Implementing Law Number 27 of 2022 in Ensuring Personal Data Security on Digital Platforms (A Case Study of the Indonesian Sharia Bank Data Leak)

Graha Ananda Zugusti Lubis, Fitri Rafianti, Siti Nurhayati

Abstract

Advances in information technology have driven the transformation of digital banking services, but have also increased the risk of personal data breaches. One case of concern is the cyberattack on Bank Syariah Indonesia (BSI) in 2023, which disrupted banking services and raised concerns about customer data security. This study aims to analyze the implementation of Law Number 27 of 2022 concerning Personal Data Protection in ensuring the security of customer personal data through a case study of Bank Syariah Indonesia. The study uses normative legal methods with legislative, conceptual, and case approaches, and is analyzed qualitatively based on primary, secondary, and tertiary legal materials. The results show that Law Number 27 of 2022 provides an adequate legal basis for personal data protection, but its implementation is suboptimal due to weak cybersecurity governance and oversight of electronic system providers. In this context, Law Number 1 of 2024 concerning Electronic Information and Transactions supports law enforcement against perpetrators of cyberattacks, thus complementing the implementation of personal data protection. Therefore, strengthening the implementation of Law Number 27 of 2022, supported by law enforcement under the Electronic Information and Transactions (ITE) Law, is a crucial step in improving personal data security in the digital banking sector.

Keywords: *Personal Data Protection, Indonesian Sharia Bank, Digital Banking, Cybersecurity, Law Number 27 of 2022.*

Graha Ananda Zugusti Lubis
Master of Law Student, Universitas Pembangunan Panca Budi Medan, Indonesia
e-mail: grahaanandalubis@gmail.com

Fitri Rafianti, Siti Nurhayati
Lecturer in the Master of Laws program, Universitas Pembangunan Panca Budi Medan, Indonesia
e-mail: fitrirafianti@dosen.pancabudi.ac.id, sitinurhayati@dosen.pancabudi.ac.id.
2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era

Introduction

The rapid development of information and communication technology has driven significant digital transformation across various sectors of life, including the economy, education, government, healthcare, commerce, and social interactions. The utilization of digital platforms in daily activities, such as electronic transactions, social media, digital financial services, marketplaces, and cloud computing, has resulted in the increasing collection and processing of personal data by electronic system providers (Harto et al., 2023). Consequently, personal data has become a highly valuable asset while simultaneously being vulnerable to various forms of misuse.

The advancement of information technology has also transformed societal behavior in many aspects of life (Siti Nurbaiti & Anisa Rahma, 2019). From a legal perspective, personal data protection constitutes an effort to safeguard individual rights and promote social justice. Furthermore, within the perspective of Islamic law, the protection of personal information and individual dignity is regarded as part of preserving human honor (*hifz al-'irdh*), which must be respected by all parties (Rafianti, 2023). In line with this view, Rasjidi and Putra (1993) emphasized that law functions to create order, legal certainty, and justice within society. Therefore, the rapid growth of digital technology accompanied by increasing threats to personal information security necessitates legal instruments capable of providing effective protection.

In Indonesia, the growing use of the internet and digital platforms has provided significant convenience in accessing services quickly and efficiently (Setiawan, 2018). However, this development has also generated new challenges related to personal data protection. Various incidents involving data breaches, identity theft, misuse of personal information, and cyberattacks demonstrate that user data security remains a serious concern (Barus & Purba, 2025). Although several regulations have governed consumer protection in electronic transactions, violations of users' rights continue to occur frequently (Anjas Fahilly, Siti Nurhayati, & Fitri Rafianti, 2025).

The high risk of data breaches is reflected in a number of cases that have occurred in Indonesia. One case that demonstrates the importance of implementing personal data protection in the banking sector is the cyberattack experienced by PT Bank Syariah Indonesia Tbk (BSI) in May 2023. Service disruptions began on May 8, 2023, resulting in customer inability to use various banking services, such as BSI Mobile, ATMs, and electronic transactions, for several days. Initially, BSI attributed the disruption to system maintenance. However, several days later, it was revealed that the disruption was allegedly the result of a ransomware attack carried out by the LockBit 3.0 hacker group, which claimed to have accessed and stolen approximately 1.5 terabytes of BSI's internal data, allegedly including both customer and internal company data.

This case raises significant concerns because the banking sector, as an electronic system provider, manages a variety of highly sensitive personal data, such as customer identities, account numbers, transaction data, financial documents, and other information related to banking activities. Data leaks in this sector not only have the potential to cause financial losses for customers, but can also trigger identity theft, misuse of personal information, digital fraud (phishing), and reduce the level of public trust in the national banking system.

In response to the growing threat of personal data misuse, the Indonesian government enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This regulation represents Indonesia’s first comprehensive legal framework specifically governing personal data protection. The PDP Law is expected to provide legal certainty, enhance the accountability of data controllers and data processors, and strengthen the protection of privacy rights in the digital environment.

According to Gustav Radbruch’s theory of legal certainty, the law must provide certainty to ensure fair protection of individuals’ rights (Radbruch, 1932). Similarly, the principle of legal

certainty (*rechtszekerheid*) is one of the fundamental pillars of a state governed by the rule of law, requiring legal regulations to provide clear norms and avoid multiple interpretations (Dewi & SH, 2026). Furthermore, unclear legal provisions may create normative conflicts and hinder the effective implementation of the law (Irianto, Rafianti, & Siregar, 2024). Therefore, the PDP Law serves as an essential legal instrument in establishing a clear framework for personal data protection in Indonesia.

Nevertheless, the implementation of the PDP Law continues to face several challenges. Limited public awareness regarding the importance of personal data protection, inadequate cybersecurity standards among various digital platforms, and insufficient resources and information security infrastructure remain significant obstacles to the effective enforcement of the regulation (Huda et al., 2024). Moreover, the alleged leak of data belonging to 279 million Indonesian citizens, reportedly originating from the BPJS Kesehatan database, illustrates that the existence of regulations alone is insufficient to prevent data breaches without strong supervision and effective law enforcement mechanisms (ELSAM, 2021).

Based on these circumstances, examining the challenges in implementing Law Number 27 of 2022 is essential to assess the extent to which the regulation is capable of ensuring personal data security on digital platforms in Indonesia. This study is expected to contribute to the academic development of personal data protection law and provide recommendations for policymakers and electronic system providers in strengthening data security governance in the digital era.

Literature Review

2.1 Personal Data Protection

Personal data protection law is rooted in respect for the individual's right to privacy as a component of human rights. Personal data encompasses any data concerning an individual whether identified or identifiable, either in isolation or in combination with other information held in either electronic or non-electronic form (Hasibuan and Sendy, 2024).Personal data protection refers to the legal protection of an individual's right to privacy in the use of information and communication technology. In the digital era, personal data has become highly valuable because nearly all social activities are conducted through electronic systems and digital platforms (Yuniarti, 2019; Kurnianingrum, 2020). Personal data protection aims to ensure the security, confidentiality, and proper use of data so that it is not misused by unauthorized parties without the consent of the data owner (Saragih, Budhijanto, & Somawijaya, 2020).

2.2 Information Security

Information security refers to efforts to protect information from various threats that may compromise its confidentiality, integrity, and availability (Whitman & Mattord, 2006). According to the ISO/IEC 27002:2013 standard, information security functions to maintain organizational continuity, minimize risks, and protect information from various forms of threats (Amirinnisa, Bisma, & Kom, 2023).

The fundamental principles of information security are commonly known as the CIA Triad, consisting of confidentiality, integrity, and availability (Pratama, Syaiful, & Rahman, 2024). These three principles serve as the foundation for managing and protecting personal data on digital platforms.

2.3 Digital Platforms

A digital platform is an information technology-based system that enables users to interact, exchange information, and conduct electronic transactions through internet networks (Setiawan, 2018). According to Castells (2013), the development of information technology has created a network society, in which social and economic activities are highly dependent on digital technology and internet connectivity.

Digital platforms are characterized by the use of electronic systems, user data management, and internet-based interactions (Setiawan, 2018). Therefore, digital platform

providers have the responsibility to ensure the security and confidentiality of the user data they manage.

2.4 Law Number 27 of 2022 on Personal Data Protection

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is a specific regulation that comprehensively governs personal data protection in Indonesia (Rosadi, 2023). The enactment of this law aims to provide legal certainty, safeguard citizens' privacy rights, and enhance personal data security within electronic systems (Nasution & Harmika, 2025).

The PDP Law regulates the rights of data subjects, the obligations of data controllers and data processors, mechanisms for data processing, as well as administrative and criminal sanctions for violations of personal data protection provisions (Law No. 27 of 2022). According to Hadjon (2015), legal protection constitutes a form of recognition of human rights that must be guaranteed by the state. Therefore, the PDP Law serves as an important instrument in ensuring the protection of privacy rights in the digital era.

Research Methodology

The type of research used in this study is normative legal research with a normative juridical approach. Normative legal research is conducted by reviewing library materials or secondary data related to legislation, legal principles, legal theory, and expert opinions related to the research object (Soekanto, 2007). According to Soekanto (2011), normative legal research is research conducted on legal principles, legal systematics, the level of legal synchronization, legal history, and comparative law. This research focuses on the analysis of legal norms applicable in society. This research is descriptive and analytical in nature, aiming to systematically, factually, and accurately describe legal regulations related to personal data protection and analyze the effectiveness of their implementation in society (Ariawan, 2013).

This research uses a statute approach and a conceptual approach (Suhaimi, 2018). The legislative approach was conducted by examining various regulations related to personal data protection and electronic systems, such as Law Number 27 of 2022 concerning Personal Data Protection and the Electronic Information and Transactions Law (Maftukhin, 2025). Meanwhile, a conceptual approach was used to examine theories, legal principles, and expert opinions regarding legal effectiveness, legal protection, privacy rights, and digital information security.

Data sources consisted of primary, secondary, and tertiary legal materials derived from laws and regulations, scientific books, journals, articles, previous research results, and other relevant literature. Data collection techniques were conducted through a review of various legal documents and literature related to personal data protection.

The data analysis technique used was qualitative analysis, which involved identifying, categorizing, and analyzing data based on legal theory and relevant legislation. The results of the analysis were then presented descriptively to illustrate the effectiveness of Law Number 27 of 2022 in ensuring the security of personal information on digital platforms in Indonesia..

Results and Discussion

4.1 Implementation of Law Number 27 of 2022 on Personal Data Protection in the Bank Syariah Indonesia Data Breach Case

The rapid advancement of information technology has accelerated the digital transformation of the banking sector, enabling financial institutions to provide more efficient and accessible services. However, this transformation has also increased the risk of personal data breaches and cyberattacks. Customers' personal data, including identity information, financial records, and transaction histories, constitute valuable assets that require comprehensive legal protection. Consequently, the enactment of Law Number 27 of 2022 on

Personal Data Protection (PDP Law) represents a significant milestone in strengthening the legal framework for personal data protection in Indonesia.

Under the PDP Law, banks are categorized as Personal Data Controllers, meaning they determine the purposes and means of processing customers' personal data. As Personal Data Controllers, banks are legally obligated to implement appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of personal data. They are also responsible for preventing unauthorized access, unlawful disclosure, misuse of personal data, and notifying affected data subjects in the event of a personal data breach.

The implementation of these legal obligations can be examined through the cyberattack against PT Bank Syariah Indonesia Tbk (BSI) in May 2023. The ransomware attack, allegedly conducted by the LockBit 3.0 group, disrupted mobile banking services, ATMs, and electronic transactions for several days. The attackers claimed to have accessed approximately 1.5 terabytes of BSI's internal data, including customer information, account records, internal documents, and transaction data. Although BSI confirmed that customers' funds remained secure, the incident demonstrated the vulnerability of personal data protection within Indonesia's digital banking sector.

From the perspective of legal implementation, the BSI incident indicates that although Law Number 27 of 2022 has established comprehensive legal obligations regarding personal data protection, its implementation has not yet been fully effective. The incident highlights deficiencies in cybersecurity governance, information security management, and institutional preparedness to prevent and respond to cyber threats. Therefore, effective implementation of the PDP Law requires not only compliance with statutory provisions but also continuous improvement of cybersecurity infrastructure, risk management systems, and organizational accountability.

4.2 The Relationship Between Law Number 27 of 2022 and Law Number 1 of 2024 on Electronic Information and Transactions

Although this study primarily focuses on the implementation of the Personal Data Protection Law, the BSI cyberattack also demonstrates the relevance of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (EIT Law). The two laws have different legal objectives but complement each other in addressing cyber incidents involving personal data. Both laws have different but complementary functions:

Law Number 27 of 2022 (Personal Data Protection Law)	**Law Number 1 of 2024 (Electronic Information and Transactions Law)**
Protects the rights of personal data subjects	Prosecutes cybercrime offenders
Regulates the obligations of Personal Data Controllers	Regulates unauthorized access to electronic systems
Governs the protection and security of personal data	Regulates the protection of electronic systems
Provides administrative and criminal sanctions for violations of personal data protection	Provides criminal sanctions for cyberattacks and electronic system offenses

Source: Data Processed by the Author 2026

Law Number 27 of 2022 emphasizes the protection of personal data subjects by regulating the responsibilities of Personal Data Controllers and Processors. In contrast, the EIT Law focuses on preventing and prosecuting cybercrimes, including unauthorized access to electronic systems, illegal interception of electronic information, disruption of electronic systems, and unlawful use of electronic data.

In the BSI case, the alleged ransomware attack involved unauthorized access to electronic systems and the unlawful acquisition of electronic information, which fall within the scope of criminal provisions under the EIT Law. Meanwhile, the responsibility of BSI as a Personal Data

Controller remains governed by the Personal Data Protection Law. Accordingly, the PDP Law provides legal protection for customers whose personal data are processed by financial institutions, whereas the EIT Law serves as the legal instrument for prosecuting perpetrators responsible for cyberattacks.

The relationship between these two legal instruments illustrates that effective personal data protection cannot rely solely on data protection regulations. Instead, it requires a comprehensive legal framework that combines preventive measures under the PDP Law with criminal law enforcement mechanisms provided by the EIT Law.

4.3 Analysis of the Implementation of Personal Data Protection in the Digital Banking Sector

The cyberattack on Bank Syariah Indonesia (BSI) demonstrates that the implementation of Law Number 27 of 2022 on Personal Data Protection has not yet been fully effective in ensuring the protection of customers' personal data within Indonesia's digital banking sector. Although the law establishes clear legal obligations for Personal Data Controllers to safeguard personal data through appropriate technical and organizational measures, the incident indicates that compliance with these obligations remains a significant challenge. The disruption of banking services and the alleged exposure of customers' personal information reveal that cybersecurity governance and information security management require further improvement.

From a legal perspective, the implementation of the Personal Data Protection Law extends beyond the existence of statutory provisions. Its effectiveness depends on the commitment of financial institutions to adopt comprehensive data protection policies, conduct regular cybersecurity risk assessments, strengthen information security infrastructure, and ensure compliance with applicable legal standards. As Personal Data Controllers, banks are expected to apply the principles of accountability, transparency, and security throughout the entire process of collecting, processing, storing, and transferring personal data.

Furthermore, the BSI case illustrates that personal data protection should be supported by effective law enforcement against cybercrime. In this regard, Law Number 1 of 2024 concerning Electronic Information and Transactions (EIT Law) complements the implementation of the Personal Data Protection Law by providing criminal sanctions for unauthorized access to electronic systems, unlawful acquisition of electronic information, and cyberattacks against electronic systems. Therefore, the integration of the Personal Data Protection Law and the EIT Law creates a more comprehensive legal framework that not only protects the rights of data subjects but also strengthens legal enforcement against cyber offenders.

Overall, the implementation of Law Number 27 of 2022 requires stronger institutional oversight, continuous enhancement of cybersecurity capabilities, and effective coordination among regulators, financial institutions, and law enforcement agencies. Such measures are essential to improve legal certainty, strengthen public trust in digital banking services, and ensure effective protection of personal data in Indonesia's increasingly digital financial ecosystem.

Conclusion

The implementation of Law Number 27 of 2022 on Personal Data Protection has established a comprehensive legal framework for protecting customers' personal data in Indonesia's digital banking sector by regulating the rights of data subjects and the obligations of Personal Data Controllers. However, the cyberattack on Bank Syariah Indonesia (BSI) demonstrates that the implementation of the law has not yet been fully effective due to challenges in cybersecurity governance, information security management, and supervision of Electronic System Operators. In addressing such incidents, Law Number 1 of 2024 concerning Electronic Information and Transactions complements the Personal Data Protection Law by providing legal mechanisms to prosecute unauthorized access to electronic systems and cyber-

related offenses. Therefore, strengthening the implementation of Law Number 27 of 2022, supported by effective law enforcement under the EIT Law, is essential to enhance personal data protection, improve cybersecurity resilience, and maintain public trust in Indonesia's digital banking services.

References

[1] Amirinnisa, M., Bisma, R., Kom, S., & Kom, M. (2023). Analysis of Information Security Risk Assessment Based on ISO 27005 for Preparation for ISO 27001 Certification in The Government of Madiun City. *Journal of Emerging Information Systems and Business Intelligence (JEISBI)*, 4(4), 47–58.

[2] Andiza, D., Nurhayati, S., & Sebayang, S. (2023). Pengalihan Hak Cipta Buku Menurut Hukum Waris Perdata Di Indonesia. *INNOVATIVE: Journal Of Social Science Research*, 3(6), 4308–4322.

[3] Anggriawan, F., & Hasugian, L. P. (2017). *Platform Build-Me: Mempertemukan Stakeholder Bangunan dengan Konsumen*.

[4] Ariawan, I. G. K. (2013). Metode Penelitian Hukum Normatif. *Kertha Widya*, 1(1).

[5] Badan Pemeriksa Keuangan Republik Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024

[6] Badan Pemeriksa Keuangan Republik Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. https://peraturan.bpk.go.id/details/229798/uu-no-27-tahun-2022

[7] Barus, R. M., & Purba, D. R. (2025). Analisis Risiko Cybercrime pada Layanan Shopee PayLater dan Implikasi terhadap Keamanan Data Pengguna. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(6), 11523–11533.

[8] Castells, M. (2013). *Communication Power*. Oxford University Press.

[9] Dewi, P. M. (2026). Prinsip dan Asas dalam Perancangan Hukum. *Legal Drafting*.

[10] Dhianty, R. (2022). Kebijakan Privasi (Privacy Policy) dan Peraturan Perundang-Undangan Sektoral Platform Digital vis a vis Kebocoran Data Pribadi. *Scripta: Jurnal Kebijakan Publik dan Hukum*, 2(1), 186–199.

[11] Fitri Rafianti. (2023). *Buku Ajar Hukum Islam*. Eureka Media Aksara.

[12] Hadjon, P. M. (2015). Peradilan Tata Usaha Negara dalam Konteks Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan. *Jurnal Hukum dan Peradilan*, 4(1), 51–64.

[13] Harto, B., Rukmana, A. Y., Subekti, R., Tahir, R., Waty, E., Situru, A. C., & Sepriano, S. (2023). *Transformasi Bisnis di Era Digital: Teknologi Informasi dalam Mendukung Transformasi Bisnis di Era Digital*. PT Sonpedia Publishing Indonesia.

[14] Hasibuan, E. N. S., & Sendy, B. (2024). Analisis Perlindungan Hukum terhadap Perdagangan Manusia Melalui Vidio Platform Media Sosial. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, 11(1), 451–461.

[15] Huda, H. U. N., Astaruddin, H. T., Nasution, M. I., dkk. (2024). *Data Pribadi, Hak Warga, dan Negara Hukum: Menjaga Privasi di Tengah Ancaman Digital*. Penerbit Widina.

[16] Hukumonline. *Pasal 28A sampai 28J UUD 1945*. https://www.hukumonline.com/berita/a/pasal-28a-sampai-28j-uud-1945-lt642a9cb7df172/

[17] Hukumonline. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. https://learning.hukumonline.com/wp-content/uploads/2023/07/Undang-Undang-No.27-Tahun-2022-Hukumonline.pdf

[18] Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.
[19] Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.
[20] Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
[21] Irianto, A. R., Fitri Rafianti, & Siregar, M. A. (2024). Juridical Analysis of the Land Bank Agency as a Land Provider Institution for the Government in Implementing Agrarian Reform. Dalam *Proceedings of the 2nd International Conference on the Epicentrum of Economic Global Framework (ICEEGLOF)* (hlm. 446–452).
[22] Kompasiana. *Kasus Hukum Ekonomi Syariah: Kebocoran Data Nasabah Bank Syariah Indonesia (BSI)*. https://www.kompasiana.com/22_pinarahmadani2541/66fb78e134777c658c7c16f2/kasus-hukum-ekonomi-syariah-kebocoran-data-nasabah-bank-syariah-indonesia-bsi
[23] Kurnianingrum, T. P. (2020). Urgensi Pelindungan Data Pribadi Konsumen di Era Ekonomi Digital. *Kajian*, 25(3), 197–216.
[24] Lembaga Studi dan Advokasi Masyarakat (ELSAM). (2021). *Dugaan Kebocoran 279 Juta Data Pribadi Penduduk: Makin Pentingnya Akselerasi Pengesahan RUU Perlindungan Data Pribadi*.
[25] LK2 FHUI. *Bank Syariah Indonesia Pasca Serangan Siber: Mengungkap Potensi Kompensasi bagi Nasabah*. https://lk2fhui.law.ui.ac.id/portfolio/bank-bsi-pasca-serangan-siber-mengungkap-potensi-kompensasi-bagi-nasabah/
[26] Maftukhin, M. (2025). Sidang Perceraian Hakim Tunggal: Tinjauan Hukum terhadap Pelaksanaan Sidang Perceraian oleh Hakim Tunggal di Pengadilan Agama Rembang. *Suloh: Jurnal Fakultas Hukum Universitas Malikussaleh*, 13(2), 347–364.
[27] Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen oleh Penyelenggara Sistem Elektronik dalam Transaksi Digital. *Jurnal USM Law Review*, 7(1), 333–347.
[28] Mumtaz, A. (2024). *Asesmen Risiko Keamanan Informasi Sistem Informasi Penerimaan Mahasiswa pada STT-NF dengan SNI ISO/IEC 27001:2022* (Tesis, Sekolah Tinggi Teknologi Terpadu Nurul Fikri).
[29] Muzakkie, S. A., & Juarsa, E. (2023). Perlindungan Hukum terhadap Penyalahgunaan Data Pribadi pada Aplikasi Pinjaman Online Ilegal Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dalam *Bandung Conference Series: Law Studies*, 3(2), 984–987.
[30] Nasution, E. R., & Harmika, Z. (2025). Perlindungan Hukum terhadap Nasabah Bank yang Mengalami Kebocoran Data Pribadi Ditinjau dari Undang-Undang Nomor 27 Tahun 2022. *Innovative: Journal of Social Science Research*, 5(4), 11373–11384.
[31] Prananingrum, L., Wahab, S. R., Supriyanto, B. F., dkk. (2025). *Pengantar Teknologi Informasi dan Komunikasi*. Yayasan Tri Edukasi Ilmiah.
[32] Pratama, A. M., Syaiful, M., & Rahman, M. F. (2024). *Keamanan Data dan Informasi*. Kaizen Media Publishing.
[33] Radbruch, G. (1932). *Legal Philosophy*.
[34] Rahardjo, S. (2006). *Membedah Hukum Progresif*. Penerbit Buku Kompas.
[35] Rasjidi, L., & Putra, I. W. (1993). *Hukum sebagai Suatu Sistem*. Remaja Rosdakarya.
[36] Rizana, R. H., & Nasution, A. R. (2024). Perlindungan Hukum Terhadap Hak Cipta Lagu Berdasarkan Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta (Studi Kasus Putusan MA Nomor: 505 K/Pdt.Sus-HKI/2021). *GOVERNANCE: Jurnal Ilmiah Kajian Politik Lokal dan Pembangunan*, 10(3).
[37] Salman, H. O. (2010). *Legal Philosophy (Development and Dynamics of Problems)*. PT Refika Aditama.

[38] Saragih, L. K., Budhijanto, D., & Somawijaya, S. (2020). Perlindungan Hukum Data Pribadi terhadap Penyalahgunaan Data Pribadi pada Platform Media Sosial Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. *Jurnal Hukum De'Rechtsstaat*, 6(2), 125–142.
[39] Saragih, Y. M., & Azis, D. A. (2020). Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi. *Soumatera Law Review*, 3(2), 265–279.
[40] Sekretariat Kabinet Republik Indonesia. *Perlindungan Hak Asasi Digital*. https://setkab.go.id/perlindungan-hak-asasi-digital/
[41] Setiawan, A. B. (2018). Revolusi Bisnis Berbasis Platform sebagai Penggerak Ekonomi Digital di Indonesia. *Masyarakat Telematika dan Informasi*, 9(1), 61.
[42] Sidauruk, H. B., Maharani, H. P., & Syafitri, N. Q. (2025). Peranan Cybersecurity dalam Meningkatkan Ketahanan Bisnis Digital terhadap Cybercrime di Indonesia. *Jurnal Ilmu Ekonomi dan Bisnis*, 3(2), 8–17.
[43] Sitorus, R., Saragih, J. Z. F., & Banke, R. (2025). Kendala Pelaksanaan Perlindungan Data Pribadi. *Locus: Jurnal Konsep Ilmu Hukum*, 5(1), 53–61.
[44] Soekanto, S. (2007). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. RajaGrafindo Persada.
[45] Suhaimi. (2018). Problem Hukum dan Pendekatan dalam Penelitian Hukum Normatif. *Jurnal Yustitia*, 19(2).
[46] Susanti, D. O., & Efendi, A. A. (2022). *Penelitian Hukum: Legal Research*. Sinar Grafika.
[47] Westin, A. F. (1968). Privacy and Freedom. *Washington and Lee Law Review*, 25(1), 166.
[48] Yudhawasthi, C. M. (2023). Dokumen dalam Perspektif Ilmu Komunikasi. *BACA: Jurnal Dokumentasi dan Informasi*, 43–58.
[49] Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, 1(1), 147–154.