, E., T. F. Kusumasari, M. Lubis, and A. R. Lubis. "Study to the Current Protection of Personal Data in the Educational Sector in Indonesia." *Journal of Physics: Conference Series* 978, no. 1 (2018): 1–7. https://doi.org/10.1088/1742-6596/978/1/012037.

Satori, Akhmad, and Subhan Agung. "Personal Data Protecion in Indonesia: Legal Perspective." *International Journal of Multicultural and Multireligious Understanding* 7, no. 7 (2020): 183–89. http://dx.doi.org/10.18415/ijmmu.v7i7.177.

Septi, Charisma, and Jayanti Suraji. "The Issues of Data Protection Against Leaking of Personal Data in Social Security Health Services (a Comparison Between Indonesia and Other Countries Regulations)." *International Journal of Business, Economics and Law* 26, no. 1 (2022): 103–6.

Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga. "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (2020): 95–109. https://doi.org/10.18196/iclr.2219.

Shandy Utama, Andrew, Hasnati, Sandra Dewi, Rizana, Ade Pratiwi Susanty, and Olivia Anggie Johar. *Problematika Penegakan Hukum*. INSAN CENDEKIA MANDIRI, 2021.

Sholehudin, Miftahus, Moh Fadli, Rachmi Sulistyarini, and Djumikasih Djumikasih. "Cancellation of Marriage Due to Apostasy in Islamic Law and Human Rights: A Comparative Analysis of Indonesia and Malaysia." *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 1 (2025): 33–51. https://doi.org/10.18860/j-fsh.v17i1.31465.

Sri Ciptorukmi, Anjar, and Adalia Safira Rahma. "Urgensi Pembentukan Pengadilan Keluarga: Refleksi Perlindungan Hak Anak Dalam Kasus Perceraian Di Indonesia." *LITIGASI* 25, no. 2 (2024): 130–49. https://doi.org/10.23969/litigasi.v25i2.18009.

Taklima, Musa, Adi Sulistiyono, and M. Syamsudin. "Consumer Protection as an Instrument for Fulfilling Human Rights in the Economic Sector and Its Constitutionalizing Efforts in the 1945 Constitution." *JURISDICTIE* 14, no. 1 (2023): 75–105. https://doi.org/10.18860/j.v14i1.20844.

Victor, Akila, Gurunathan Arunkumar, Rajendran Kannadasan, Soundrapandiyan Rajkumar, and Ramani Selvanambi. "Survey on Effective Disposal of E-Waste to Prevent Data Leakage." *Computer Assisted Methods in Engineering and Science* 31, no. 2 (2024): 187–212. https://doi.org/10.24423/cames.2024.492.

Watson, Judy, David Lacey, Don Kerr, Paul Salmon, and Natassia Goode. "Understanding the Effects of Compromise and Misuse of Personal Details on Older People." *Australasian Journal of Information Systems* 23 (2019): 1–29. https://doi.org/10.3127/ajis.v23i0.1721.

Widyanti, Yenny Eta. "Human Rights and Indonesian Legal Protection of Traditional Cultural Expressions: A Comparative Study in Kenya and South Africa." *Jurisdictie: Jurnal Hukum Dan Syariah* 14, no. 2 (2024): 315–34. https://doi.org/10.18860/j.v14i2.24318.

Zaman, Akbari Amarul, Jumadi Anwar, and Aryo Fadlan. "Pertanggung Jawaban Pidana Kebocoran Data Bpjs Dalam Perspektif Uu Ite." *De Juncto Delicti: Journal of Law* 1, no. 2 (2021): 146–57. https://doi.org/10.35706/djd.v1i2.5732.