

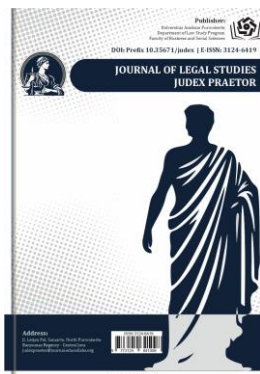


Protection of Personal Data in the Digital Era: Legal Analysis and Implementation Challenges in Indonesia

Carissa Tanuwidjaja¹

¹ Department of Law, Faculty of Law, Social Sciences and Political Sciences, Universitas Terbuka

ARTICLE INFO



History :

Submit on 3 July 2026

Review on 17 July 2026

Accepted on 31 July 2026

Keyword :

Personal Data Protection, Privacy Rights, Cybersecurity, Information Technology Law, Cybercrime.

ABSTRACT

The development of information and communication technology has had a significant impact on people's lives, especially in the exchange and use of personal data thru digital media. The high usage of the internet, social media, and electronic-based services in Indonesia has made personal data increasingly vulnerable to misuse, such as data breaches, identity theft, and the dissemination of information without the data owner's consent. This research aims to analyze the legal protection of personal data and examine the challenges of implementing personal data protection in the digital era in Indonesia. The research uses a normative juridical method with a legislative approach and a case approach. Research data is obtained thru library studies by collecting primary, secondary, and tertiary legal materials related to personal data protection, which are then analyzed using a qualitative descriptive method. Research results show that Law Number 27 of 2022 on Personal Data Protection has provided a more comprehensive legal basis in ensuring the privacy rights of the community. However, its implementation still faces various obstacles, such as low public awareness, weak data security systems, and suboptimal law enforcement. This research concludes that personal data protection requires strengthened oversight, increased digital literacy, and cooperation between the government, society, and electronic system operators. The research results are expected to provide input for the development of more effective personal data protection policies in Indonesia.

© 2026 Author

The copyright of this article belongs entirely to the author

Corresponding Author: carissatanuwidjaja09@gmail.com





INTRODUCTION

The rapid development of technology and information has provided various conveniences and benefits in modern society. The utilization of digital technology can be felt in almost all aspects of life, ranging from the transportation sector, tourism, trade, financial industry, to government services. This condition shows that mastery of information technology and science is an important part of efforts to improve the quality of life of the Indonesian people sustainably while also facing global challenges in the modern era.¹ The government's efforts in developing information and communication technology are fundamentally aimed at ensuring the protection of personal data for all Indonesian citizens.

As a developing country, Indonesia continues to make progress through various innovations in the field of information and communication technology that enable the processes of data collection, storage, and analysis to be carried out more effectively and efficiently. These developments have made almost all sectors of life increasingly dependent on the utilization of information technology systems, such as electronic commerce (e-commerce) in the trade and business sector, electronic education (e-education) in the field of education, electronic health (e-health) in the health sector, and electronic government (e-government) in the administration of government. In addition, the utilization of technology is also reflected in the use of search engines, social networks, smartphones, mobile internet, and the development of cloud computing technology.² The use of digital services in daily life, such as social media, electronic commerce transactions, and data entry through online platforms, causes personal data to be continuously processed and stored electronically, leading to increasingly serious legal issues related to personal data protection in Indonesia.³

The rapid development of information and communication technology also opens up opportunities for the misuse of digital technology, causing unrest, especially through various crimes that utilize digital media and social

¹ CSA Teddy Lesmana, Eva Elis, and Siti Hamimah, "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia," *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, Vol. 3, No. 2, (2022), p. 1-6.

² Erlina Maria Christin Sinaga and Mery Christian Putri, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, Vol. 9, No. 2, (2020), p. 237.

³ Predderics Hockop Simanjuntak, "Perlindungan Hukum Terhadap Data Pribadi Pada Era Digital di Indonesia: Studi Undang - Undang Perlindungan Data Pribadi Dan General Data Protection Regulation (GDPR)," *Esensi Hukum*, Vol. 6, No. 2 (2025), p. 105.



media as means or objects of crime known as cybercrime.⁴ For example, perpetrators can misuse various features on digital platforms to commit phishing, identity theft, hate speech dissemination, or organized content manipulation.⁵ These actions are generally related to the use of personal data, which includes all information attached to an individual and can be used to identify someone either directly or indirectly, such as name, address, national identification number (NIK), phone number, health history, and digital activities and preferences.⁶

In the development of the digital era, personal data is viewed as an important asset that requires adequate legal protection, considering the high risk of privacy violations that can occur in various electronic activities and transactions. The leakage of personal data is not only a violation of an individual's right to privacy but also has the potential to cause both material and immaterial harm to the victim.⁷ In this case, the concept of privacy itself can be understood as an effort to maintain a person's integrity and dignity, where the right to privacy grants individuals the authority to determine who can access information about them and how that information is used.⁸

Among the various data breach cases that occurred in Indonesia, there are two prominent incidents, namely the Tokopedia data breach in 2020 and the Health Social Security Agency (BPJS Kesehatan) data breach in 2021. The Tokopedia case began with a hacking incident that occurred on March 20, 2020, which resulted in the exposure of approximately 91 million user accounts and 7 million merchant accounts. The data obtained unlawfully was then sold on the dark web, including information such as user ID, email address, full name, date of birth, gender, phone number, and even user passwords. Meanwhile, the BPJS Kesehatan case also occurred due to hacking, resulting in the leakage of personal data belonging to 279 million individuals, including data of deceased residents. The data sold includes names, phone numbers, addresses, income information, and demographic data, with around 20 million of the data also containing personal photos. Both

⁴ Alejandro Morion Ruben Thomas and Happy Yulia Anggraeni, "Cybercrime Dan Media Sosial: Analisis Hukum Terhadap Tren Peningkatan Tindak Pidana Di Era Digital," *Jurnal Hukum Lex Generalis*, Vol. 6, No. 7, (2025), p. 1-22.

⁵ Thomas, A. M. R., & Anggraeni, H. Y. Cybercrime dan Media Sosial: Analisis Hukum terhadap Tren Peningkatan Tindak Pidana di Era Digital. *Jurnal Hukum Lex Generalis*, Vol. 6, No. 7, (2025), p.7.

⁶ Simanjuntak, Op.Cit., p. 106.

⁷ Farha Nadiyah and Sidi Ahyar Wiraguna, "Tinjauan Hukum Terhadap Perlindungan Data Pribadi Dalam Transaksi Elektronik di Indonesia," *Jurnal Riset Multidisiplin Edukasi*, Vol. 2, No. 6, (2025), p. 270.

⁸ Erlina Maria Christin Sinaga, and Mery Christian Putri. "Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, Vol. 9, No. 2, (2020), p. 237



incidents demonstrate that data breaches have caused significant impacts and serious losses for the affected parties.⁹

The phenomenon of data harvesting or large-scale data collection by third parties without clear user consent is also one of the factors that trigger data breaches. This practice is generally carried out by advertisers, third-party application developers, or social media platforms for commercial purposes. The data that has been successfully collected can then be sold to data brokers or used to create user profiles for psychological, political, or economic targeting purposes. These conditions ultimately create an exploitative digital ecosystem that is not in line with the principles of privacy protection.

In addition, the low level of digital literacy also contributes to the increased vulnerability to data breaches. Many social media users do not yet understand the importance of privacy settings, the use of secure passwords, and the risks of sharing personal information in the digital space. This is further exacerbated by the lack of structured education, both from the government and digital service providers. As a result, users have difficulty identifying potential risks and avoiding harmful digital practices, making the improvement of digital literacy a very important preventive measure.¹⁰

The need for stronger and more stringent legal protection is increasing along with the rise in data breaches and the misuse of personal information. Several major incidents, such as data breaches of users on various digital platforms and e-commerce services, indicate weaknesses in the current data protection system. This condition has prompted demands from various parties, both the public and non-governmental organizations, for the immediate establishment of more comprehensive regulations regarding personal information security that are oriented toward protecting the interests of data subjects or service users.

The role of the government in protecting public data in the digital space still faces various obstacles, even tho the ITE Law includes provisions regarding sanctions for perpetrators who commit hacking or data misuse. In practice, law enforcement against cybercrime perpetrators still encounters various challenges, especially in the identification process and the capture of perpetrators in the digital space that is cross-border. As a result, many cases of data breaches are not handled optimally. In addition, the lack of comprehensive regulations governing the accountability of data controllers

⁹ Callista Lauren et al., "Kebocoran Data Pribadi di Indonesia Sebagai Ancaman Keamanan Siber Dalam Kasus Tokopedia Dan BPJS Kesehatan," *Jurnal Pendidikan Tambusai*, Vol. 10, No. 1, (2026), p. 8145.

¹⁰ Rendy Lesmana and Muhammad Irwan Padli Nasution, "Kebocoran Data Di Media Sosial: Analisis Pola Dan Strategi Pencegahannya," *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, Vol. 2, No. 10, (2025), p. 123.



or data storage entities also constitutes a weakness in the existing legal system. This condition has driven the increasing need for more specific regulations, leading to the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law). However, in its implementation, the provisions of the law have not yet been optimally and evenly applied in society.¹¹

Based on this background, this research examines the urgency of the Personal Data Protection Law in ensuring the security of personal data as part of fulfilling the right to privacy of society in the digital era, the implementation of personal data protection in Indonesia amidst technological developments and increasing digital activities, as well as various obstacles and solutions in enhancing the effectiveness of personal data protection in Indonesia. Thus, this research is expected to provide a more comprehensive understanding of the importance of personal data protection and serve as a study material to support the effectiveness of personal data protection law enforcement in Indonesia.

METHOD

This research uses the normative juridical legal research method or doctrinal research that focuses on library studies by utilizing secondary data in the form of laws and regulations, court decisions, as well as the opinions of legal experts related to the issues being studied. The approaches used include the statute approach and the case approach to analyze legal provisions and their application in practice. Data analysis is conducted qualitatively with a legal perspective, emphasizing legal reasoning based on applicable norms, principles, and legal doctrines.¹²

The normative legal approach has the advantage of providing a clear, systematic, and structured legal framework. This approach also offers a strong theoretical foundation in analyzing legal issues thru the examination of norms in legislation. In addition, this approach helps provide certainty in the interpretation of law based on the applicable provisions. Thus, the normative approach becomes an important foundation in legal studies.

The normative legal approach has the advantage of providing a clear, systematic, and structured legal framework. This approach also offers a strong theoretical foundation in analyzing legal issues thru the examination of norms in legislation. In addition, this approach helps provide certainty in

¹¹ Asa Pramudya Kristanto, "Perlindungan Terhadap Data Pribadi Dalam Aplikasi Digital Sebagai Bentuk Perlindungan Hak Asasi Manusia," *UNES Law Review*, Vol. 5, No. 3, (2023), p. 952.

¹² Yulia Audina Sukmawan and Dwi Damayanti, "Metode Penelitian Hukum Normatif Dan Empiris Sebagai Strategi Penguatan Perspektif Kajian Ilmu Hukum," *Notary Law Journal*, Vol. 4, No. 3, (2025), p. 114–28.



the interpretation of law based on the applicable provisions. Thus, the normative approach becomes an important foundation in legal studies.

The normative approach has limitations because it tends to be static and only focuses on legal texts. This causes the approach to be less capable of capturing the social dynamics that develop in society. In addition, this approach does not fully encompass empirical aspects, such as the application of law in practice and the public's acceptance of the law. Therefore, this approach has a limited scope in depicting the legal reality as a whole.¹³

RESULT & DISCUSSION

A. Analysis of Legal Protection for Personal Data Privacy in the Digital Era

Analysis of Legal Protection for Personal Data Privacy in the Digital Era The principle of the right to privacy of personal data is an important aspect in the development of the digital era, where society cannot be separated from the use of technology that involves the exchange of personal data online. Personal data includes information that can identify an individual, either directly or indirectly, such as name, address, phone number, email address, date of birth, identification number, financial data, and health information. However, the use of digital services has the potential to pose risks of misuse and privacy violations. The right to privacy over personal data grants individuals the authority to know the management of their personal data, including who accesses it, the purpose of its use, as well as the mechanisms for storing and processing the data. It also includes the right to give consent, request deletion (right to be forgotten), and make corrections if there are inaccuracies in the data.¹⁴

The concept of privacy was first developed by Warren and Brandeis thru a scientific article published in the Harvard Law Review titled The Right to Privacy, which essentially asserts an individual's right to be left undisturbed. In their writing, Warren and Brandeis explain that technological advancements have raised a new awareness in society regarding the importance of an individual's right to enjoy their life peacefully. They also stated that "Privacy is the right to enjoy life and the right to be left alone, and this development of the law was inevitable and

¹³ Sidi Ahyar Wiraguna, "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif Di Indonesia," *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum*, Vol. 3, No. 3, (2024).

¹⁴ Kadek Rima Anggen Suari and I Made Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi di Indonesia," *Jurnal Analisis Hukum*, Vol. 6, No. 1, (2023), p. 132.



demanded legal recognition," which indicates that the right to privacy is a part that requires legal acknowledgment.¹⁵

According to Danrivanto Budhijanto, the protection of private rights or personal rights can enhance humanitarian values, strengthen the relationship between individuals and society, reinforce independence or autonomy in self-control and achieving eligibility, foster a spirit of tolerance, prevent discriminatory actions, and limit the abuse of authority by the government.¹⁶

In international law and human rights, wiretapping is fundamentally categorized as a prohibited act because it contradicts the protection of individual privacy rights. Article 12 of the Universal Declaration of Human Rights (UDHR) 1948 asserts that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, and everyone has the right to the protection of the law against such interference or attacks.¹⁷ A similar provision is also stipulated in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) 1966, which prohibits arbitrary or unlawful interference with privacy, family, home, or correspondence, and guarantees everyone the right to legal protection against such interference or attacks.

In General Comment No. 16 on Article 17 of the ICCPR, it is emphasized that states are obliged to ensure the confidentiality of communications, including correspondence, both legally and in practice, and to prohibit all forms of surveillance, interception of communications, and recording of conversations without a valid legal basis.¹⁸ In line with this, Article 8(1) of the European Convention on Human Rights also affirms the right of every individual to respect for their private and family life, home, and correspondence.¹⁹ Various provisions indicate that privacy protection is a fundamental principle in international law. Therefore, wiretapping without a valid legal basis is essentially considered a violation of human rights as it deprives

¹⁵ Kusnadi Sekaring Ayumeida and Andy Usmina Wijaya, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi," *Al Wasath Jurnal Ilmu Hukum*, Vol. 2, No. 1, (2021), p. 9.

¹⁶ Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran Dan Teknologi Informasi: Regulasi Dan Konvergensi*, 1st ed., Bandung, PT Refika Aditama, (2010).

¹⁷ Lesmana, Elis, dan Hamimah, *Loc.Cit.*

¹⁸ Danil Erlangga Mahameru et al., "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas di Indonesia," *Esensi Hukum*, Vol. 5, No. 2, (2024), p. 115.

¹⁹ Jawahir Thontowi, "Penyadapan Dalam Hukum Internasional Dan Implikasinya Terhadap Hubungan Diplomatik Indonesia Dengan Australia," *Jurnal Hukum IUS QUIA IUSTUM*, Vol. 22, No. 2, (2015), p. 183.



individuals of their rights to privacy, dignity, and security in their personal lives.

Indonesia has a strategic position in international trade at the global economic level, including in the development of electronic transactions that further encourage the widespread dissemination of personal data. However, until now, Indonesia is still classified as one of the countries in the ASEAN region that does not yet have specific regulations that comprehensively govern the protection of personal data.²⁰ Nevertheless, legal protection for personal data has actually been pursued thru the Indonesian Constitution and various applicable sectoral regulations, so its regulation can be traced in several existing legal instruments.

Although Indonesia does not yet have a *lex specialis* regulation specifically governing the protection of personal data, the protection of privacy rights still finds its regulatory basis in the constitution, namely the 1945 Constitution of the Republic of Indonesia (UUD 1945), particularly Article 28G. This article affirms that everyone has the right to personal protection, family, honor, dignity, and property under their control, as well as the right to a sense of security and protection from the threat of fear of performing or not performing an action that is a human right. Although it does not explicitly mention the terms privacy or personal data protection, this provision can still be interpreted as a constitutional basis for providing protection to personal data and serves as a reference in the formulation of more specific regulations in this field.²¹

After the amendment of the 1945 Constitution of the Republic of Indonesia (UUD 1945), regulations regarding privacy rights have been further strengthened thru various laws and regulations, one of which is Law Number 11 of 2008 concerning Electronic Information and Transactions, which has been amended by Law Number 19 of 2016. These provisions are the implementation of constitutional mandates to provide protection for personal data as part of human rights. In Article 26 paragraph (1) of the ITE Law, it is stipulated that everyone has the right to the protection of their personal data, including the right to live a private life independently, interact without unauthorized surveillance, and obtain protection against the use of their personal information.

²⁰ Olisias Gultom, Auditya Firza Saputra, and Muhammad Faiz Aziz, "Perlindungan Data Pribadi di Indonesia Menyikapi Liberalisasi Ekonomi Digital", Indonesia for Global Justice, (2021).

²¹ Wahyudi Djafar, Ruben Fritz, and Blandina Lintang Setianti, *Perlindungan Data Pribadi di Indonesia: Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia*, Jakarta: ELSAM, (2016).



More comprehensive regulations regarding personal data protection are governed by Law Number 27 of 2022 on Personal Data Protection. This law was enacted to strengthen the guaranty of privacy rights protection, raise public legal awareness, and ensure the recognition and respect for the principles of personal data protection. In addition, the law also regulates administrative and criminal sanctions as outlined in Article 57 as a form of law enforcement against personal data violations. Furthermore, technical provisions regarding personal data protection are also regulated in ministerial regulations issued by the Ministry of Communication and Information, Article (3) of Article 17 No. 12 of 2016, which emphasizes that personal data must be kept confidential, intact, and authentic. Furthermore, electronic system operators are required to protect user data and grant data subjects the right to access, correct, object to, and request the deletion of personal data in accordance with applicable laws and regulations.

The implementation of the Personal Data Protection Law (UU PDP) in practice has not yet fully met expectations. One of the main obstacles is the absence of a personal data supervisory authority as mandated by the law, whereas the existence of this institution plays a crucial role in ensuring compliance and the effectiveness of personal data protection.²² In addition, there are still many business operators, especially micro, small, and medium enterprises (MSMEs), who do not fully understand the obligations that must be met, thus potentially causing unintentional violations.

In addition, data breaches still occur despite the regulations being implemented, indicating weaknesses in both technical aspects and data management governance in various institutions. Although Law Number 27 of 2022 on Personal Data Protection has become the main legal basis for personal data protection in Indonesia, its implementation still faces various obstacles, including the suboptimal handling of data breach cases and the absence of an independent supervisory body as a law enforcement authority. In addition, the implementation of sanctions has not been effective because technical mechanisms such as the classification of violations and the determination of the types of sanctions have not been detailed, leading to uncertainty in law enforcement practices.²³

²² Muhamad Adri Rinjani and Ricky Firmansyah, "Hambatan Implementasi UU 27/2022 Dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia," *Jurnal Analisis Hukum*, Vol. 8, No. 1, (2025), p. 70.

²³ *Ibid.*, p. 72.



This condition is exacerbated by the low level of awareness and the limited technical capacity of electronic system managers in both the public and private sectors, which affects the weakness of the data protection system and complicates the process of investigating and proving violations. Therefore, the effectiveness of personal data protection does not only depend on the existence of legal norms but also requires institutional strengthening, enhancement of human resource competencies, and clarity of operational guidelines to ensure optimal implementation. In addition, a more comprehensive national strategy is needed thru the enhancement of public education, strengthening of technical capacity, and harmonization of regulations related to personal data protection so that the implementation of the PDP Law can provide more effective protection for the community.

B. Implementation of Personal Data Legal Protection in Indonesia

In practice, the implementation of legal protection for personal data in Indonesia still faces various challenges, as evidenced by a number of data breach cases on digital platforms. The data breach case on Tokopedia that occurred in 2020 began with a suspected hacking incident on March 20, 2020, and was then published on the Raid Forums by a hacker named Whysodank on May 2. Initially, the number of affected accounts was reported to be around 15 million, but it later grew to approximately 91 million user accounts and 7 million merchant accounts, nearly encompassing all accounts on the platform. The allegedly leaked data includes user IDs, email addresses, full names, dates of birth, genders, phone numbers, and passwords still in hash form. This data was then sold on the dark web for around USD 5,000 or the equivalent of IDR 74 million, and it was reported that millions of accounts could be downloaded thru certain links.

In the development of the case, the hacker also announced the sale of the data thru the Empire Market forum under the account name ShinyHunters. The circulating information indicates that the leaked data does not only cover a small portion of users, but reaches approximately 91 million accounts. In response to this, Tokopedia stated that they have discovered an attempt to steal user data, but emphasized that sensitive information such as payment data, including debit cards, credit cards, accounts, and the OVO digital wallet, remains safe.²⁴ The leak of Tokopedia's customers' personal data indicates that the e-commerce

²⁴ CNN Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan dijual," May 2020, <https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual>.



platform has not fully implemented optimal personal data protection principles, allowing user data to be accessed by irresponsible parties, then hacked and sold, indicating unauthorized disclosure of personal information.

Based on the chronology of the Tokopedia data breach case, the incident can be classified as an Unlawful Act as regulated in Article 1365 of the Civil Code (KUHPerdata). The provision emphasizes that any unlawful act causing harm to another party obliges the perpetrator to provide compensation for their wrongdoing. In this context, the electronic system organizer as a business operator has legal responsibility for the occurrence of user personal data breaches. In connection with the incident, the Chairman of the Indonesian Consumer Community (KKI), David Tobing, stated that they received reports from several Tokopedia users regarding allegations of misuse of personal data by third parties without the consent of the data owners. The public's concern about the potential misuse of data that could cause future harm was the basis for filing the report.

On May 6, 2020, KKI filed a lawsuit against the Minister of Communication and Information as Defendant I and PT Tokopedia as Defendant II thru the Central Jakarta District Court with case number 235/PDT.G/PN.JKT.PST. In its petition, KKI requested the revocation of Tokopedia's Electronic System Organizer Registration Certificate (TD PSE) and the imposition of an administrative sanction in the form of a fine of IDR 100,000,000,000 to be deposited into the state treasury after the decision becomes legally binding. In addition, Tokopedia is also requested to issue an apology and take responsibility toward users for the alleged misuse of personal data, as well as provide written notification to all users regarding personal data that is suspected to have been unlawfully accessed by third parties.²⁵

This was clarified by Ayu and Nasution (2023), in the case of the data breach, Tokopedia as the electronic system provider is suspected of not complying with the provisions of Article 3 paragraph (1) of Government Regulation Number 71 of 2019, which requires the operation of electronic systems to be reliable, secure, and responsible. Additionally, Tokopedia is also considered to have violated the provisions of Article 2 paragraph (2) and Article 28 letter c of Minister of Communication and Information Regulation Number 20 of 2016 because

²⁵ Ragil Putri Anindya and Achmad Edi Subianto, "Tanggung Jawab Platform Tokopedia Dalam Kasus Kebocoran Data Menurut Undang-Undang Tentang Perlindungan Data Pribadi," *RIGGS: Journal of Artificial Intelligence and Digital Business*, Vol. 4, No. 3, (2025), 1105.



it is deemed not to have transparently communicated information regarding the personal data breach to users. At the beginning of the case's revelation, Tokopedia only communicated the occurrence of a data breach and emphasized that users' passwords and financial data remained safe, but it later became known that approximately 91 million user accounts experienced a personal data breach that could be accessed by unauthorized parties, raising public concern about the security of personal data on digital platforms.²⁶

Before the Tokopedia data breach incident, Indonesia did not have specific regulations governing comprehensive personal data protection. Regulations regarding data protection at that time were still scattered across various sectoral regulations, such as Law Number 11 of 2008 on Information and Electronic Transactions, Government Regulation Number 82 of 2012, and Minister of Communication and Information Regulation Number 20 of 2016. This condition has resulted in personal data protection lacking an integrated and comprehensive legal basis to address the rapid development of digital technology.²⁷

The increase in data breach cases, including the Tokopedia, BPJS Kesehatan, and eHAC incidents, has prompted the government to expedite the ratification of Law Number 27 of 2022 on Personal Data Protection. This law regulates various obligations for electronic system organizers, such as the appointment of a Data Protection Officer (DPO), the obligation to report data breach incidents within 72 hours, and granting users the right to access, correct, and delete their personal data. In addition, the PDP Law also includes provisions regarding administrative and criminal sanctions for violations of personal data protection. In this context, Tokopedia, as an electronic system organizer, needs to adjust its security system and data protection policies to align with the applicable legal regulations.

The Tokopedia data breach case shows weaknesses in the implementation of preventive and repressive protections in the management of personal data. This is evident from the inability of the electronic system operators to prevent illegal access to the user database, which resulted in approximately 91 million user data being accessed and unlawfully sold by third parties. In addition, the response

²⁶ Sinta Sukma Ayu and Muhammad Irwan Padli Nasution, "Analisis Kebocoran Data Privacy Pada E-Commerce Tokopedia," *JUEB: Jurnal Ekonomi Dan Bisnis*, Vol. 2, No. 3, (2023), p. 21-24.

²⁷ Abelia Mita Baqis and Muhammad Irwan Padli Nasution, "Pentingnya Perlindungan Dan Keamanan Data Privasi Di Era Digital," *Jurnal Manajemen Dan Pendidikan Agama Islam*, Vol. 3, No. 3, (2025), p. 396.



to the incident is considered suboptimal, especially in terms of notification, protection, and recovery of user rights as regulated in Law Number 27 of 2022 on Personal Data Protection. This condition reflects ongoing weaknesses in the implementation of personal data protection principles in the digital space.

Although the incident occurred before the Personal Data Protection Law was officially enacted, its impact is still felt to this day and has also raised awareness among the public and business actors regarding the urgency of personal data protection. Various data breach cases also show that there is still a gap between the legal regulations that have been established and the readiness of technical infrastructure in their implementation. Many institutions in Indonesia still do not have adequate data protection systems, both in terms of technology and organizational governance that supports data security. Therefore, there is a need to strengthen institutional capacity and improve data protection standards in a more systematic and sustainable manner.

Thus, as a personal data controller, Tokopedia should fulfill its responsibilities based on the principles of personal data protection in accordance with the provisions of the Personal Data Protection Law. This can be realized thru the implementation of preventive measures such as data encryption, the use of firewalls, regular security audits, and strict access control to the system. On the other hand, repressive measures are also necessary, such as public notification, compensation or restitution for affected data subjects, and involvement in dispute resolution mechanisms. All these efforts must be carried out by prioritizing the principles of accountability and transparency in the management of personal data.

C. Challenges and Solutions for Protecting Personal Data Privacy in the Digital Era

In the current development of the digital era, personal data has become one of the most valuable assets for both individuals and organizations. Personal information such as names, addresses, phone numbers, and financial data often becomes an object that is vulnerable to misuse by irresponsible parties. One of the factors contributing to the weak protection of personal data in Indonesia is the still low public understanding of the importance of maintaining the confidentiality of information in the digital space. Many users still use simple passwords, share personal data on social media without adequate consideration, and do not yet understand the risks of using untrustworthy websites or applications. On the other hand, several business operators have not yet implemented adequate data security systems, such as end-to-end



encryption, multi-factor authentication, and direct monitoring of suspicious activities. The situation is worsened by the suboptimal implementation of internal policies and the lack of regular cybersecurity audits.²⁸

Conceptually, personal data protection encompasses two main aspects: securing various forms of data, both physical and non-physical, and regulating the use of data to prevent misuse by unauthorized parties, including access restrictions, usage for legitimate purposes, and data deletion when necessary. In practice, personal data breaches still frequently occur in society, accompanied by ineffective law enforcement mechanisms against violations, indicating that legal protection in this area is not yet optimal and reinforcing the urgency for more comprehensive regulations. On the other hand, Article 28G of the 1945 Constitution of the Republic of Indonesia emphasizes that the protection of personal self, including personal data, is part of human rights that must be guaranteed by the state. Thus, the development of information technology and the increasing use of digital services demand a more structured, comprehensive, and responsive personal data protection system to effectively guarantee privacy protection for the public.

In light of the various issues outlined above, a number of measures are required to address them, which can be summarised as follows:²⁹

1. Strengthening Institutional and Independent Supervisory Authority

There is a need for the acceleration of the establishment of an independent personal data supervisory authority, with clear authority, and functioning effectively in supervision, law enforcement, sanctioning, and public education. This institution must have strong operational capacity and be free from certain interest interventions to ensure legal certainty in personal data protection.

2. Harmonization and Synchronization of Regulations

The government needs to harmonize the Personal Data Protection Law with other sectoral regulations, such as the ITE Law, health sector regulations, finance, and telecommunications. This alignment is important to avoid overlapping norms, clarify authority, and create legal certainty in the implementation of data protection across various sectors.

²⁸ Baqis dan Nasution, "Pentingnya Perlindungan Dan Keamanan Data Privasi."

²⁹ Rolib Sitorus, Joy Zaman, and Ricky Banke, "Kendala Pelaksanaan Perlindungan Data Pribadi," *Locus: Jurnal Konsep Ilmu Hukum* 5, no. 1 (March 2025): 53–61, <https://doi.org/10.56128/jkih.v5i1.438>.



3. Strengthening Effective and Just Law Enforcement

Law enforcement must be carried out consistently by imposing strict, proportional sanctions that have a deterrent effect. The mechanisms for reporting, investigating, and imposing sanctions need to be clarified in derivative regulations to prevent legal ambiguities in practice. In addition, protection for victims must be a priority in every law enforcement process.

4. Improvement of Cybersecurity Infrastructure

Strengthening data security systems must be carried out thru investments in cybersecurity technologies such as data encryption, firewalls, intrusion detection systems, and regular security audits. Additionally, improving the quality of human resources in the field of information security is an important factor to ensure that data protection systems operate optimally.

5. Improvement of Community Digital Literacy

The public needs to be continuously educated about the importance of personal data protection, the risks of data misuse, and their legal rights. This education can be carried out thru public campaigns, integration into the education curriculum, and the use of digital media to reach all layers of society.

6. Strengthening Business Compliance

Business actors, especially MSMEs, need to be encouraged to implement data security standards thru the provision of simple compliance guidelines, technical training, and incentives for regulatory compliance. The government also needs to provide support mechanisms so that data protection implementation can run effectively in the private sector.

7. Regulation of Cross-Border Data Transfers

More detailed regulations are needed regarding the mechanism of cross-border data transfer to ensure data protection is maintained even when processed outside Indonesia's jurisdiction. In addition, international cooperation needs to be strengthened to address the challenges of digital globalization.

8. Strengthening Multistakeholder Collaboration

Personal data protection must be built thru collaboration between the government, the private sector, academia, and civil society. This approach is important to create a safe, transparent, and sustainable digital ecosystem and to ensure comprehensive protection of the public's privacy rights.



CONCLUTIONS

The development of digital technology has had a significant impact on the use and management of personal data in people's lives. The use of various electronic-based services has made personal data an important part that must receive legal protection because it relates to the privacy rights of each individual. Based on research findings, the protection of personal data in Indonesia has a legal basis thru Law Number 27 of 2022 on Personal Data Protection, which regulates the rights of data owners, the obligations of data controllers, and sanctions for personal data violations. The presence of such regulations demonstrates the state's efforts to provide legal certainty and protection to the public in the digital era.

However, the implementation of personal data protection in Indonesia still faces various obstacles. The low public awareness regarding the importance of protecting personal data, the weak cybersecurity system, and the suboptimal supervision and law enforcement are the main obstacles in the implementation of personal data protection. In addition, the rapid development of technology makes the management of personal data increasingly complex, requiring adequate regulatory readiness, infrastructure, and human resources.

Based on the research findings, more optimal efforts are needed to enhance personal data protection in Indonesia. The government needs to strengthen oversight and law enforcement against personal data violations to create legal certainty and effective protection for the public. In addition, improving digital literacy among the public is also important so that people better understand the risks of personal data misuse in the use of digital services. Electronic system providers and business actors also need to enhance their information security systems to prevent data leaks and misuse. With the cooperation between the government, society, and the private sector, the protection of personal data in Indonesia is expected to be more effective and able to provide a sense of security in the use of digital technology.

REFERENCE

- Anindya, Ragil Putri, and Achmad Edi Subianto. "Tanggung Jawab Platform Tokopedia Dalam Kasus Kebocoran Data Menurut Undang-Undang Tentang Perlindungan Data Pribadi." *RIGGS: Journal of Artificial Intelligence and Digital Business* 4, no. 3 (August 2025): 1105–12. <https://doi.org/10.31004/riggs.v4i3.2105>.
- Ayu, Sinta Sukma, and Muhammad Irwan Padli Nasution. "Analisis Kebocoran Data Privacy Pada E-Commerce Tokopedia." *JUEB : Jurnal*



- Ekonomi Dan Bisnis* 2, no. 3 (September 2023): 21–24.
<https://doi.org/10.57218/jueb.v2i3.716>.
- Baqis, Abelia Mita, and Muhammad Irwan Padli Nasution. "Pentingnya Perlindungan Dan Keamanan Data Privasi Di Era Digital." *Jurnal Manajemen Dan Pendidikan Agama Islam* 3, no. 3 (May 2025): 396–404.
<https://doi.org/10.61132/jmpai.v3i3.1150>.
- CNN Indonesia. "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual," May 2020.
<https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual>.
- Danil Erlangga Mahameru, Aisyah Nurhalizah, Haikal Badjeber, Ahmad Wildan, and Haikal Rahmadia. "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia." *Esensi Hukum* 5, no. 2 (August 2024): 115–31.
<https://doi.org/10.35586/esensihukum.v5i2.240>.
- Danrivanto Budhijanto. *Hukum Telekomunikasi, Penyiaran Dan Teknologi Informasi : Regulasi Dan Konvergensi*. 1st ed. PT Refika Aditama, 2010.
- Jawahir Thontowi. "Penyadapan Dalam Hukum Internasional Dan Implikasinya Terhadap Hubungan Diplomatik Indonesia Dengan Australia." *Jurnal Hukum IUS QUIA IUSTUM* 22, no. 2 (April 2015): 183–202. <https://doi.org/10.20885/iustum.vol22.iss2.art1>.
- Kementerian Komunikasi dan Informatika. "Peraturan Menteri Komunikasi Dan Informatika Nomor 12 Tahun 2016 Tentang Registrasi Pelanggan Jasa Telekomunikasi." bpk.go.id. BN 2016/NO 1135; KOMINFO.GO.ID; 17 HLM, August 2016.
<https://peraturan.bpk.go.id/Details/150534/permenkominfo-no-12-tahun-2016>.
- Kristanto, Asa Pramudya. "Perlindungan Terhadap Data Pribadi dalam Aplikasi Digital Sebagai Bentuk Perlindungan Hak Asasi Manusia." *UNES Law Review* 5, no. 3 (March 2023): 952–60.
<https://reviewunes.com/index.php/law/article/view/367/251>.
- Lauren, Callista, Cassie Andrea Jonathan, Christy Abigail Tjahyadi, and Angelita Butar. "Kebocoran Data Pribadi di Indonesia Sebagai Ancaman Keamanan Siber Dalam Kasus Tokopedia Dan BPJS Kesehatan." *Jurnal Pendidikan Tambusai* 10, no. 1 (April 2026): 8145–53.
<https://doi.org/10.31004/jptam.v10i1.37691>.
- Lesmana, CSA Teddy, Eva Elis, and Siti Hamimah. "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi



- Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia.” *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia* 3, no. 2 (June 2022): 1–6. <https://doi.org/10.52005/rechten.v3i2.78>.
- Lesmana, Rendy, and Muhammad Irwan Padli Nasution. “Kebocoran Data Di Media Sosial: Analisis Pola Dan Strategi Pencegahannya.” *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial* 2, no. 10 (2025): 123–28. <https://doi.org/10.5281/zenodo.15388529>.
- Nadiah, Farha, and Sidi Ahyar Wiraguna. “Tinjauan Hukum Terhadap Perlindungan Data Pribadi dalam Transaksi Elektronik Di Indonesia.” *Jurnal Riset Multidisiplin Edukasi* 2, no. 6 (June 2025): 270–78. <https://doi.org/10.71282/jurmie.v2i6.443>.
- Olisias Gultom, Auditya Firza Saputra, and Muhammad Faiz Aziz. “Perlindungan Data Pribadi di Indonesia Menyikapi Liberalisasi Ekonomi Digital.” Indonesia for Global Justice, 2021.
- RI, Peraturan Pemerintah. “Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.” LN.2022/No.196, TLN No.6820, jdih.setneg.go.id: 34 hlm., October 2022. <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>.
- . “Undang-Undang Informasi Dan Transaksi Elektronik (Pasal 26 Ayat 1, Nomor 19 Tahun 2016,” 2016.
- Rinjani, Muhamad Adri, and Ricky Firmansyah. “Hambatan Implementasi UU 27/2022 Dan Strategi Penguatan Perlindungan Data Pribadi Di Indonesia.” *Jurnal Analisis Hukum* 8, no. 1 (April 2025): 70–83. <https://doi.org/10.38043/jah.v8i1.6793>.
- Sekaring Ayumeida, Kusnadi, and Andy Usmina Wijaya. “PERLINDUNGAN HUKUM DATA PRIBADI SEBAGAI HAK PRIVASI.” *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (April 2021): 9–16. <https://doi.org/10.47776/alwasath.v2i1.127>.
- Simanjuntak, Predderics Hockop. “Perlindungan Hukum Terhadap Data Pribadi Pada Era Digital di Indonesia: Studi Undang - Undang Perlindungan Data Pribadi Dan General Data Protection Regulation (GDPR).” *Esensi Hukum* 6, no. 2 (June 2025): 105–24. <https://doi.org/10.35586/esensihukum.v6i2.412>.
- Sinaga, Erlina Maria Christin, and Mery Christian Putri. “Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0.” *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 2 (August 2020): 237. <https://doi.org/10.33331/rechtsvinding.v9i2.428>.



- Sitorus, Rolib, Joy Zaman, and Ricky Banke. "Kendala Pelaksanaan Perlindungan Data Pribadi." *Locus: Jurnal Konsep Ilmu Hukum* 5, no. 1 (March 2025): 53–61. <https://doi.org/10.56128/jkih.v5i1.438>.
- Sitorus, Rolib, Joy Zaman, Ricky Banke, Baqis Abelia Mita, Nasution Muhammad, Ayu, Sinta Sukma, Nasution Muhammad, et al. "Urgensi UndangUndang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia." *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia* 3, no. 2 (2022). <https://doi.org/10.52005/rechten.v3i2.78>.
- Suari, Kadek Rima Anggen, and I Made Sarjana. "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi di Indonesia." *Jurnal Analisis Hukum* 6, no. 1 (April 2023): 132–42. <https://doi.org/10.38043/jah.v6i1.4484>.
- Sukmawan, Yulia Audina, and Dwi Damayanti. "Metode Penelitian Hukum Normatif Dan Empiris Sebagai Strategi Penguatan Perspektif Kajian Ilmu Hukum." *Notary Law Journal* 4, no. 3 (2025): 114–28. <https://notarylaw.journal.ulm.ac.id/index.php/nolaj/article/view/116/72>.
- Thomas, Alejandro Morion Ruben, and Happy Yulia Anggraeni. "Cybercrime Dan Media Sosial: Analisis Hukum Terhadap Tren Peningkatan Tindak Pidana Di Era Digital." *Jurnal Hukum Lex Generalis* 6, no. 7 (2025): 1–22. <https://doi.org/10.56370/jhlg.v6i7.2173>.
- Wahyudi Djafar, Ruben Fritz, and Blandina Lintang Setianti. *Perlindungan Data Pribadi di Indonesia: Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia*. ELSAM, 2016.
- Wiraguna, Sidi Ahyar. "Metode Normatif Dan Empiris Dalam Penelitian Hukum: Studi Eksploratif di Indonesia." *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3, no. 3 (November 30, 2024). <https://doi.org/10.59818/jps.v3i3.1390>.