International Journal of Health, Economics, and Social Sciences (IJHESS)
Vol. 7, No. 2, April 2025, pp. 986~991
DOI: 10.56338/ijhess.v7i2.8300
Website: https://jurnal.unismuhpalu.ac.id/index.php/IJHESS

Criminal Law Implications of Personal Data Misuse in the Digital Age

Aliman
Universitas Indonesia Timur

Article Info

Article history:

Received 24 Jan, 2025
Revised 07 Mar, 2025
Accepted 30 Apr, 2025

Keywords:

personal data, criminal law, misuse, digital era, legal protection

ABSTRACT

The rapid advancement of information technology has significantly transformed modern society, particularly in the way personal data is collected, stored, and processed. While the digital era offers convenience and efficiency, it also presents substantial risks, especially concerning the misuse of personal data by irresponsible individuals, corporations, or other entities with access to sensitive information. Such misuse can take the form of identity theft, online fraud, or unauthorized exploitation of data for economic gain without the data owner's consent. These circumstances highlight the urgent need for comprehensive regulations and effective criminal law mechanisms to protect personal data. This article aims to explore the criminal law implications of personal data misuse within the Indonesian context and assess the extent to which current legal instruments address these challenges. The research adopts a normative juridical approach by analyzing Law No. 27 of 2022 on Personal Data Protection (PDP Law), the Indonesian Penal Code (KUHP), and other related legal provisions. Furthermore, the study examines recent cases to illustrate the weaknesses in cyber law enforcement. The findings reveal that although personal data protection regulations exist, significant gaps remain in implementation, inter-agency coordination, and the effectiveness of criminal sanctions.

Corresponding Author:

Aliman
Universitas Indonesia Timur
alimanmakassar@gmail.com

INTRODUCTION

Over the past two decades, the development of information and communication technology has brought about profound changes in many aspects of human life. The digital revolution has transformed how individuals communicate, access information, conduct economic transactions, and manage personal data. In today's digital age, personal data has emerged as a highly valuable commodity. It no longer functions as passive information but has become a strategic asset utilized for business, political, and social interests (Simbolon & Juwono, 2022).

However, alongside these advantages and efficiencies, digital transformation also presents serious threats especially regarding personal data protection. The misuse of personal data not only infringes upon individuals' privacy rights but can also lead to both material and non material harm. Common forms of data misuse include identity theft, digital document forgery, data driven fraud, and the unauthorized dissemination of sensitive information. Psychological impacts such as anxiety, trauma, and a loss of personal security are also frequently experienced by victims (Solikhah, 2025).

This growing phenomenon indicates that data protection is no longer merely a technological or ethical issue, but a pressing legal concern. The state holds a constitutional responsibility to safeguard its citizens' rights to privacy and personal security, as stipulated in Article 28G paragraph (1) of the 1945 Indonesian Constitution, which affirms that "everyone has the right to personal protection, including that of their family, honor, dignity, and property under their control."

In response to the escalating threats of personal data misuse, Indonesia enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law). This legislation marks a significant milestone in the nation's efforts to establish a robust legal framework for safeguarding personal information. The PDP Law outlines key aspects such as the definition of personal data, the rights of data subjects, the obligations of data controllers and processors, as well as administrative and criminal sanctions for violations. It also introduces several categories of data-related crimes and prescribes substantial penalties, including imprisonment and fines.

Nonetheless, the practical implementation of the PDP Law still faces considerable challenges. A major concern is the lack of integration between the PDP Law and other criminal legal instruments, such as the Indonesian Penal Code (KUHP) and the Law on Electronic Information and Transactions (ITE Law). Regulatory inconsistencies often create confusion in law enforcement and diminish the legal system's effectiveness in protecting victims. For instance, in SIM card registration data breach cases, although privacy rights were evidently violated, enforcement rarely referred to the PDP Law due to weak inter agency coordination and inadequate oversight mechanisms (Matheus & Gunadi, 2024).

Several major data breaches in recent years further highlight Indonesia's fragile data protection system. Incidents involving the leakage of user data from e-commerce platforms, customer data from BPJS Kesehatan, and educational records from online learning systems clearly show the widespread illegal exposure of personal information. Unfortunately, many of the perpetrators faced minimal criminal consequences, while victims often received little to no legal remedy (Bukit & Ayunda, 2022).

Globally, numerous countries have adopted more comprehensive and integrated legal frameworks for data protection. The European Union, for example, has implemented the General Data Protection Regulation (GDPR) since 2018. This regulation not only safeguards EU citizens' data but also extends its applicability to entities outside the EU that handle such data. The GDPR sets high standards for consent, transparency, and accountability, while imposing severe financial penalties for violations.

In light of these international best practices, Indonesia must continue strengthening its criminal law framework to address personal data misuse more effectively. This includes updating the Penal Code to be more responsive to cybercrimes, harmonizing sectoral regulations, enhancing the capacity of law enforcement agencies, and establishing an independent, professional data protection authority.

Given this background, the present study aims to explore in depth the criminal law implications of personal data misuse in the digital era and to assess the effectiveness of existing legal regulations in ensuring adequate protection for individuals. Such an analysis is essential to formulating stronger policy recommendations in the face of ever evolving legal challenges in the digital landscape.

RESEARCH METHODOLOGY

This study employs a normative juridical method, which focuses on the analysis of existing legal norms within the framework of positive law. This method is selected due to the research objective: examining how the criminal justice system in Indonesia responds to the misuse of personal data in the digital era. A normative juridical approach conceptualizes law as a structured and autonomous system of norms. Therefore, this study does not involve empirical field data but relies on legal sources such as statutory regulations, academic literature, and official legal documents. The core of the analysis lies in the textual and systematic examination of relevant legal instruments to assess the effectiveness of criminal norms in safeguarding personal data.

To enhance the depth of analysis, the research incorporates two primary approaches: the statute approach and the conceptual approach. The statute approach is utilized to critically examine legislation directly related to the issue of data misuse, including Law No. 27 of 2022 on Personal Data Protection (PDP Law), the Indonesian Criminal Code (KUHP), the Law on Electronic Information and Transactions (ITE Law), as well as other sectoral or implementing regulations that govern data management and protection. Meanwhile, the conceptual approach is used to explore and compare fundamental legal concepts such as the right to privacy, data control rights, the principle of ultimum remedium, and the principle of lex certa in criminal law, to understand the normative orientation underlying the existing legal framework.

The research relies entirely on secondary data, classified into three categories of legal materials. First, primary legal materials consist of binding legal statutes and regulations. Second, secondary legal materials include legal doctrines and theories sourced from scholarly literature and relevant academic journals concerning personal data protection and criminal law. Third, tertiary legal materials such as legal dictionaries, law encyclopedias, and explanatory notes on legislation are used to support and complement the analysis. These materials are collected through library research, drawing from both print and digital official sources.

Data analysis is conducted qualitatively, emphasizing systematic and teleological legal interpretation. This process involves classifying norms, articulating the legal principles underlying the regulations, and evaluating the implementation of these norms in actual legal practice. Through this approach, the study identifies key issues in legal protection of personal data, including gaps in legislation, regulatory inconsistencies, and weaknesses in the enforcement of criminal law.

The use of the normative juridical method is grounded in the primary aim of this research: to evaluate whether Indonesia's criminal law system is adequately equipped to address emerging legal challenges arising from personal data misuse in the digital landscape. Moreover, this method enables the researcher to propose normative and solution-oriented recommendations for policymakers, law enforcement authorities, and data protection agencies. With this methodological foundation, the study aims to contribute to the reform of a more responsive legal system, attuned to the evolving demands of technological advancement and the public's need for robust personal data protection.

DISCUSSION

The Misuse of Personal Data as a Criminal Offense

In the framework of criminal law, an act is considered a crime if it fulfills certain elements namely, a violation of legal norms, the presence of culpability (whether intentional or due to negligence), and the perpetrator's legal accountability. When applied to the misuse of personal data, such acts can be categorized as criminal offenses if an individual accesses, discloses, distributes, or utilizes someone else's personal information unlawfully and without the data subject's consent. Personal data in this context refers to information that can directly or indirectly identify a person, such as full names, national identification numbers, biometric details, financial information, and medical history.

Indonesia's legal system has taken a significant step forward with the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which establishes a firmer legal foundation against the misuse of personal information. Articles 67 to 70 of the PDP Law explicitly stipulate criminal penalties for the unlawful collection, processing, and dissemination of personal data. For example, Article 67 states that any individual who intentionally and unlawfully discloses another person's personal data may face up to five years of imprisonment and/or a fine of up to five billion rupiah. This provision confirms that data misuse is not merely an administrative violation but a serious criminal act subject to heavy penalties.

Despite this legal clarity, the enforcement of these criminal provisions faces several obstacles. One primary challenge lies in evidence gathering, as personal data misuse typically occurs in digital spaces that are difficult to monitor using conventional investigative methods. Perpetrators often obscure their digital footprints through encryption, VPN usage, and anonymized accounts or servers, which complicates efforts to prove intent and establish causality between the offender's actions and the harm suffered by the victim (Prasetyo et al., 2025).

Jurisdictional challenges also arise due to the transnational nature of many data-related offenses. For instance, an offender residing abroad can exploit or steal data belonging to Indonesian citizens via internet-based systems. In such scenarios, Indonesia's national jurisdiction is limited by the principle of state sovereignty, unless supported by effective international cooperation mechanisms such as mutual legal assistance treaties (MLATs) or extradition agreements. Unfortunately, Indonesia still faces significant limitations in establishing a robust and comprehensive legal cooperation network, especially in the realm of cybercrime (Solikhah, 2025).

Furthermore, there are still legal inconsistencies and regulatory gaps in harmonizing the PDP Law with other legal instruments such as the Criminal Code (KUHP) and the Electronic Information and Transactions Law (ITE Law). Although the PDP Law introduces specific criminal sanctions, not all types of data misuse are explicitly addressed in the KUHP, which remains a legacy of colonial legal structures. This creates potential overlaps or legal vacuums in the enforcement of criminal sanctions.

The classification of data misuse as either a public offense or a complaint-based offense (delik aduan) also has practical implications. If it is treated as a complaint-based offense, law enforcement cannot proceed without a formal report from the victim. This may hinder the effectiveness of legal proceedings, especially when victims are reluctant to report due to lack of legal awareness, fear of social stigma, or even unawareness that their data has been compromised.

In comparison, several countries have made significant strides in criminalizing data misuse. The European Union's General Data Protection Regulation (GDPR), for instance, allows for fines of up to €20 million or 4% of a company's global annual turnover for severe violations of data privacy. Countries like Germany and France have integrated criminal provisions within their legal systems, empowering data protection authorities with substantial investigatory powers, including the ability to seize devices and detain suspects.

In Indonesia, the criminalization of personal data misuse still requires substantial reinforcement both in terms of institutional capacity and public awareness. Effective law enforcement depends not only on the written penal provisions but also on the government's ability to apply the law consistently and transparently. A coordinated effort is essential among the Ministry of Communication and Informatics (Kominfo), the National Police, the Public Prosecutor's Office, and an independent data protection authority as mandated by the PDP Law to ensure the protection of citizens' constitutional rights in the digital era.

Synchronization Between General and Special Criminal Law

One of the major challenges in enforcing legal protection against personal data misuse in Indonesia lies in the lack of alignment between the general criminal law codified in the Indonesian Penal Code (KUHP) and the special criminal provisions outlined in laws such as the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law). The KUHP, as the foundational criminal code, does not explicitly regulate offenses involving personal data breaches. Provisions often relied upon such as Article 362 on theft and Article 378 on fraud are overly general and not designed to address the complex nature of cybercrimes, especially those involving digital data violations (Daeng et al., 2023).

In contrast, the ITE Law and the PDP Law have introduced more specific legal standards concerning the misuse of personal data. For instance, Articles 67 to 70 of the PDP Law stipulate criminal penalties for individuals or entities that unlawfully collect, disclose, or disseminate personal data without consent. Similarly, Article 26 of the ITE Law addresses privacy violations in electronic systems. Despite these advancements, enforcement remains fragmented and operates in silos, lacking systematic integration with the KUHP.

This disjointed approach leads to enforcement complications, including overlapping authority, contradictory regulations, and varying interpretations by law enforcement agencies. As a result, perpetrators of cybercrime involving personal data often escape prosecution due to inconsistencies between general and special laws or the absence of explicit provisions in the KUHP that investigators and prosecutors can readily apply. Moreover, the lack of detailed technical guidelines on how these laws should interact further contributes to legal uncertainty (Situmeang, 2021).

To overcome these issues, strategic efforts are needed to harmonize the KUHP, the ITE Law, and the PDP Law, ensuring a cohesive and integrated legal framework that can effectively respond to the evolving nature of cybercrime. This synchronization may be achieved through the development of implementing regulations or revisions to the KUHP that incorporate digital crime and data protection elements. Institutional coordination also needs to be strengthened so that law enforcement officials are equipped with a unified understanding and legal tools to address personal data violations in the digital age.

Effectiveness of Law Enforcement

The enforcement of laws regarding personal data misuse in Indonesia continues to face structural and cultural challenges. One significant barrier is the low level of digital literacy among the general public. Many individuals are unaware of the value and vulnerability of their personal data, making them easily share it with third parties without understanding the associated risks. This lack of awareness creates opportunities for malicious actors to commit data breaches, unauthorized access, and commercial exploitation without consent. Furthermore, victims often do not report such incidents or are unaware that they have suffered digital harm, which hampers the ability of legal institutions to respond proactively (Mahuli, 2023).

Institutional weaknesses within law enforcement agencies also pose serious obstacles. Law enforcement officers, including investigators and prosecutors, frequently lack sufficient training in handling cybercrimes, particularly those involving data privacy violations. Digital crime investigation requires expertise in digital forensics and cooperation with internet service providers and digital platforms partnerships that are not always forthcoming. Jurisdictional challenges also arise when perpetrators operate across borders, making it difficult for national authorities to pursue legal action without international collaboration. In many cases, investigations are delayed or abandoned due to a lack of strong digital evidence or technical limitations in tracking offenders in cyberspace (Noviantama, 2023).

Although Law No. 27 of 2022 on Personal Data Protection mandates the establishment of an independent supervisory authority with administrative and enforcement powers, this body has yet to become fully operational. Institutional gaps remain in terms of funding, organizational structure, and human resources. Without a fully empowered and autonomous supervisory body, the implementation of the PDP Law remains largely normative and lacks tangible enforcement on the ground (Ayiliani & Farida, 2024).

To enhance law enforcement, systemic measures are required, including capacity building for human resources, stronger cross-sectoral and international cooperation, and the adoption of digital technologies to support regulatory oversight. For example, a nationally integrated reporting and monitoring system that is connected with major digital platforms could improve responsiveness. Without coordinated and forward-looking efforts, legal enforcement will continue to lag behind the rapidly evolving methods of cybercrime.

The Urgency of Digital Criminal Law Reform

The rapid advancement of information technology has given rise to new forms of cybercrime, including the large-scale and cross-border misuse of personal data—types of offenses that were previously unimaginable. These developments demand a legal response that is swift, adaptive, and integrated, particularly to ensure the protection of fundamental human rights such as privacy and data security. Consequently, reforming Indonesia’s digital criminal law framework has become an urgent necessity. Although Law No. 27 of 2022 on Personal Data Protection (PDP Law) has been enacted, its implementation remains fragmented and has not yet been fully harmonized with broader criminal law instruments such as the Criminal Code (KUHP) or the Electronic Information and Transactions Law (ITE Law).

In contrast, the European Union has implemented the General Data Protection Regulation (GDPR) since 2018, serving as a comprehensive legal framework for personal data protection. The GDPR not only governs how data is collected and processed but also stipulates both administrative and criminal sanctions, while establishing an independent supervisory authority with broad oversight powers. Its implementation has been widely recognized as effective in safeguarding individual rights and has set a global benchmark for data governance standards. Indonesia could look to the GDPR as a model in developing a more cohesive and responsive digital criminal legal system.

Digital criminal law reform in Indonesia should also encompass institutional strengthening, the revision of substantive criminal law, and enhanced capacity-building for law enforcement agencies. These measures are crucial given that the challenges in addressing cybercrime extend beyond legal loopholes. They include weak inter-agency coordination, limited expertise in digital forensics, and restricted access to international cooperation mechanisms. Therefore, establishing an independent data protection authority, providing specialized training for law enforcement personnel, and enacting detailed legal provisions on digital offenses and their associated penalties must become integral parts of Indonesia’s legal reform agenda (Suari & Sarjana, 2023). Without these reforms, the legal protection of citizens’ personal data will remain fragile and vulnerable to exploitation by irresponsible parties.

CONCLUSION

The protection of personal data in the digital era is a fundamental element in safeguarding citizens' privacy rights. However, ongoing challenges in legal implementation, weak enforcement mechanisms, and delays in establishing an independent supervisory authority reflect that the current legal framework has yet to fully respond to the complexity of digital crimes. While the enactment of the Personal Data Protection Law (UU PDP) marks a positive initial step, it remains insufficient in addressing the need for a comprehensive and adaptive legal enforcement system.

In light of this, reforming digital criminal law is an urgent necessity. Indonesia must re-evaluate its criminal law framework to ensure it can effectively tackle the increasingly sophisticated and transnational nature of cybercrime. The European Union’s General Data Protection Regulation (GDPR) provides a strong and integrated legal model that can serve as a reference for Indonesia’s regulatory development. Such reform must include updating legal norms, strengthening institutional roles, and enhancing the capacity of law enforcement personnel in digital-related cases. Without holistic legal reform, the protection of personal data will remain vulnerable, and law enforcement efforts will continue to fall short of achieving the desired level of effectiveness.

REFERENCES

Ayiliani, F. M., & Farida, E. (2024). Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara. Jurnal Pembangunan Hukum Indonesia, 6(3), 431-455.

Bukit, A. N., & Ayunda, R. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat: The Urgency Ratification RUU PDP to the Protection Data Leakage Receive SMS Dana Cepat. Reformasi Hukum, 26(1), 1-20.

Daeng, Y., Levin, J., Karolina, K., Prayudha, M. R., Ramadhani, N. P., Noverto, N., ... & Virgio, V. (2023). Analisis penerapan sistem keamanan siber terhadap kejahatan siber di indonesia. Innovative: Journal Of Social Science Research, 3(6), 1135-1145.

Mahuli, J. I. (2023). Perlindungan Hukum Terhadap Data Pribadi dalam Era Digital. All Fields of Science Journal Liaison Academia and Sosiety, 3(4), 188-194.

Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU. Justisi, 10(1), 20-35.

Noviantama, D. (2023). Penegakan Hukum terhadap Pelaku Tindak Tindak Pidana Peretasan oleh Direktorat Reserse Kriminal Khusus Kepolisian Daerah Istimewa Yogyakarta (Doctoral dissertation, Universitas Islam Indonesia).

Prasetyo, B., Handayani, I. G. A. K. R., & Sulistiyono, A. (2025). Data Protection Laws in Indonesia: Navigating Privacy in the Digital Age. Side: Scientific Development Journal, 2(1), 9-16.

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.

Solikhah, M. A. (2025). Personal Data Protection in the Era of Digital Transformation: Challenges and

Solutions in the Indonesian Cyber Law Framework. Indonesian Cyber Law Review, 2(1), 39-50.

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. Jurnal Analisis Hukum, 6(1), 132-142.