Journal of Cyber Law and Information Security
Volume 2, Number 1, 2023

A Normative Analysis of the Effectiveness of Sanctions under Law No. 27 of 2022 in Cases of Personal Data Misuse

Cika Liyana[1*]

[1] Universitas Bandar Lampung, Lampung, Indonesia

Abstract

Article history:
Received: January 13, 2023
Revised: February 11, 2023
Accepted: March 22, 2023
Published: June 30, 2023

Keywords:
Cyber Law, Law No. 27 of 2022, Personal Data Misuse, Personal Data Protection, Sanctions.

Identifier:
Zera Open
Page: 1-20
https://zeraopen.com/journal/jclis

This article examines the effectiveness of sanctions under Law No. 27 of 2022 concerning Personal Data Protection in responding to personal data misuse in Indonesia. The discussion is situated within the growing urgency of cyber law and information security, particularly as digital platforms, public services, financial technology, and electronic transactions increasingly rely on large-scale personal data processing. Using a normative legal approach, this study analyzes statutory provisions, legal principles, scholarly literature, and selected reputable news reports as factual illustrations of personal data misuse. The findings show that Law No. 27 of 2022 provides a stronger legal foundation than the previous fragmented framework by regulating data subject rights, controller and processor obligations, and administrative and criminal sanctions. However, the effectiveness of these sanctions remains dependent on implementing regulations, institutional supervision, enforcement coordination, evidentiary capacity, corporate compliance, and accessible remedies for victims. The article concludes that the sanction framework is normatively important but requires further regulatory and institutional strengthening to ensure effective personal data protection.

*Corresponding author:
(Cika Liyana)

1. Introduction

The rapid expansion of digital platforms, public service digitalization, financial technology, e-commerce, and social media has placed personal data at the center of Indonesia's cyber law discourse. Personal data is no longer merely an administrative identifier, but has become an economic, social, and legal asset that can be collected, processed, transferred, profiled, and misused across digital systems. Rosadi and Pratama (2018) argue that privacy and personal data protection are increasingly urgent in the digital economy because individuals are required to disclose personal information when accessing online services, while the risks of misuse continue to grow. Sautunnida (2018) similarly emphasizes that Indonesia requires a specific legal framework on personal data protection because digital transactions create new vulnerabilities that cannot be fully addressed through general civil, criminal, or administrative law instruments.

Before the enactment of Law No. 27 of 2022 concerning Personal Data Protection, Indonesia's legal framework was fragmented across several sectoral instruments, including electronic information regulations, population administration rules, consumer protection norms, and financial services regulations. Yuniarti (2019) notes that this sectoral approach created legal uncertainty because there was no single statute that comprehensively regulated the rights of data subjects, the obligations of data controllers, and the consequences of personal data violations. Hisbulloh (2021) also explains that the absence of a dedicated personal data protection law created weak legal certainty, especially in determining responsibility when data was processed, transferred, or leaked by electronic system providers. This

condition became increasingly problematic as personal data misuse became more visible in public life. Reports on large-scale incidents, including the BPJS Kesehatan data leak, the e-HAC data exposure, and the alleged leak of SIM card registration data linked to the Bjorka case, show that personal data violations may produce serious legal and social consequences, including identity theft, fraud, reputational harm, and declining public trust in digital governance.

Law No. 27 of 2022 marks an important turning point in Indonesia's personal data protection regime. The law introduces data subject rights, regulates the obligations of personal data controllers and processors, and provides administrative as well as criminal sanctions for violations. These sanction provisions are central to the effectiveness of the law because personal data protection cannot rely only on normative recognition of rights. It also requires enforceable consequences for parties that unlawfully collect, disclose, use, transfer, falsify, or misuse personal data. Niffari (2020) places personal data protection within the broader framework of human rights, particularly the right to personal self-protection. This means that misuse of personal data is not only a technical or administrative failure, but also a violation of individual autonomy, dignity, and control over personal identity. Situmeang (2021) further explains that personal data misuse can be understood as a serious form of cybercrime because victims may permanently lose control over information once it is distributed through digital networks. Therefore, sanctions under the Personal Data Protection Law must be examined not only as punitive measures, but also as instruments of deterrence, accountability, and legal protection for data subjects.

Nevertheless, the existence of sanctions does not automatically guarantee effective protection. Mahira et al. (2020) argue that personal data protection requires cooperation among regulators, business actors, digital platforms, and consumers because data misuse often occurs within complex digital ecosystems. Comparative studies also show that the strength of a data protection regime depends on how clearly obligations are formulated and how consistently sanctions are enforced. Rizal (2019), for example, compares Indonesian and Malaysian personal data protection frameworks and highlights that clearer institutional and sectoral enforcement structures may support stronger compliance. Ramadhani (2022), through comparison with the European Union, similarly emphasizes that effective data protection requires not only written rights and obligations, but also institutional supervision and reliable enforcement mechanisms. This means that the effectiveness of sanctions under Law No. 27 of 2022 depends on several legal and institutional factors, including the clarity of prohibited acts, proportionality of penalties, enforcement capacity, corporate accountability, and the availability of remedies for victims.

The research gap in this study lies in the limited normative discussion on the effectiveness of sanctions under Law No. 27 of 2022 in responding specifically to personal data misuse. Existing studies have generally emphasized the urgency of personal data protection, comparative lessons from other jurisdictions, the human rights dimension of data privacy, and the inadequacy of Indonesia's fragmented framework before the enactment of the Personal Data Protection Law. Rosadi and Pratama (2018), Sautunnida (2018), Yuniarti (2019), Hisbulloh (2021), and Niffari

(2020) mainly underline the need for comprehensive personal data regulation, while Rizal (2019) and Ramadhani (2022) provide comparative perspectives. Yuniarti (2022) also discusses Indonesia's personal data protection after the ratification of the Personal Data Protection Act, but the specific normative effectiveness of sanctions in personal data misuse cases still requires further study. This gap is important because sanctions are the main legal mechanism through which personal data protection can be transformed from a formal right into an enforceable obligation.

Based on this gap, this article addresses two research questions. First, to what extent are the sanctions under Law No. 27 of 2022 effective in responding to cases of personal data misuse? Second, why is the regulation of sanctions in personal data protection important to be studied within Indonesia's cyber law framework? Using a normative legal approach, this study examines statutory provisions, legal principles, scholarly literature, and selected reputable news reports as factual illustrations of personal data misuse. The article is expected to contribute to cyber law scholarship by assessing whether the sanction framework under Law No. 27 of 2022 provides sufficient legal certainty, deterrence, and accountability, or whether further regulatory and institutional strengthening is still required.

2. Research Methods

This study uses a normative legal research method to examine the effectiveness of sanctions under Law No. 27 of 2022 concerning Personal Data Protection in cases of personal data misuse. A normative approach is appropriate because the main focus of this article is not to measure public perception or

institutional practice empirically, but to analyze legal norms, statutory provisions, legal principles, and doctrinal arguments relevant to personal data protection. The object of analysis is the sanction framework contained in Law No. 27 of 2022, particularly provisions regulating administrative and criminal consequences for unlawful collection, disclosure, use, falsification, and misuse of personal data. This approach allows the study to evaluate whether the legal construction of sanctions provides sufficient legal certainty, deterrence, proportionality, and accountability for personal data controllers, processors, corporations, and individuals.

The study applies statutory, conceptual, and case-based approaches. The statutory approach is used to examine Law No. 27 of 2022 as the primary legal material, supported by related Indonesian cyber law and electronic system regulations where relevant. The conceptual approach is used to discuss key legal concepts such as personal data, data subject rights, data controller responsibility, administrative sanctions, criminal sanctions, legal certainty, deterrence, and accountability. Meanwhile, the case-based approach is used in a limited manner by referring to selected personal data misuse incidents reported by reputable news portals. These cases are not treated as empirical samples, but as factual illustrations that show the practical urgency of sanction regulation in Indonesia's digital ecosystem. Therefore, the analysis remains normative while still being connected to real legal problems arising from data misuse.

The legal materials used in this study consist of primary, secondary, and supporting materials. Primary legal materials include Law No. 27 of 2022 concerning Personal Data Protection and other relevant statutory regulations. Secondary

materials include peer-reviewed journal articles, scholarly legal studies, and comparative literature on personal data protection published through Google Scholar-indexed sources. Supporting materials include reputable news reports used only to illustrate personal data misuse cases. The collected materials are analyzed qualitatively through descriptive and prescriptive legal analysis. Descriptive analysis is used to explain the structure and scope of sanctions under Law No. 27 of 2022, while prescriptive analysis is used to assess whether these sanctions are normatively adequate to answer the two research questions. Through this method, the article seeks to determine whether the sanction framework has strengthened personal data protection or whether further regulatory and institutional improvements are still needed.

3. Results and Discussion

3.1. To What Extent Are the Sanctions under Law No. 27 of 2022 Effective in Responding to Cases of Personal Data Misuse?

Law No. 27 of 2022 concerning Personal Data Protection represents an important legal development because it transforms personal data protection from a scattered sectoral issue into a specific statutory regime. Before this law, Indonesia relied on various legal instruments, such as electronic information regulations, population administration rules, financial service regulations, and consumer protection norms. However, these instruments were not designed as a comprehensive framework for personal data protection. Yuniarti (2019) argues that this fragmented structure created legal uncertainty, especially in determining the

rights of data subjects and the legal responsibility of parties processing personal data. In this context, Law No. 27 of 2022 is more effective than the previous regulatory framework because it provides clearer legal categories, obligations, prohibitions, and sanction mechanisms.

The sanction framework under Law No. 27 of 2022 can be considered normatively significant because it combines administrative and criminal sanctions. Administrative sanctions are important for regulatory compliance because not every personal data violation should immediately be treated as a criminal offense. Under the law, administrative sanctions may include written warnings, temporary suspension of personal data processing activities, deletion or destruction of personal data, and administrative fines. This mechanism allows the state to respond to violations committed by personal data controllers or processors in a flexible and corrective manner. Administrative sanctions are particularly relevant in cases involving negligence, weak internal governance, failure to secure personal data, or failure to fulfill obligations toward data subjects.

In addition, Law No. 27 of 2022 also provides criminal sanctions for more serious forms of personal data misuse. The law prohibits unlawful collection, disclosure, use, and falsification of personal data. These provisions are important because many personal data misuse cases involve deliberate actions, such as collecting identity information without consent, selling personal data, using another person's data for fraud, or disclosing private information to harm a victim. Situmeang (2021) describes personal data misuse as a serious form of cybercrime because digital dissemination can cause long-term harm and make it difficult for

victims to regain control over their personal information. Therefore, criminal sanctions are needed not only to punish offenders, but also to express that personal data misuse is a serious legal violation.

From the perspective of deterrence, the sanctions under Law No. 27 of 2022 have stronger normative force than previous regulations because they directly attach legal consequences to specific prohibited acts. The law does not merely state that personal data must be protected, but also regulates what conduct is prohibited and what sanctions may be imposed. This structure supports legal certainty because individuals, corporations, and electronic system providers can identify the legal boundaries of personal data processing. Hisbulloh (2021) emphasizes that a dedicated personal data protection law is necessary to reduce uncertainty in the digital environment, particularly when personal data is processed by multiple actors. The existence of sanctions strengthens this certainty because obligations become enforceable rather than merely declaratory.

The effectiveness of the sanction framework can also be seen from its recognition of corporate accountability. Personal data misuse often occurs within institutional systems rather than through individual action alone. Digital platforms, financial technology companies, telecommunication providers, marketplaces, and public service systems process large volumes of personal data. If sanctions only targeted individual offenders, the law would not be adequate to address structural failures in data governance. Law No. 27 of 2022 allows sanctions to be imposed on corporations, including higher fines in certain circumstances. This is normatively important because corporate actors often have greater control over personal data

infrastructure and greater capacity to prevent misuse. Mahira et al. (2020) note that personal data protection requires collaboration among regulators, business actors, platforms, and consumers. Corporate sanctions therefore function as a compliance mechanism that encourages organizations to build stronger data protection systems.

However, the effectiveness of sanctions under Law No. 27 of 2022 is not absolute. A first limitation concerns the operational clarity of enforcement. A sanction may be well written in statutory text, but its effectiveness depends on how it is implemented by supervisory authorities, investigators, prosecutors, and courts. Attidhira and Permana (2022) explain that legal loopholes and weak enforcement mechanisms have contributed to continuing personal data leaks and misuse in Indonesia. This means that Law No. 27 of 2022 may provide a stronger legal foundation, but its sanctions still require clear procedural mechanisms. Without detailed implementing regulations, technical standards, and institutional coordination, sanctions may be difficult to apply consistently.

A second limitation concerns the relationship between administrative and criminal sanctions. In theory, administrative sanctions should address compliance failures, while criminal sanctions should address intentional or serious violations. However, in practice, boundaries between negligence, unlawful processing, and intentional misuse may be difficult to establish. For example, a data breach may occur because of weak cybersecurity, but the leaked data may later be sold or used by third parties for fraud. In such cases, enforcement authorities must determine whether the data controller is administratively responsible, whether an individual actor is criminally liable, or whether both forms of liability should apply. Nugroho

et al. (2020) argue that personal data protection in Indonesia requires clearer legal arrangements because digital data processing creates complex relationships between data owners, data users, and electronic system providers. Therefore, the effectiveness of sanctions depends on the ability of legal institutions to classify violations accurately.

A third limitation concerns victim protection and remedies. Sanctions are important, but they do not automatically restore the position of the data subject. Victims of personal data misuse may suffer financial loss, identity theft, harassment, reputational damage, or emotional distress. Niffari (2020) argues that personal data protection is part of the broader human right to personal self-protection. If sanctions only punish violators but do not provide accessible remedies for victims, the law may remain incomplete from the perspective of justice. Law No. 27 of 2022 recognizes data subject rights, but effective protection also requires practical complaint mechanisms, compensation pathways, and accessible enforcement procedures.

Comparative scholarship further shows that sanctions are more effective when supported by independent and credible supervision. Ramadhani (2022), in comparing Indonesia and the European Union, highlights that strong personal data protection requires not only written norms, but also institutional supervision and reliable enforcement. Simbolon and Juwono (2022) also note that Indonesia's PDP Law was influenced by the European Union's General Data Protection Regulation, especially in its effort to provide legal certainty for citizens affected by personal data leaks. However, the effectiveness of this model depends on whether Indonesia can

develop institutions capable of monitoring compliance, investigating violations, and imposing sanctions fairly. Thus, Law No. 27 of 2022 is normatively effective in providing a stronger sanction framework, but its practical effectiveness remains dependent on institutional readiness and regulatory follow-up.

Overall, the sanctions under Law No. 27 of 2022 are effective at the normative level because they address the main weaknesses of the previous fragmented framework. They define prohibited conduct, provide administrative and criminal consequences, recognize corporate liability, and strengthen legal certainty in personal data governance. However, the sanctions are not fully sufficient by themselves. Their effectiveness depends on implementing regulations, supervisory authority, enforcement coordination, evidentiary capacity, victim remedies, and organizational compliance. Therefore, the law should be understood as a strong foundation, but not yet a complete guarantee of protection against personal data misuse.

3.2. Why Is the Regulation of Sanctions in Personal Data Protection Important to Be Studied within Indonesia's Cyber Law Framework?

The regulation of sanctions in personal data protection is important to be studied because personal data misuse has become one of the most urgent cyber law problems in Indonesia. Digital transformation has made personal data a key element in almost every sector, including banking, health services, telecommunications, education, public administration, transportation, and online commerce. Rosadi and Pratama (2018) state that privacy protection is increasingly urgent in the digital economy because people are required to disclose personal information as a condition

for accessing digital services. When personal data is collected and processed on a large scale, the risk of misuse also increases. Therefore, cyber law must not only regulate electronic transactions or cybercrime in a narrow sense, but also protect individuals from unlawful data exploitation.

Sanctions are central to this framework because rights without consequences are weak rights. Law No. 27 of 2022 recognizes the rights of data subjects, but these rights require enforceable obligations on the part of data controllers and processors. If personal data controllers can collect, disclose, or use personal data unlawfully without facing meaningful consequences, then the recognition of data subject rights becomes merely symbolic. Sautunnida (2018) previously argued that Indonesia needed a personal data protection law because general legal instruments were insufficient to respond to digital privacy risks. The study of sanctions is therefore necessary because sanctions are the mechanism through which the law moves from abstract protection to concrete enforcement.

The urgency of sanction regulation is also connected to the nature of harm in personal data misuse. Unlike conventional property loss, personal data misuse may continue to produce harm even after the initial violation occurs. Once identity numbers, phone numbers, addresses, health data, or financial information are leaked or sold, the data may be copied, transferred, and reused repeatedly. Situmeang (2021) describes this as a serious cybercrime problem because victims may permanently lose control over their personal information. This characteristic makes sanctions important as a preventive instrument. Effective sanctions should create deterrence before violations occur by encouraging organizations to adopt privacy-by-design,

data minimization, access control, breach notification, and internal compliance systems.

The regulation of sanctions is also important because Indonesia's digital economy depends heavily on public trust. E-commerce, fintech, telemedicine, online education, and digital public services require users to submit personal data. If the public believes that personal data is not protected or that violations will not be punished, trust in digital services may decline. Mahira et al. (2020) highlight the need for a collaborative consumer protection system in which personal data protection involves regulators, business actors, and consumers. Sanctions support this collaborative model by setting minimum standards of responsibility. They signal to business actors that data protection is not optional, but a legal obligation attached to digital service provision.

In the context of cyber law, sanction regulation is also important because personal data misuse often intersects with other offenses. Misused data may be used for phishing, illegal online lending, identity fraud, account takeover, doxing, harassment, or unauthorized profiling. This shows that personal data protection is not isolated from broader cybercrime prevention. Nugroho et al. (2020) explain that personal data protection must be viewed as part of the national legal response to technological development. If sanctions under the PDP Law are weak, unclear, or inconsistently enforced, other cybercrimes may become easier to commit because offenders can exploit personal information with limited risk.

Furthermore, the study of sanctions is urgent because Law No. 27 of 2022 is a relatively new legal regime that requires doctrinal interpretation. Legal scholars

need to examine whether the sanctions are proportionate, whether they reflect the seriousness of violations, and whether they are compatible with the principles of criminal law and administrative law. Not every violation should be criminalized, but serious misuse must receive an adequate punitive response. This balance is important to avoid two risks: over-criminalization that may burden enforcement institutions, and under-enforcement that may weaken protection. Attidhira and Permana (2022) emphasize the need for better mechanisms to achieve effective protection of personal data in Indonesia. This supports the view that sanction analysis is not only about the severity of punishment, but also about coherence, fairness, and enforceability.

The importance of studying sanctions is also strengthened by comparative perspectives. Rizal (2019) compares Indonesian and Malaysian personal data protection frameworks and shows that data protection regulation requires clear institutional and enforcement design. Ramadhani (2022) and Simbolon and Juwono (2022) further show that comparison with the European Union is relevant because the GDPR demonstrates how strong supervision and significant administrative fines can shape compliance behavior. However, Indonesia cannot simply copy foreign models without considering its own legal culture, institutional capacity, and enforcement challenges. A normative study of sanctions is therefore needed to assess whether Indonesia's model is suitable for its cyber law environment.

Another reason why sanction regulation must be studied is the need to protect vulnerable data subjects. Personal data misuse does not affect all individuals equally. Children, patients, consumers, borrowers, workers, and users of public services may

have limited bargaining power when dealing with institutions that collect their data. Niffari (2020) connects personal data protection with human rights, especially the right to personal autonomy and self-protection. From this perspective, sanctions are not merely technical enforcement tools. They are part of the state's obligation to protect individuals from abuse of power by private and public data controllers.

Finally, the regulation of sanctions under Law No. 27 of 2022 is important because it reflects the future direction of Indonesia's cyber law. Earlier scholarship focused mainly on the urgency of enacting a personal data protection law. After the enactment of Law No. 27 of 2022, the question has shifted from whether Indonesia needs a PDP Law to whether the law can be enforced effectively. Yuniarti (2022) notes that the ratification of the PDP Law is an important step in Indonesia's data protection development, but post-ratification protection still requires further legal and institutional strengthening. This article therefore places sanctions at the center of analysis because they determine whether the law can function as a real instrument of accountability.

Based on the discussion above, the regulation of sanctions in personal data protection is important to be studied for at least four reasons. First, sanctions determine whether data subject rights can be practically enforced. Second, sanctions create deterrence against unlawful data processing and misuse. Third, sanctions strengthen public trust in Indonesia's digital ecosystem. Fourth, sanctions clarify the responsibility of individuals, corporations, and electronic system providers within the broader cyber law framework. Thus, the study of sanctions under Law No. 27

of 2022 is essential to evaluate whether Indonesia's personal data protection regime is capable of responding to current and future challenges in digital governance.

4. Conclusion

This article concludes that the sanctions under Law No. 27 of 2022 concerning Personal Data Protection are normatively significant in strengthening Indonesia's response to personal data misuse. Compared with the previous fragmented framework, the law provides a clearer legal basis for identifying prohibited conduct, determining the obligations of personal data controllers and processors, and imposing consequences for violations. Its combination of administrative and criminal sanctions reflects an important legal development because personal data misuse may arise from different levels of wrongdoing, ranging from weak compliance and negligent data governance to intentional collection, disclosure, use, falsification, or sale of personal data. Therefore, the sanction framework has the potential to improve legal certainty, create deterrence, and strengthen accountability in Indonesia's digital ecosystem.

However, the effectiveness of these sanctions cannot be assessed only from their existence in statutory text. The discussion shows that Law No. 27 of 2022 is effective at the normative level, but its practical effectiveness still depends on several supporting factors. These include the clarity of implementing regulations, the capacity of supervisory institutions, coordination among enforcement authorities, evidentiary mechanisms for digital violations, corporate compliance systems, and accessible remedies for victims. Without these elements, administrative and criminal

sanctions may remain formal provisions that are difficult to enforce consistently. This is particularly important because personal data misuse often involves complex actors, including corporations, electronic system providers, public institutions, third-party processors, and individual offenders. In such situations, law enforcement must be able to distinguish between administrative negligence, systemic governance failure, and intentional criminal misuse.

The urgency of studying sanctions under Law No. 27 of 2022 also lies in the broader role of personal data protection within cyber law. Personal data misuse is not an isolated privacy issue, but a gateway to other digital harms such as identity theft, phishing, illegal profiling, online fraud, harassment, and unauthorized commercial exploitation. For this reason, sanctions are essential to transform data subject rights into enforceable legal protection. They also encourage data controllers and processors to adopt stronger internal safeguards, improve compliance, and treat personal data protection as a legal obligation rather than a voluntary ethical standard. In a digital economy that depends on public trust, sanction regulation becomes a key instrument for maintaining confidence in online services and digital governance.

Overall, Law No. 27 of 2022 provides an important foundation for personal data protection in Indonesia, but further strengthening is still required. The government should ensure that implementing regulations clarify sanction procedures, supervisory authority, complaint mechanisms, compensation pathways, and standards for corporate accountability. Legal institutions must also develop technical capacity to investigate and prove personal data misuse. Thus, the sanction framework under Law No. 27 of 2022 should be viewed as a necessary starting point,

but not the final stage, in building an effective and accountable personal data protection regime in Indonesia.

References

Attidhira, S. W., & Permana, Y. S. (2022). Review of personal data protection legal regulations in Indonesia. *Awang Long Law Review, 5*(1), 280–294.

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum Unissula, 37*(2), 119–133.

Mahira, D. F. F., Yofita, E., & Azizah, L. N. (2020). Consumer Protection System (CPS): Sistem perlindungan data pribadi konsumen melalui collaboration concept. *Jurnal Legislatif, 3*(2), 287–302.

Niffari, H. (2020). Perlindungan data pribadi sebagai bagian dari hak asasi manusia atas perlindungan diri pribadi: Suatu tinjauan komparatif dengan peraturan perundang-undangan di negara lain. *Jurnal Yuridis, 7*(1), 105–119.

Nugroho, A. A., Winanti, A., & Surahmad. (2020). Personal data protection in Indonesia: Legal perspective. *International Journal of Multicultural and Multireligious Understanding, 7*(7), 183–189.

Ramadhani, S. A. (2022). Komparasi perlindungan data pribadi di Indonesia dan Uni Eropa. *Jurnal Hukum Lex Generalis, 3*(1), 73–84.

Republic of Indonesia. (2022). Law Number 27 of 2022 concerning Personal Data Protection.

Rizal, M. S. (2019). Perbandingan perlindungan data pribadi Indonesia dan Malaysia. *Jurnal Cakrawala Hukum, 10*(2), 218–227.

Rosadi, S. D., & Pratama, G. G. (2018). Urgensi perlindungan data privasi dalam era ekonomi digital di Indonesia. *Veritas et Justitia, 4*(1), 88–110.

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi perbandingan hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum, 20*(2), 369–384.

Simbolon, V. A., & Juwono, V. (2022). Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. *Publik: Jurnal Ilmu Administrasi, 11*(2), 178–190.

Situmeang, S. M. T. (2021). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber. *SASI, 27*(1), 38–52.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal, 1*(1), 147–154.

Yuniarti, S. (2022). Protection of Indonesia's personal data after ratification of Personal Data Protection Act. *Progressive Law Review, 4*(2), 54–68.