



DOI: <https://doi.org/10.38035/gijlss.v3i2>
<https://creativecommons.org/licenses/by/4.0/>

Legal Problems of Personal Data Protection in The Digital Era in Personal Data Protection Law in Indonesia

Indra Lutrianto¹, Riswadi²

¹Universitas Borobudur, Jakarta, Indonesia, lutriantoindra@gmail.com

²Universitas Borobudur, Jakarta, Indonesia, riswadi@borobudur.ac.id

Corresponding Author: lutriantoindra@gmail.com¹

Abstract: The rapid development of digital technology has brought significant changes in various aspects of life, including in the management of personal data. In Indonesia, the use of personal data is increasingly widespread, especially in the digital sector such as e-commerce, fintech, and social media. The condition increases the risk of data leakage and misuse so personal data protection becomes a crucial issue. To respond to these challenges, Indonesia has passed Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) which aims to provide legal protection for data owners and regulate data management mechanisms by data controllers. This investigation seeks to evaluate the PDP Law in Indonesia in the context of the digital era. The approach used in this study is the juridical-normative method with descriptive analysis. Data were obtained through literature studies that include analysis of laws and regulations and legal literature. In addition, it also conducts a study of case studies of data leakage in Indonesia to understand the implementation of regulations and the challenges faced in practice. The main focus of this study is to evaluate the effectiveness of the PDP Law in providing comprehensive protection for personal data and identifying obstacles in its enforcement. The results of this study are expected to provide deeper insight into the state of personal data protection in Indonesia and offer recommendations for improving regulations and data protection practices in the future.

Keywords: Technological Development, Personal Data, Personal Data Protection.

INTRODUCTION

In society, the era of modernization is developing rapidly, marked by relentless speed, efficacy, and efficiency in all aspects of life. The modernity concept has become an inevitable necessity in various fields of human endeavor, while alternative approaches are considered old-fashioned or conventional (Wibawa, 2016). The presence of digital technology in Indonesia has had a profound impact on various aspects of life. Digitalization has penetrated almost every sector, including communication, economy, education, and government (Adha, 2020). The presence of technologies such as the internet, social media, and digital-based applications has revolutionized the way individuals engage in activities and interact. In the economic sector, for example, e-commerce and fintech have experienced exponential growth, facilitating smooth and fast online transactions (Sopang, 2024). This phenomenon is further driven by the soaring

number of internet and mobile device users in Indonesia, which continues to show a very rapid growth trajectory every year. Digital transformation also presents great opportunities for innovation and the development of the national digital economy (Judijanto, 2024).

The increasing use of personal data in various sectors, such as e-commerce, fintech, and social media, is a consequence of the rapid digitalization in Indonesia. In the e-commerce sector, users' data, such as name, address, telephone number, and payment information, are an important part of the transaction process (Priliyasi, 2023). E-commerce service providers use this data to provide more personalized services, such as product recommendations or promotions that suit user preferences. The same thing also happens in the fintech sector, where personal data is used to verify identity, assess creditworthiness, and manage digital-based financial services. The existence of fintech services has made it easier for people to access financial products, such as online loans and digital wallets, which were previously difficult to reach (Setiyono, 2021).

However, the rapid development of digital technology also brings challenges, especially in terms of personal data security. People are increasingly dependent on digital technology and are often unaware of the risks of data leaks and misuse (Asari, 2023). Social media has become the main platform for the massive exchange of personal data. Users often unknowingly share personal information, such as location, habits, and interests, which can then be exploited by platforms for commercial purposes, such as behavioral advertising (Noorikhshan, 2023). Although this data helps improve users' digital experience, the risk of data misuse and leakage is increasing. Cases of data misuse by third parties for business or political interests are a serious warning of the importance of strict regulations in managing personal data (Sasongko, 2020). Therefore, the protection of personal data in the digital era must be a primary concern, especially for the government, technology companies, and users themselves.

METHOD

The research method used in this study is the juridical-normative method with a descriptive-analytical approach. The juridical-normative method emphasizes the study of legal norms contained in laws and regulations and various relevant legal literature. This study focuses on the analysis of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) in the context of data protection in the digital era. A descriptive approach is used to provide a comprehensive overview of the concepts, principles, and legal frameworks related to personal data protection in Indonesia. Primary data were obtained from a study of applicable laws and regulations in Indonesia, especially the PDP Law. This study also uses secondary data taken from scientific journals and books. The study was conducted to evaluate the effectiveness of existing regulations, identify legal barriers, and find solutions that can improve personal data protection in Indonesia. The analysis results are expected to contribute to the development of better policies and increase awareness of the importance of personal data protection in the digital era.

RESULT AND DISCUSSION

Personal Data Protection in the Personal Data Protection Law

Personal data protection in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is a legal effort aimed at protecting individual rights over their data amidst the rapid development of digital technology. The PDP Law defines personal data as any data about an individual that can be identified directly or indirectly through certain information, such as name, identity number, health data, financial information, and so on. This law gives individuals, referred to as data subjects, the right to have control over their data, including the right to know how their data is collected, used, and processed by the data controller (Sinaga, 2020).

One of the main elements in the PDP Law is the granting of rights to data subjects, which are regulated in Articles 5 to 12. These rights include the right to know the purpose and legal basis for collecting their data, the right to access and correct inaccurate data, the right to delete data under certain conditions, and the right to withdraw consent to the use of their data. In addition, data subjects also have the right to request information regarding third parties who access their data and the right to object to data processing for certain purposes, such as direct marketing. These rights aim to provide individuals with full control over their data, so as to prevent misuse of data by controllers or third parties (Nuhi, 2024).

On the other hand, the PDP Law also imposes strict obligations on data controllers and data processors. Articles 14 to 16 mandate that data controllers ensure lawful, transparent, and appropriate data collection, processing, and storage. Data controllers are required to implement appropriate technical and organizational measures to protect data from unauthorized access, leakage, or theft (Pranata, 2024). In the event of a data breach, Article 46 requires data controllers to immediately notify data subjects and relevant authorities within 72 hours of the incident being detected.

Furthermore, the PDP Law in administrative responsibilities includes sanctions for personal data breaches. These sanctions can be in the form of administrative sanctions, such as written warnings, temporary suspension of data processing activities, to administrative fines that can reach 2% of the annual income of the violating company, as stipulated in Article 55. Criminal sanctions are also stipulated in Articles 67 to 69, which include imprisonment of up to 6 years or a maximum fine of IDR 6 billion for perpetrators who intentionally disclose personal data for profit or cause harm to the data subject.

Obstacles and Solutions in the Implementation of Personal Data Protection in Indonesia

The effectiveness of personal data protection under the PDP Law depends on the content of its regulations and its effective implementation (Yolanda, 2023). The main challenges faced include limited digital literacy among the public and the lack of infrastructure and human resources needed for effective supervision and law enforcement. Many small and medium enterprises (SMEs) do not understand their responsibilities as data controllers, which has the potential to lead to unwitting violations of regulations (Erikha, 2025). Furthermore, the capacity of the supervisory agency to monitor the activities of thousands of data controllers throughout Indonesia is still an important area that needs to be improved.

The next obstacle is the absence of an independent agency specifically for personal data protection in Indonesia (Christine B. &, 2022). Article 58 of the PDP Law mandates the establishment of an agency to organize personal data protection. The personal data protection agency is responsible to the President and has fifteen authorities to organize personal data protection. Furthermore, Article 61 of the PDP Law mandates that provisions regarding the procedures for the authority to organize the agency will be further regulated in government regulations. However, because there is no government regulation as an implementing regulation for the PDP Law, the establishment of a special institution for personal data protection in Indonesia is hampered.

A personal data protection institution is critical in Indonesia, given the strong legal framework established by Article 58 of the Personal Data Protection Law. The institution is entrusted with the responsibility to supervise, maintain, and enforce individual privacy rights. In addition, they oversee the responsible use of personal data by personal data controllers. The main function of this institution is to ensure the security of personal data and maintain compliance with the standards set by the relevant laws. Thus, they aim to foster the trust of the Indonesian people in the responsible handling of personal data in the digital era (Christine B., 2021).

To ensure that the implementation of personal data protection runs effectively, it is necessary to strengthen and improve regulations, increase the capacity of supervisory institutions, digital education and literacy, and collaboration between the government and the community. Improvement of regulations is needed to ensure that Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) remains relevant to technological advances and international practices. The main reference for this purpose is the General Data Protection Regulation (GDPR) in the European Union, which has been established as the global standard for personal data protection. Improvements to the regulation may include modifications to the definition of sensitive data, regulations on cross-border data transfers, and enhanced user consent mechanisms. The regulation should also be accompanied by technical guidance for data controllers, allowing them to understand and apply appropriate protection standards according to their operational needs (Yudistira, 2023).

The supervisory institution regulated in Article 58 of the PDP Law, namely the Personal Data Protection Authority (OPDP), must have adequate capacity to carry out supervisory, law enforcement, and education functions. This capacity building includes the addition of competent human resources in the fields of data security, information technology, and cyber law. In addition, strengthening the technological infrastructure for OPDP is very important to monitor data breaches in real-time. This institution also needs to be equipped with stronger authority to conduct audits, impose sanctions, and handle complaints from the public effectively (Khansa, 2021).

Then, increasing public awareness is a crucial step in preventing misuse of personal data. Awareness campaigns must be carried out massively through various media, both online and offline. Campaign materials can include the dangers of data leaks, how to protect personal information, and steps to take in the event of a data breach. The government can work with the mass media, digital influencers, and the technology community to reach various levels of society (Satria, 2024). In addition, formal and informal education is also needed for digital users, including students, professionals, and the general public. This education can be in the form of digital security training, which includes techniques for creating secure passwords, identifying phishing attacks, and understanding their rights under the PDP Law. Conversely, companies, especially MSMEs, also need training on their obligations as data controllers. This training includes managing data according to security standards, handling data breach incidents, and ensuring transparency to their customers (Manurung, 2023).

Collaboration between various parties is also essential to create an effective data protection ecosystem. The government acts as a regulator and facilitator, while the private sector can contribute through technological innovations that strengthen data security. Civil society, including non-governmental organizations and digital communities, can play a role in monitoring and policy advocacy. This collaboration can be carried out through regular forums that discuss data protection issues, jointly handling data leak incidents, and creating common security standards that are applied in various sectors. It is also an important measure to mitigate cyber risks nationally. For example, the banking and fintech sectors can share data and experiences regarding the cyber threats they face with the government so that a more comprehensive security strategy can be developed. With the involvement of all parties, personal data protection can become part of a collective awareness that benefits all Indonesian people in this digital era (Azzani, 2023).

CONCLUSION

The digital era has brought about major transformations in various sectors of life, from communication, economy, to government. Digital technology, such as the internet and social media, has facilitated human activities and interactions, while e-commerce and fintech have driven the growth of the national digital economy by relying on users' data. However, rapid

digitalization has also increased the risk of personal data leaks and misuse, especially in the e-commerce, fintech, and social media sectors. Personal data used to provide personal services is also often exploited commercially by third parties without the user's knowledge. This situation shows the importance of strict data protection regulations and increasing digital literacy for the public so that they can protect their personal information.

The effectiveness of personal data protection in Indonesia is highly dependent on strong regulations and careful implementation, as stated in Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). The challenges faced include low digital literacy among the public, the limited capacity of supervisory institutions, and the absence of an independent body specifically tasked with overseeing personal data protection. To improve the effectiveness of data protection measures, it is essential to revise regulations by international standards, such as the General Data Protection Regulation (GDPR), increase the capacity of supervisory institutions, and provide digital education and literacy programs for the general public and businesses. Collaboration between the government, private sector, and civil society is essential in building a safe and trusted digital ecosystem. Through this initiative, it is hoped that incidents of data leaks and misuse can be reduced significantly, and public trust in the management of personal data can be realized effectively in this digital era.

REFERENCES

- Adha, L. A. (2020). Digitalisasi industri dan pengaruhnya terhadap ketenagakerjaan dan hubungan kerja di Indonesia. *Jurnal Kompilasi Hukum*, 5(2), 267-298.
- Sopang, F. I. (2024). PENYELESAIAN SENGKETA TRANSAKSI BISNIS DI ERA DIGITAL SECARA ONLINE (ONLINE DISPUTE RESOLUTION). *Bisnis-Net Jurnal Ekonomi dan Bisnis*, 7(1), 155-163.
- Judijanto, L. K. (2024). *Pengembangan Startup Digital: Referensi Sukses Memulai Bisnis Startup Digital Era Industri 4.0 dan Society 5.0*. Yogyakarta: PT Green Pustaka Indonesia.
- Wibawa, I. (2016). Era Digital (Pergeseran Paradigma Dari Hukum Modern Ke Post Modernisme). *Masalah-Masalah Hukum*, 45(4), 285-291.
- Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 12(2).
- Setiyono, W. P. (2021). *Buku Ajar Financial Technology*. Sidoarjo: Umsida Press.
- Asari, N. A. (2023). Peran Hukum Dalam Menanggapi Perubahan Sosial Dan Teknologi Di Era Revolusi Industri 4.0. *Mediation: Journal of Law*, 38-44.
- Noorikhshan, F. F. (2023). Dinamika Internet, Media Sosial, dan Politik di Era Kontemporer: Tinjauan Relasi Negara-Masyarakat. *Journal of Political Issues*, 5(1), 95-109.
- Sasongko, S. D. (2020). Konsep Perlindungan Hukum Data Pribadi dan Sanksi Hukum atas Penyalahgunaan Data Pribadi oleh Pihak Ketiga. *In Proceeding of Conference on Law and Social Studies*, 16-27.
- Sinaga, E. M. (2020). Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 9(2), 237.
- Nuhi, M. H. (2024). Tinjauan Hak Asasi Manusia terhadap Perlindungan Data Pribadi dan Kepastian Hukumnya di Indonesia. *National Conference on Law Studies (NCOLS)*, 6(1), 433-447.
- Pranata, A. J. (2024). Implementasi Asas Kehati-Hatian dalam Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi di Era Digital 5.0. *JOURNAL OF LAW AND NATION*, 3(3), 721-730.
- Yolanda, E. &. (2023). URGENSI LEMBAGA PELINDUNGAN DATA PRIBADI DI INDONESIA BERDASARKAN ASAS HUKUM RESPONSIF. *Journal of Syntax Literate*, 8(6).

- Erikha, A. &. (2025). Strategi Pencegahan Kebocoran Data Pribadi melalui Peran Kominfo dan Gerakan Siberkreasi dalam Edukasi Digital. *Jurnal Retentum*, 48-64.
- Christine, B. &. (2022). Hambatan Penerapan Perlindungan Data Pribadi di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Syntax Literate; Jurnal Ilmiah Indonesia*, 7(9), 16331-16339.
- Christine, B. (2021). Mandate of Procurement of Independent Commission for Personal Data Protection In Indonesia Reviewed from International Legal Instruments. *International Journal of Social Service and Research*, 1(2), 64-71.
- Yudistira, M. &. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO. *UNES Law Review*, 5(4), 3917-3929.
- Khansa, F. N. (2021). Penguatan Hukum dan Urgensi Otoritas Pengawas Independen dalam Pelindungan Data Pribadi di Indonesia. *Jurnal Hukum Lex Generalis*, 2(8), 649-662.
- Satria, M. K. (2024). Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Intelek Dan Cendikiawan Nusantara*, 1(2), 2442-2456.
- Manurung, J. S. (2023). Sosialisasi Dan Edukasi Tentang Keamanan Data Dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran Dan Perlindungan Masyarakat. *Jurnal Pengabdian Masyarakat Nauli*, 2(1), 1-7.
- Azzani, I. K. (2023). Urgensi peningkatan kesadaran masyarakat tentang kasus penipuan online berkedok kerja paruh waktu sebagai ancaman negara. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, 10(7), 3556-3568.