LEGAL BRIEF
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 14, No. 6, 2026, pp. 1392-1401
Published by: IHSA Institute (Institut Hukum Sumberdaya Alam)

The Effectiveness of Law Number 27 of 2022 Concerning Personal Data Protection in Combating Cybercrime in Indonesia

Teguh Satria Putra Pratama Sihotang[1], Elvira Dewi Ginting[2]

[1,2]Universitas Islam Negeri Sumatera Utara , Sumatera Utara, Indonesia

Abstract: The development of information technology brings new challenges to personal data protection in the digital world. This study aims to evaluate the effectiveness of personal data protection policies in Indonesia in preventing and addressing cybercrime. Using a qualitative approach and normative-empirical research, this study combines a doctrinal analysis of the legal framework stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) with secondary data analysis in the form of reports, scientific journals, and cybercrime statistics. The results show that although the PDP Law represents a step forward in digital privacy protection, its implementation still faces significant challenges, such as weak law enforcement, a lack of supporting facilities, and low public awareness. The functional analysis in this study highlights the need for institutional strengthening, increased digital literacy, and the development of an independent monitoring system to ensure the effectiveness of personal data protection in Indonesia. This research is expected to provide constructive recommendations for improving national policies on personal data protection and strengthening digital social control to prevent cybercrime.

Keywords: Cyber Crime, Effectiveness, Personal Data Protection, PDP Law, Regulation.

1. Introduction

The development of digital technology has made personal data management increasingly complex. While data utilization facilitates ease of service, it also opens up opportunities for misuse of personal information. This is where personal data protection becomes a fundamental necessity, ensuring that everyone maintains control over their digital identity. The government has responded to this situation through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which serves as the primary legal umbrella for maintaining the confidentiality, use, and security of public data (Ramadhani, 2021).

Although the PDP Law represents a step forward, its implementation on the ground has not been fully effective. Challenges such as weak law enforcement, limited coordination between institutions, a lack of skilled human resources, and low public awareness remain frequent obstacles. This situation is further exacerbated by the increasing threat of cybercrime from year to year (Aji, 2023). Data shows that cyberattacks in Indonesia surged from 290 million attacks in 2019 to 495 million in 2020, then again to more than 741 million attacks in just the first seven months of 2021. This surge demonstrates that existing regulations often lag behind the rapid development of digital crime methods (Christianingrum, 2020).

Not only is the number of attacks increasing, but their impact is also broader. According to a report on the level of cybercrime in Indonesia, economic losses due to cyber incidents reached USD 34.2 billion in 2017, or approximately 3.7% of national GDP. Online fraud, identity theft, and data breaches pose a real threat to society and the country. At the same time, Indonesia's position in the global cybersecurity index remains suboptimal, indicating gaps that need to be addressed in the national data protection system (Christianingrum, 2020).

The increasing misuse of personal data and cybercrime in Indonesia demonstrates the urgent need for legal protection for personal data. Various forms of cybercrime, such

Correspondence:
Name: Teguh Satria Putra Pratama Sihotang
Email: teguh0206212045@uinsu.ac.id

Received: Jan 30, 2026;
Revised: Feb 02, 2026;
Accepted: Feb 09, 2026;
Published : Feb 28, 2026;

as data theft, digital fraud, threats, illegal access, and information manipulation, are regulated through several provisions of the Criminal Code, such as Article 362 on theft and Article 378 on fraud, as well as through articles in the Electronic Information and Transactions (ITE) Law, including Articles 27, 28, 29, 30, 31, 35, and 36, which regulate the distribution of harmful content, the spread of false information, threats, unauthorized access, wiretapping, and the manipulation of electronic data. However, the cross-border and increasingly complex nature of cybercrime means that existing regulations are not yet fully capable of providing effective protection. The enactment of the Personal Data Protection Law is an important step towards strengthening digital security, but the effectiveness of its implementation still requires in-depth study. Therefore, this study focuses on the extent to which personal data protection regulations can play a role in preventing and suppressing cybercrime, while also assessing their relationship with existing criminal provisions (Situmeang, 2020).

In recent years, Indonesia's digital space has exhibited increasingly serious threat dynamics. Since the implementation of personal data protection regulations in 2022, there was hope that cyber incidents would decrease. However, in reality, attacks have actually increased in intensity. At the national level, threat activity monitored throughout 2024 showed a significant escalation. Various attack categories, such as ransomware, phishing, vulnerability exploitation, and even Advanced Persistent Threat Group (APT) activity, which targets high-value targets, continue to dominate. This increase is evident in the ever-increasing volume of anomalous traffic, illustrating that malicious activity on the Indonesian internet shows no signs of slowing.

Based on monitoring results from the BSSN (National Cyber and Crypto Agency) throughout 2024, Indonesia's cybersecurity situation showed a significant spike in attack activity. Throughout the year, 330,527,636 anomalous cyber attack traffic was recorded, indicating the high intensity of attempted attacks on the national digital space. The most attack activity occurred in the Mirai Botnet category (internet devices infected with malicious software called Mirai), with 81,286,596 activities, indicating that IoT (Internet of Things) devices, namely physical devices for collecting and exchanging data in real-time via the internet network, in Indonesia remain easy targets for large-scale automated attacks. Furthermore, activity from the Advanced Persistent Threat (APT) group also remained intense with 2,487,041 activities, followed by 514,508 ransomware activities and 26,771,610 phishing activities that have the potential to become entry points for further attacks. Cyber intelligence monitoring also recorded 241 suspected data breach incidents, while public content monitoring detected 5,780 web defacement incidents (cyber attacks that alter the appearance of a website without the owner's permission) throughout the year (Indonesian Cybersecurity Landscape, 2024).

This data shows that despite the implementation of personal data protection policies, Indonesia's digital space remains under significant pressure. The surge in anomalous traffic and the increasing number of attacks indicate that cyber threats are evolving faster than many agencies are prepared to secure their systems.

A similar situation was also seen in the central government's digital systems. Throughout 2024, more than 2,117 gigabytes of anomalous traffic were recorded, with the highest spike reaching 491.4 gigabytes in just one month. The number of attacks identified was also significant. Over the course of the year, 27 cyber incidents had to be addressed, most of which involved malicious file insertion, occurring 14 times. The increase in requests for security checks through vulnerability testing also indicates that more government applications are at risk. In one month, the number of vulnerability testing requests reached 80, reflecting significant concern about potential exploitation (Kominfo-CSIRT Annual Report, 2024).

Compared to the period before the personal data protection regulations came into effect, this threat pattern indicates that cyberattacks in Indonesia have not significantly decreased. Despite the now clearer legal framework, technical implementation at the organizational level remains uneven. System vulnerabilities, lack of early detection, weak internal security practices, and low digital awareness among service providers mean that

the regulations have not yet had a significant impact on reducing the number of attacks. In other words, despite the presence of regulations as a strong legal framework, on-the-ground conditions indicate that cyber challenges are increasingly complex and require far more thorough preparedness from digital service providers.

Given these conditions, it can be concluded that the effectiveness of personal data protection in Indonesia is determined not only by the existence of regulations, but also by the readiness of the systems implementing them. Increasing attack data—both in terms of the number of incidents and the magnitude of anomalous traffic—is a sign that the journey towards a secure digital ecosystem remains long. Efforts to strengthen technical security, improve human resource competency, and more consistent enforcement remain urgently needed to ensure that existing regulations can truly provide real protection for the public.

These facts reinforce the importance of this research. This study aims to assess whether the PDP Law is truly capable of protecting the public and reducing cybercrime, as well as the extent to which existing regulations need to be updated to align with the dynamics of transnational digital threats. By understanding implementation barriers and examining the effectiveness of oversight and sanction mechanisms, this study is expected to provide a clearer picture of the need for reform of Indonesian criminal law in the face of the rapidly evolving era of cybercrime.

Various previous studies have extensively discussed personal data protection, but most remain normative and comparative. Ariesta's 2024 study, "Comparative Study of Legal Protection of Personal Data in the European Union and Indonesia under the Principle of the Right to Be Forgotten," and Ramadhani's 2021 study, "Comparative Regulations on Personal Data Protection in Indonesia and the European Union," for example, focused on comparing Indonesian and European Union regulations, particularly regarding the definition of personal data, the right to be forgotten mechanism, the monitoring system, and the sanction model. These studies are important for assessing Indonesia's global standing, but their focus remains on written regulations. Meanwhile, research by Prabowo, Wibawa, and Azmi conducted in 2020 entitled "Cyber Personal Data Protection in Indonesia" further highlights the weaknesses of data protection in Indonesia before the PDP Law, emphasizing the issue of data leak risks and Indonesia's position in the world cybersecurity index. (Ariesta, 2024) (Ramadhani, 2021) (Prabowo, 2020).

Unlike those studies, this study presents a more practical and evaluative orientation. Its primary focus is no longer simply comparing regulations or outlining normative weaknesses, but rather assessing the extent to which Law Number 27 of 2022 concerning Personal Data Protection is actually implemented in practice, particularly in preventing and addressing cybercrime. This study addresses more factual issues, such as the lack of an independent oversight body, weak coordination between agencies, low public digital literacy, and the suboptimal infrastructure such as the Intrusion Detection and Prevention System (IDPS), a technology that monitors networks and detects and automatically blocks malicious activity. By directly examining implementation barriers and their impact on the rise of cybercrime, this study provides a novel contribution in the form of empirical evaluation while emphasizing the urgency of criminal law reforms that are more adaptive to the development of transnational digital crime.

In the national cyber law study map, this research positions itself in the realm of empirical evaluation of the effectiveness of personal data protection laws, which still receive relatively little attention compared to normative and comparative-normative studies. Unlike previous studies that focused on the substantive compliance of Law No. 27 of 2022 on Personal Data Protection (PDP Law) with international standards, this study assesses the extent to which these norms function in practice to prevent and address cybercrime. By linking legal norms to factual data on cyberattack trends, institutional readiness, digital security infrastructure, and the level of public compliance and digital literacy, this study contributes to the development of empirically-based law by placing law in action. The academic urgency of this research lies in revealing the gap between the normative objectives of the PDP Law and the reality of its implementation such as the

absence of an independent supervisory authority and weak law enforcement which shows that the existence of regulations does not automatically guarantee the effectiveness of personal data protection amid the transnational and evolving dynamics of cybercrime.

2. Materials and Methods

This study uses a qualitative approach with descriptive analysis to evaluate the effectiveness of personal data protection policies in Indonesia, specifically the implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), in preventing and addressing cybercrime. The research method employed is normative legal research enriched with empirical data, so that the analysis focuses not only on written legal provisions but also on the actual conditions and developments in digital security in Indonesia. The research data sources consist of laws and regulations, scientific literature, official reports, academic articles, and the latest statistics and findings on national cybercrime trends, including information on the frequency of attacks, economic losses, and Indonesia's position in the global cybersecurity index. Data collection was conducted through literature review and analysis of various relevant written sources. All data were then analyzed evaluatively based on indicators of legal effectiveness, such as clarity of norms, level of enforcement, compliance of data controllers, adequacy of supporting facilities, and their impact on reducing cybercrime rates. To ensure the validity of the findings, the study employed triangulation techniques by comparing the results of legal studies, academic publications, and empirical data from various national reports. This research analysis is based on several key theories. Soerjono Soekanto's Theory of Legal Effectiveness is used to assess the extent to which the law is effective in society, because effectiveness is not only determined by the existence of norms, but also by their implementation, compliance, and support from supporting structures. (Badri, 2021). Maskun's theory of cybercrime provides a framework for understanding the characteristics of digital crime which is transnational, anonymous, and difficult to trace, thus requiring an adaptive legal response. (Umbara, 2022). Meanwhile, Jeremy Bentham's theory of legal utility is used to assess whether personal data protection laws actually bring benefits to society, especially in minimizing risks and increasing the sense of security in the digital space. (Noorsanti, 2023). Through the use of these theories, this study seeks to provide a comprehensive picture of the strengths and weaknesses of the implementation of the PDP Law in dealing with the dynamics of cybercrime in Indonesia.

3. Results and Discussion

3.1. *Lack of Cybersecurity Institutions and Technology is a Barrier to the Implementation of the Personal Data Protection Law*

In terms of objectives and legal principles, the PDP Law emphasizes the importance of protecting personal data as part of citizens' constitutional rights, as stated in Article 1, point (2), and is regulated based on legal principles such as legal certainty, prudence, and responsibility (Articles 2 and 3). These principles serve as the normative foundation that guides all personal data protection policies and mechanisms in Indonesia.

In terms of definition and scope, the PDP Law provides explanations of key terms such as personal data, data controller, processor, and data subject (Article 1, paragraphs 1–10), and establishes the legal scope applicable to all parties, both domestic and international, who process Indonesian citizens' data (Article 2, paragraphs 1–2). These provisions demonstrate that the PDP Law has an extraterritoriality principle that provides protection for citizens' data even if it is processed outside of Indonesian jurisdiction.

Regarding data subject rights, the PDP Law, through Articles 5–15, provides individuals with various rights, such as the right to know, the right to access, the right to correction, the right to erasure, the right to withdraw consent, and the right to object to automated processing. These rights are intended to give data subjects full control over their personal information and strengthen the public's legal standing against potential data misuse.

Regarding the legal basis for data processing, the PDP Law (Articles 20–24) establishes six legal bases: consent, contract, legal obligation, vital interests, public duty, and legitimate interests. These provisions aim to ensure that all data processing is carried out with clear legitimacy, thereby reducing the risk of misuse.

The obligations of data controllers and processors are explicitly set out in Articles 27–32, which require them to maintain data accuracy, transparency, and security, as well as to record processing activities. Article 16 emphasizes the obligation to protect data from unauthorized access, unauthorized disclosure, and data manipulation.

In terms of handling violations, the PDP Law stipulates that controllers are required to notify data subjects of any violations (Articles 35–36) and grant data subjects the right to sue or seek compensation (Article 12). However, to date, the independent supervisory body mandated in Articles 58–59 has not been established, resulting in suboptimal oversight and law enforcement.

The handling of data breaches under the PDP Law remains general. Article 16 states that controllers are obliged to maintain data security and are responsible for any failure to protect personal data. However, there are no specific provisions regarding the reporting time for breaches or the obligation to notify data subjects. Reporting mechanisms and administrative sanctions will be further regulated by a supervisory body that has not yet been formally established.

Sanctions under the PDP Law include both administrative and criminal sanctions. Perpetrators who intentionally disclose, use, or falsify personal data without authorization can face up to six years in prison or a fine of up to IDR 6 billion. Additionally, controllers can be subject to administrative sanctions in the form of warnings, temporary suspension of activities, deletion of data, and administrative fines of up to 2% of annual revenue. Law enforcement involves the police and the prosecutor's office.

The PDP Law stipulates the need for data security controls, including against unauthorized access and misuse. However, the law's cybersecurity approach lacks technical details, such as the use of encryption or pseudonymization. Furthermore, there are no explicit provisions regarding system oversight, security audits, or comprehensive information technology risk management.

Sanctions under the PDP Law include both criminal and administrative sanctions. Intentional violations are punishable by up to six years' imprisonment or a fine of up to six billion rupiah (Articles 67–70). Additionally, controllers may be subject to administrative sanctions such as warnings, temporary suspension of activities, deletion of data, and administrative fines of up to 2% of annual revenue (Susanto, 2025).

Although this regulation contains important principles and provisions, its implementation still faces various obstacles. These include: the lack of an independent

oversight body responsible for monitoring, auditing, and imposing sanctions in an accountable manner; limited digital security infrastructure, including the suboptimal operation of the Indonesia Data Protection System (IDPS), which should function to detect and mitigate data leaks in real time; a lack of digital literacy among the public, resulting in many users not understanding their rights as data subjects and how to protect their personal information; and a lack of integrated coordination between agencies in handling data breaches and cybercrime incidents.

The effectiveness of the Indonesian legal system in resolving personal data breaches and combating cybercrime can be analyzed using a functional approach. This approach emphasizes how existing regulations address issues on the ground, not just at the level of written norms.

In the context of personal data breaches, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) provides a fairly clear legal framework for digital privacy protection. This regulation contains provisions regarding the rights of data subjects, the obligations of data controllers and processors, criminal and administrative sanctions, and mechanisms for handling violations. However, in terms of implementation, various obstacles remain, such as a suboptimal incident reporting system, low levels of data controller compliance, and weak technical capacity of law enforcement officials.

Data from the National Cyber Security Index (NCSI) shows that Indonesia's score remains suboptimal compared to the expected cybersecurity targets. This indicates that Indonesia's cybersecurity infrastructure and data protection policies need to be strengthened. Furthermore, major data breaches, such as those in the e-commerce and public services sectors, demonstrate that preventive and mitigation measures have not been effective.

One factor hampering effectiveness is limited human resources and technology within relevant institutions, such as the National Cyber and Crypto Agency (BSSN) and the Ministry of Communication and Informatics. Inter-agency coordination in handling cybercrime is also not fully integrated, resulting in response often being reactive and unable to prevent similar incidents in the future.

Legal disincentives in the context of personal data protection mean the threat of severe sanctions to deter violations. Under the Personal Data Protection Law, these disincentives are reflected in criminal sanctions of up to six years in prison or a maximum fine of six billion rupiah, as well as administrative sanctions of up to 2% of annual revenue. However, these disincentives will only be effective if law enforcement is carried out consistently and transparently, thus creating a real deterrent effect for violators.

Unfortunately, to date, these sanctions have rarely been strictly enforced. Many data breach cases end without clear action or compensation for the victims. This weakens the disincentive function of the PDP Law, as perpetrators do not experience adequate legal consequences.

In order for the PDP Law to function as an effective digital social control tool, it is necessary to: Strengthen independent supervisory institutions that have the authority to investigate and impose sanctions, A digital-based public reporting system that makes it

easier for the public to report suspected personal data violations quickly and safely, Increase the technical capacity of officers in digital forensics, cyber incident analysis, and electronic evidence-based law enforcement, Consistent application of sanctions for violations, both in the public and private sectors.

In general, the effectiveness of the PDP Law in preventing and addressing cybercrime will depend heavily on the government's commitment to accelerating the establishment of oversight bodies, strengthening technical infrastructure, raising public awareness, and ensuring compliance by data controllers. Without these measures, this regulation risks remaining merely a legal norm without adequate implementation power on the ground. (Christianingrum, 2020).

3.2. Indonesian law has not yet ratified the Budapest Convention, posing a challenge to law enforcement against transnational cybercrime.

The rapid development of information technology has given rise to various forms of transnational cybercrime, one of which is the misuse of personal data. This phenomenon poses a serious challenge to the Indonesian criminal justice system, given the transnational, complex, and evolving nature of cybercrime. Therefore, the urgency of criminal law reform is crucial for Indonesia to adapt to these dynamics.

Globally, the international legal framework emphasizes the importance of regulatory harmonization and cooperation between countries. The main obstacles to cross-border personal data protection lie in legal fragmentation, weak enforcement mechanisms, and the absence of effective global instruments for resolving disputes (Khan, 2025). This demonstrates that Indonesia cannot stand alone but must integrate its criminal law with international standards.

At the national level, Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) is a significant milestone. While the PDP Law provides a comprehensive framework, its implementation faces significant obstacles, such as low public awareness, business readiness, and limited capacity of regulatory agencies. Even the application of criminal sanctions requires further evaluation to create a deterrent effect (Kurniawan, 2024). This emphasizes that criminal law reform is not merely a matter of paperwork; it must also strengthen institutional aspects and enforcement.

Indonesia has not yet fully integrated with international standards such as the Budapest Convention on Cybercrime. This limits Indonesia's ability to collaborate globally to prosecute transnational cybercriminals. It also highlights the need to improve the capacity of law enforcement officials, digital forensics, and public literacy to close legal loopholes frequently exploited by cybercriminals (Rusydi, 2025).

Personal data protection is a strategic issue in digital governance, particularly in the era of globalization marked by the rise of transnational cybercrime. Indonesia has responded to this challenge by enacting Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). However, a crucial question arises: to what extent does this regulation align with international standards, particularly the European Union's General Data Protection Regulation (GDPR), in combating cybercrime?

In terms of substance, the PDP Law recognizes the rights of data subjects and establishes administrative and criminal sanctions. This is a step forward, but its

weakness lies in the incomplete implementation instruments. For example, the PDP Law does not yet regulate in detail privacy by design, data portability, and cross-border data flow mechanisms, which are key principles of the GDPR. Furthermore, the absence of an independent supervisory authority makes the implementation of the PDP Law less effective. In this context, it shows that the PDP Law is still in its early stages of development and requires further harmonization with international standards to provide more comprehensive protection for personal data in the digital era (Karnedi, 2025).

From an institutional perspective, the weaknesses of the PDP Law are also demonstrated through overlapping authority between institutions, weak coordination, and low accountability. The main obstacle to implementing the PDP Law lies in the unpreparedness of the legal system and supervisory institutions, resulting in inadequate protection of personal data rights (Rinjani, 2025). This contrasts with the GDPR, which has the European Data Protection Board (EDPB) as an independent authority to oversee, impose sanctions, and ensure cross-border compliance.

In practice, massive data breaches in Indonesia—such as those involving Tokopedia and BPJS Kesehatan—demonstrate weak legal protection and cybersecurity. The PDP Law does contain criminal penalties for perpetrators of personal data misuse, such as those punishable by imprisonment in cases of identity theft, but consumer protection remains inadequate. This is reinforced by the finding that the new Criminal Code does not explicitly regulate online data theft (Karnedi, 2025). Furthermore, misuse of consumer data by companies also indicates weak business compliance and the absence of an integrated public reporting mechanism (Jefry, 2025).

Regarding transnational cybercrime, the PDP Law does not specifically regulate forms of crime such as malware-based phishing or APK-based phishing. Indonesian regulations are not yet comprehensive in addressing the transnational nature of phishing, unlike regulations in the European Union, which are more stringent in anticipating cross-jurisdictional data leaks (Anjheli, 2024). These limitations create vulnerabilities in the face of global cyberattacks.

In terms of cybersecurity, Indonesia also remains weak. Indonesia's cybersecurity index score was only 38.96 in 2022, making it one of the lowest among G20 countries. Although Article 30 of the Privacy and Data Protection Law provides a basis for legal accountability for data controllers, the weak cybersecurity system makes it difficult to enforce this regulation effectively (Usman, 2024). This demonstrates a significant gap between legal norms and practical reality.

Furthermore, from the perspective of big data and the dominance of giant digital platforms, the PDP Law is considered incapable of providing balanced protection. Without strengthening inclusive and trust-based data governance, individuals' right to privacy remains vulnerable to violations (Abdullah, 2025). In fact, on more specific issues such as genomic data protection, Indonesia still lags far behind. The PDP Law does not recognize genomic data as a special category like the GDPR and the Australian Privacy Act, so protection for this data remains weak (Puananndini, 2025).

4. Conclusions

This study demonstrates that the effectiveness of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in combating cybercrime in Indonesia remains limited, as normative advances have not yet been matched by effective institutional implementation. The findings provide practical guidance for policymakers by emphasizing that a safe and equitable digital ecosystem requires not only regulatory clarity but also the accelerated establishment of an independent supervisory authority, strengthened inter-agency coordination, mandatory cybersecurity standards for data controllers, and inclusive digital literacy policies to ensure equal protection for all data subjects. From an academic perspective, this study highlights the need for follow-up research that moves beyond secondary data analysis toward primary empirical investigations involving regulators, law enforcement, and affected users, as well as comparative and sector-specific studies to examine how the PDP Law interacts with criminal law enforcement and international cybercrime frameworks. Such research is essential to develop an evidence-based and adaptive cyber law regime capable of responding to the transnational and rapidly evolving nature of cyber threats in Indonesia.

References

Abdullah, Chairunnisa, Nursakina Durand & Roy Marthen Moonti.(2025). *"Transformasi Digital dan Hak atas Privasi: Tinjauan Kritis Pelaksanaan UU Perlindungan Data Pribadi (PDP) Tahun 2022 di Era Big Data."* Amandemen: Jurnal Ilmu Pertahanan, Politik dan Hukum Indonesia, Vol. 2, No. 3.

Aji, M. P. (2022). *Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective].* Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, Vol. 13, No. 2.

Anjheli, Devi.(2024). *"Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP."* STAATSRECHT: Jurnal Hukum Kenegaraan dan Politik Islam, Vol. 4, No. 1.

Ariesta, W., & Pasuruan, U. M. (2024). *STUDI KOMPARASI PERLINDUNGAN HUKUM DATA PRIBADI UNI EROPA DAN INDONESIA DALAM PRINSIP THE RIGHT TO BE FORGOTTEN MENURUT PASAL 26 UU NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UU NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK.* JURNAL ILMIAH HUKUM (YURIJAYA), Vol. 6, No. 2.

Badan Siber dan Sandi Negara. 2024. *Lanskap Keamanan Siber Indonesia 2024*. Jakarta: BSSN.

Badri, Ainul. (2021). *Efektivitas Kebijakan Pembatasan Sosial Berskala Besar (PSBB) di Indonesia Ditinjau dari Perspektif Hukum.* Jurnal Analisis Hukum (JAH), Vol. 2, No. 2.

Christianingrum, Ratna & Ade Nurul Aida.(2020). *"Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan Nasional."* Pusat Kajian Anggaran DPR RI.

Jefry, Buala, Elisatris Gultom & Deviana Yuanitasari.(2025). *"Penyalahgunaan Data Pribadi Konsumen oleh Perusahaan: Kajian Yuridis dalam Perspektif UU Perlindungan Konsumen dan UU Perlindungan Data Pribadi."* Jurnal Pendidikan Indonesia, Vol. 6, No. 5.

Karnedi, Gunawan & RG Guntur Alam.(2025). *"Evaluasi Regulasi Perlindungan Data Pribadi di Indonesia: Komparasi dengan GDPR Uni Eropa."* El-Mujtama: Jurnal Pengabdian Masyarakat, Vol. 5, No. 3.

Kementerian Komunikasi dan Informatika. 2024. *Laporan Tahunan Kamsiber 2024: KOMINFO-CSIRT*. Jakarta: Kementerian Komunikasi dan Informatika.

Khan, M. N. I. (2025). *Cross-Border Data Privacy and Legal Support: A Systematic Review of International Compliance Standards and Cyber Law Practices.* American Journal of Scholarly Research and Innovation, Vol. 4, No. 1.

Kurniawan, K. D., Hehanussa, D. J. A., Setiawan, R., Susilowati, I., Sopian, & Helfisar, D. (2024). *Criminal Sanctions and Personal Data Protection in Indonesia.* Lex Publica, Vol. 11, No. 2.

Noorsanti, I. A., & Yudhanti, R. (2023). *Kemanfaatan Hukum Jeremy Bentham Relevansinya dengan Kebijakan Pemerintah melalui Bantuan Langsung Tunai Dana Desa*. Sultan Jurisprudence: Jurnal Riset Ilmu Hukum, Vol. 3, No. 2.

Prabowo, W., Wibawa, S., & Azmi, F. (2020). *Perlindungan Data Personal Siber di Indonesia.* Padjadjaran Journal of International Relations, Vol. 1, No. 3.

Puananndini, Dewi Asri, Aldi SatyaPutranto, Mustafid & Indah Thalita.(2025). *"Urgensi Regulasi Khusus untuk Perlindungan Data Genomik di Indonesia: Studi Perbandingan dengan GDPR dan Australian Privacy Act."* al-Battar: Jurnal Pamungkas Hukum, Vol. 2, No. 1.

Ramadhani, S. A. (2022). *Komparasi pengaturan perlindungan data pribadi di Indonesia dan Uni Eropa.* Jurnal Hukum Lex Generali, Vol. 3, No. 1.

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

Rusydi, M. T. (2025). *Cyber Law Policy Development: Indonesia's Response to International Cybercrime Threats.* Journal of Progressive Law and Legal Studies, Vol. 3, No. 1.

Susanto, Bagus Kurniawan.(2025). *"Analisis UU Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dalam Perspektif Kepentingan Umum: Studi Banding dengan GDPR Uni Eropa, PDPA Singapura, dan DPA Filipina."* Research and Legal Analysis Journal (Reslaj), Vol. 7, No. 5.

Umbara, A., & Setiawan, D. A. (2022). *Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19.* Jurnal Riset Ilmu Hukum, Vol. 2, No. 2.

Usman, Noval bin & Satria Unggul Wicaksana Prakasa.(2024). *"Perlindungan Hukum Data Pribadi dan Pertanggungjawaban Otoritas terhadap Keamanan Siber Menurut Tinjauan UU PDP."* Doktrina: Journal of Law, Vol. 7, No. 2.