PERSONAL DATA PROTECTION IN INDONESIA'S DIGITAL LAW ENFORCEMENT SYSTEM

Hadi Purnomo
Universitas Langlangbuana, Bandung, Indonesia
Email: hadipurnomo1104@gmail.com

Abstract

The rapid digitalization of law enforcement in Indonesia has increased the use of personal data in investigative, intelligence, and criminal justice processes. While digital technologies improve the effectiveness and efficiency of law enforcement, they also create significant risks to privacy rights and personal data protection. The enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) represents an important milestone in establishing a comprehensive legal framework for personal data protection. However, challenges remain in ensuring the effective implementation of personal data protection principles within digital law enforcement practices. This study aims to analyse the implementation of personal data protection in Indonesia's digital law enforcement system, identify the challenges encountered, and formulate strategies to strengthen legal protection mechanisms while maintaining a balance between law enforcement interests and the protection of individual privacy rights. This research employs normative legal research using statutory, conceptual, and comparative approaches. Legal materials were collected through library research consisting of primary, secondary, and tertiary legal sources and analysed qualitatively through inventorying, classifying, interpreting, and systematically examining relevant legal norms and doctrines. The findings indicate that the implementation of personal data protection remains constrained by the absence of specific technical regulations, limited institutional capacity, weak supervisory mechanisms, and the growing use of artificial intelligence, facial recognition, big data analytics, and digital surveillance technologies. The study also reveals a gap between regulatory norms and practical implementation that may undermine privacy rights and legal certainty. The novelty of this research lies in proposing an integrated strengthening model based on regulatory harmonization, independent oversight, institutional capacity building, and privacy-by-design principles to support accountable, transparent, and human rights-oriented digital law enforcement.

Keywords: *Personal Data Protection, Digital Law Enforcement, Privacy Rights, Digital Governance.*

A. INTRODUCTION

The development of information and communication technology has driven digital transformation across various sectors, including the law enforcement system. The utilization of digital technology by law enforcement agencies is becoming increasingly widespread, ranging from electronic evidence collection, digital data analysis, and online activity monitoring, to the use of artificial intelligence-based systems to support investigation processes (Sihombing et al., 2026). While this digitalization enhances the effectiveness and efficiency of law enforcement, it simultaneously poses new risks to the protection of public personal data. According to Nurarafah et al. (2025) the increasing use of digital technology by state institutions must be balanced with the strengthening of regulations and data protection mechanisms to prevent the misuse of personal information and to maintain public trust in law enforcement agencies.

Personal data protection has now become a global legal issue closely linked to the respect for privacy rights as a fundamental part of human rights. In various countries, data protection regulations have evolved into legal instruments that govern the boundaries of state authority in accessing, processing, and storing citizens' personal data. The presence of the General Data Protection Regulation (GDPR) in the European Union has become an international benchmark emphasizing the principles of legality, transparency, accountability, and the protection of data subjects' rights. In the context of law enforcement, the processing of personal data remains permissible for criminal investigation and prevention purposes; however, it must be conducted proportionally and in accordance with the principles of human rights protection (Khadzhiradieva et al., 2024).

In Indonesia, the state's commitment to protecting personal data is manifested through Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). The enactment of this law marks a significant milestone in establishing a more comprehensive data protection system. Nonetheless, the implementation of the UU PDP within the law enforcement sector still faces various challenges. Law enforcement officials hold the authority to access and process personal data for both preliminary and full criminal investigations, yet adequate technical guidelines regarding the limitations, oversight mechanisms, and accountability standards in managing such data remain unavailable. This condition potentially triggers legal uncertainty and the risk of violating the public's right to privacy.

This problem indicates a gap between the normative condition (*das sollen*) and the empirical condition (*das sein*). Normatively, the UU PDP mandates personal data protection that guarantees the rights of data subjects, transparency in data processing, and the accountability of the managing institutions. In practice, however, various cases of data breaches, weak oversight of data processing by state institutions, and suboptimal grievance mechanisms for citizens experiencing personal data violations are still encountered. Furthermore, technological advancements such as artificial intelligence (AI), facial recognition, big data analytics, and digital surveillance continue to expand the scope of data collection by law enforcement agencies without being accompanied by adaptive and comprehensive regulations.

Several previous studies have examined the issue of personal data protection within the context of law enforcement and digital technology. Antoliš (2023) examined jurisdictional conflicts between EU data protection law and US law enforcement access to cross-border digital evidence. Yang Zheng (2025) discussed the dynamics of data access regulations for law enforcement purposes within EU-US relations. Meanwhile, Almasoud & Idowu (2025) highlighted the risks of utilizing data and algorithms in predictive policing practices, which have the potential to cause discrimination and privacy violations. While these studies offer crucial insights into the relationship between data protection and law enforcement, they remain focused on the international context and do not specifically examine the implementation of personal data protection within the digital law enforcement system in Indonesia.

Additionally, most existing studies focus heavily on personal data protection in the digital economy, electronic services, and electronic-based government governance. Research specifically addressing personal data governance by law enforcement agencies remains relatively limited. In fact, law enforcement institutions are among the parties with extensive access to public personal data in executing technology-based intelligence, investigation, and enforcement functions. This limitation in existing literature reveals a research gap that needs to be addressed through a study focusing on personal data protection within Indonesia's digital law enforcement system.

The novelty of this study lies in its analysis of personal data protection within Indonesia's digital law enforcement system, with a specific focus on the regulatory, implementation, oversight, and challenging aspects of digital technology utilization by law

enforcement officials following the enactment of the UU PDP. Unlike previous studies that emphasize international jurisdiction, cross-border data access conflicts, or data protection in non-law enforcement sectors, this research specifically examines how personal data protection is applied within Indonesia's digital law enforcement system and formulates efforts to strengthen public privacy rights amidst digital technology advancements.

Based on the background, identifying the problems in this research is essential to address the increasingly complex challenges of personal data protection within the digital law enforcement system. Therefore, this study aims to analyse the implementation of personal data protection within the digital law enforcement system in Indonesia, identify the various challenges faced, and formulate recommendations for strengthening regulations and data protection mechanisms capable of ensuring a balance between law enforcement interests and the protection of public privacy rights.

B. METHOD

This study is a normative legal research that aims to analyse personal data protection within the digital law enforcement system in Indonesia. The approaches utilized include the statute approach, the conceptual approach, and the comparative approach. The research specification is descriptive-analytical, examining various statutory regulations, legal concepts, and literature related to personal data protection in digital law enforcement. The data collection method is conducted through library research, utilizing primary, secondary, and tertiary legal materials relevant to the object of research. Data analysis is performed qualitatively through the process of inventorying, classifying, interpreting, and systematizing legal materials to obtain answers to the research problems. According to Soekanto & Mamudji (2010) normative legal research is conducted by examining library materials or secondary data as a basis for analyzing legal issues, whereas according to Marzuki (2017) legal research aims to discover legal rules, legal principles, and legal doctrines to answer the legal issues faced.

C. RESULTS AND DISCUSSION

1. Implementation of Personal Data Protection in Indonesia's Digital Law Enforcement

Digital transformation has altered how law enforcement agencies exercise their duties and authority. The utilization of digital technology in the processes of preliminary inquiry, full criminal investigation, and electronic evidence collection has enhanced the effectiveness of law enforcement. Various forms of digital data, such as electronic identities, communication metadata, CCTV footage, social media activities, and electronic transaction information, have become vital sources of information in uncovering criminal offenses. In this context, personal data protection has become an inseparable aspect of the digital law enforcement system. According to Riswanto et al. (2024) while the digitalization of law enforcement facilitates the disclosure of criminal offenses, it simultaneously introduces risks to the security and confidentiality of personal data managed by law enforcement officials.

The enactment of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) serves as a significant step toward establishing a data protection legal framework in Indonesia. This law provides recognition for the rights of data subjects while establishing obligations for parties processing personal data. Within the law enforcement sector, the processing of personal data is permitted for the purposes of preliminary inquiry, full criminal investigation, prosecution, and the execution of court decisions. Nonetheless, the use of personal data must strictly adhere to the principles of legality, clear purpose, accountability, and the protection of public privacy rights. Pratiwi et al. (2024) personal data protection is an integral part of human rights protection that demands legal certainty over every form of data collection and processing by both state institutions and private entities.

Although personal data protection has normatively acquired an adequate legal basis, its implementation in digital law enforcement practices still encounters various obstacles. The unavailability of technical regulations specifically governing personal data governance by law enforcement officials has led to disparate practices in data collection, storage, utilization, and destruction. This condition potentially triggers legal uncertainty and increases the risk of personal data misuse. Pakina & Solekhan (2024) explain that the advancement of digital surveillance technology, if not balanced with adequate regulations and oversight mechanisms, can lead to violations of privacy rights and diminish the accountability of law enforcement institutions in managing personal data.

From a legal protection perspective, the existence of regulation functions not only as an instrument to control state power but also as a means to protect citizens' rights. Therefore, the implementation of personal data protection in digital law enforcement must be positioned as part of the efforts to ensure a balance between law enforcement interests and respect for public privacy rights. Aji (2023) asserts that strengthening the personal data protection system is a vital prerequisite for realizing accountable digital governance capable of maintaining a balance between national security interests and the protection of citizens' rights in the era of digital transformation.

2. Challenges of Personal Data Protection in the Digital Law Enforcement System

The advancement of digital technology presents new challenges for personal data protection. Law enforcement officials now have increasingly extensive access to various types of digital data stored on electronic devices and digital platforms. On one hand, this condition supports the effectiveness of law enforcement in uncovering information technology-based crimes. On the other hand, this expansion of access increases the potential for privacy rights violations if it is not balanced with adequate oversight mechanisms. According to Ade Rizki Saputra (2023) the development of digital technology has broadened the space for personal data processing, thereby requiring legal arrangements capable of ensuring a balance between security interests and the protection of individual rights. This condition indicates that digital transformation in law enforcement must be followed by the strengthening of the personal data protection system to prevent the abuse of authority by state institutions.

One of the primary challenges is the lack of comprehensive standard operating procedures regarding the management of personal data in the law enforcement process. Ambiguity regarding the boundaries of data access authority, data retention periods, data erasure mechanisms, and information security procedures potentially leads to the abuse of power. Furthermore, low data protection literacy among law enforcement officials also affects the effective implementation of Law Number 27 of 2022 concerning Personal Data Protection. Pratiwi et al. (2024) explain that personal data protection requires not only the presence of adequate regulations but also institutional readiness and human resources capable of implementing data protection principles consistently. Accordingly, capacity building for law enforcement officials is a crucial part of strengthening the effectiveness of personal data protection in the digital era.

Other challenges arise from the use of artificial intelligence (AI)-based technology, facial recognition, big data analytics, and digital surveillance systems. These technologies enable faster and more massive identification, tracking, and analysis of individual behaviour. However, their utilization also poses risks of algorithmic discrimination, misidentification, and excessive data collection. Alikhademi et al. (2022) explains that the use of algorithms in predictive policing practices has the potential to generate bias and discrimination unless accompanied by strict oversight mechanisms. In addition, Renuka et al. (2024) emphasizes that the expansion of data access by law enforcement officials in the digital environment creates new challenges related to privacy rights protection and data utilization accountability.

Therefore, the use of digital technology in law enforcement must incorporate the principles of proportionality, transparency, and accountability so as not to conflict with human rights.

Aside from regulatory and technological factors, institutional challenges also represent a significant issue. To date, oversight mechanisms for personal data processing by law enforcement officials remain suboptimal. This condition leaves the public with limited options for obtaining legal protection when their privacy rights are violated. Pakina & Solekhan (2024) state that weak oversight over the use of information technology by state institutions can elevate the risk of personal data misuse and lower public trust in law enforcement agencies. The absence of an effectively functioning supervisory authority also hinders the accountability process when personal data breaches occur. Consequently, strengthening oversight mechanisms, increasing transparency, and establishing easily accessible public grievance systems have become urgent necessities to support personal data protection within Indonesia's digital law enforcement system.

3. The Gap between Regulation and Practice in Personal Data Protection

Normatively, Indonesia possesses various legal instruments that provide protection for the personal data and privacy rights of its citizens. In addition to Law Number 27 of 2022 concerning Personal Data Protection, such protection can also be found in the 1945 Constitution of the Republic of Indonesia, the Electronic Information and Transactions Law, and various other sectoral regulations. The existence of these diverse legal instruments demonstrates the state's commitment to guaranteeing the protection of privacy rights as an integral part of human rights. According to Rosadi (2023) the enactment of the Personal Data Protection Law is a strategic step toward building a comprehensive data protection system aligned with global developments in data protection law. However, the existence of these regulations has not fully addressed the data protection needs within the increasingly complex practices of digital law enforcement.

The gap between the normative and implementational aspects is evident in the lack of harmonization among various regulations governing data access by law enforcement officials. Several provisions still leave broad room for interpretation, potentially leading to actions that run counter to personal data protection principles. Consequently, there is a risk that law enforcement interests are prioritized over the protection of public privacy rights. Shurson (2020) explains that in digital law enforcement practices, tension frequently arises between the necessity of data access for investigation purposes and the state's obligation to protect individual privacy rights. A similar condition is observed in Indonesia, where the data access authority held by law enforcement officials has not been fully balanced with clear oversight mechanisms and limitations, thereby creating potential violations of data subjects' rights.

This condition illustrates a discrepancy between *das sollen* and *das sein*. Normatively, personal data protection is positioned as a right that must be respected and protected by the state. In practice, however, oversight, accountability, and rights-restoration mechanisms for victims of personal data violations have not functioned optimally. Christakis & Terpan (2021) state that personal data protection within the law enforcement sector requires a balance between security interests and respect for the fundamental rights of citizens. When oversight mechanisms fail to operate effectively, the exemptions granted to law enforcement officials run the risk of expanding into unchecked authority. Therefore, the gap between norms and practice underscores the urgency of regulatory strengthening and institutional reform to ensure that personal data protection does not remain confined to the normative realm.

From a constitutional state (*rechtsstaat*) perspective, every action taken by law enforcement officials must be grounded in law that is clear, proportional, and accountable. According to Wicaksono & Yasin (2024) cyber law and data protection reforms must be directed toward establishing a supervisory system capable of guaranteeing legal certainty

alongside the protection of human rights in the digital era. Accordingly, strengthening the principles of personal data protection is vital to achieving a digital law enforcement system that is just and respectful of human rights. This effort requires not only regulatory refinement but also institutional capacity building, the harmonization of statutory regulations, and the establishment of an independent and effective supervisory mechanism to oversee personal data processing by law enforcement officials.

4. Strengthening Personal Data Protection in Digital Law Enforcement

Efforts to strengthen personal data protection within the digital law enforcement system must be pursued through regulatory, institutional, and technological approaches. From the regulatory aspect, the government needs to draft implementing regulations that specifically govern personal data governance by law enforcement officials. These regulations must incorporate provisions regarding data access procedures, data storage, data erasure, information security audits, and accountability mechanisms in the event of violations. According to Rosadi (2023) the effectiveness of personal data protection is determined not only by the existence of a statute but also by the availability of implementing instruments capable of providing legal certainty in practice. Therefore, harmonization between the Personal Data Protection Law and various sectoral regulations related to law enforcement serves as a crucial step to mitigate potential conflicts of norms and reinforce public privacy rights protection.

From the institutional aspect, strengthening the supervisory function over personal data processing is required. The presence of an independent supervisory authority will reinforce accountability and ensure that the utilization of personal data by law enforcement officials remains within legal boundaries and human rights principles. Additionally, sustainable institutional capacity building through education and training on personal data protection must be consistently conducted. Pratiwi et al. (2024) explain that the successful implementation of personal data protection is heavily influenced by institutional quality and the ability of officials to understand data protection principles. Thus, institutional strengthening is oriented not only toward establishing supervisory mechanisms but also toward enhancing the professionalism of law enforcement officials in managing personal data responsibly.

From the technological aspect, the application of *privacy by design* and *privacy by default* principles must become an integral part of digital law enforcement system development. Every technology deployed for law enforcement purposes must be engineered with data protection considerations from the initial stages of system architecture. This approach can minimize the risk of privacy violations while elevating public trust in law enforcement institutions. According to Wempy et al. (2024) strengthening cybersecurity and privacy protection must serve as primary elements in any digital technology development utilized by state institutions. Furthermore, the use of technologies such as artificial intelligence, facial recognition, and big data analytics must be accompanied by algorithmic audit mechanisms, risk evaluations, and independent oversight to prevent data misuse or algorithm-based discrimination.

Strengthening personal data protection also necessitates the adoption of best practices established within the international legal system. Shurson (2020) asserts that data access by law enforcement officials must be executed based on the principles of legality, necessity, and proportionality to avoid diminishing the protection of citizens' privacy rights. Implementing these principles is vital in the Indonesian context, given the expanding use of digital technology in law enforcement processes. With clear standards governing the access and utilization of personal data, a balance between law enforcement interests and human rights protection can be better secured.

Consequently, personal data protection in digital law enforcement requires not only adequate regulations but also institutional strengthening, effective oversight, and the

deployment of human rights-oriented technology. This comprehensive approach is an essential prerequisite for realizing an accountable, transparent, and equitable digital law enforcement system. Beyond reinforcing public confidence in law enforcement institutions, this step represents a concrete implementation of a constitutional state that guarantees the protection of privacy rights as a fundamental component of human rights in the digital era.

D. CONCLUSION

Personal data protection within Indonesia's digital law enforcement system has normatively gained a strong legal foundation through Law Number 27 of 2022 on Personal Data Protection; however, its implementation remains constrained by the absence of specific technical regulations, weak oversight mechanisms, limited institutional capacity, and the growing use of advanced digital technologies such as artificial intelligence, facial recognition, and big data analytics. This study finds a significant gap between regulatory norms and practical implementation, creating risks to privacy rights and legal uncertainty in personal data governance by law enforcement agencies. The novelty of this research lies in its analysis of personal data protection specifically within Indonesia's digital law enforcement framework and its formulation of a strengthening model based on regulatory harmonization, independent supervision, institutional capacity building, and the adoption of privacy-oriented technological safeguards. Therefore, strengthening personal data protection is essential to ensure a digital law enforcement system that remains effective, accountable, transparent, and aligned with the protection of human rights in the digital era.

REFERENCES

Ade Rizki Saputra. (2023). Aspects of Personal Data Protection According to International Law. *Formosa Journal of Social Sciences (FJSS)*, *2*(3). https://doi.org/10.55927/fjss.v2i3.6192

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi). *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *13*(2). https://doi.org/10.22212/jp.v13i2.3299

Alikhademi, K., Drobina, E., Prioleau, D., Richardson, B., Purves, D., & Gilbert, J. E. (2022). A review of predictive policing from the perspective of fairness. *Artificial Intelligence and Law, 30*(1). https://doi.org/10.1007/s10506-021-09286-4

Almasoud, A. S., & Idowu, J. A. (2025). Algorithmic fairness in predictive policing. *AI and Ethics*, *5*(3). https://doi.org/10.1007/s43681-024-00541-3

Antoliš, K. (2023). The Challenges of Collecting Digital Evidence Across Borders. *Policija i Sigurnost*, *32*(3). https://doi.org/10.59245/ps.32.3.2

Christakis, T., & Terpan, F. (2021). EU-US negotiations on law enforcement access to data: Divergences, challenges and EU law procedures and options. *International Data Privacy Law, 11*(2). https://doi.org/10.1093/idpl/ipaa022

Khadzhiradieva, S., Bezverkhniuk, T., Nazarenko, O., Bazyka, S., & Dotsenko, T. (2024). Personal data protection: Between human rights protection and national security. *Social and Legal Studios*, *7*(3). https://doi.org/10.32518/sals3.2024.245

Marzuki, P. M. (2017). *Penelitian Hukum: Edisi Revisi*. Jakarta: Kencana.

Nurarafah, N., Sulaiman, Kurniasari, T. W., & Husni. (2025). Perlindungan Data Pribadi pada Transaksi Digital. *AL-BUYU': Jurnal Hukum Ekonomi Syari'ah*, *2*(1), 104–114.

Pakina, R., & Solekhan, M. (2024). Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan di Indonesia: Keseimbangan Antara Keamanan dan Hak Asasi Manusia. *Journal of Scientech Research and Development*, *6*(1).

Pratiwi, S. C. G., Nababan, R., & Juliana, S. R. (2024). Peran Hukum Dalam Melindungi Data Pribadi. *Innovative: Journal Of Social Science Research*, *4*.

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2024). Data Privacy and Protection: Legal and Ethical Challenges. In *Emerging Threats and Countermeasures in Cybersecurity*. https://doi.org/10.1002/9781394230600.ch19

Riswanto, Muh. F., Kamal, M., & Badaru, B. (2024). Pelaksanaan Fungsi Kepolisian Dalam Menanggulangi Perjudian Online. *Journal of Lex Philosophy (JLP)*, *5*(1).

Rosadi, S. D. (2023). Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*.

Shurson, J. (2020). Data protection and law enforcement access to digital evidence: Resolving the reciprocal conflicts between EU and US law. *International Journal of Law and Information Technology*, *28*(2). https://doi.org/10.1093/ijlit/eaaa011

Sihombing, L. A., Nuraeni, Y., Rozaan, R., Pranadita, N., & Syam, R. Z. A. (2026). Can Digital Restorative Mediation Transform Indonesia's Criminal Procedure Law and Deliver Justice? *Petita: Jurnal Kajian Ilmu Hukum dan Syariah*, *11*(1). https://doi.org/10.22373/petita.v11i1.886

Soekanto, S., & Mamudji, S. (2010). *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Depok: Raja Grafindo Persada.

Wempy, A., Efendi, Z., & Putra, M. D. (2024). Regulation of Cybersecurity Technology as an Effort to Address Security Threats to Privacy in the Digital Era. *Jurnal Hukum Sehasen*, *10*(2). https://doi.org/10.37676/jhs.v10i2.6732

Wicaksono, A. T., & Yasin, I. F. (2024). Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection. *Al-Jinayah: Jurnal Hukum Pidana Islam*, *10*(2). https://doi.org/10.15642/aj.2024.10.2.237-261

Yang Zheng. (2025). Global Law and Cross-Border Data Security: From the Perspective of Cross-Border Regulatory Cooperation. *Law, Economics and Society*, *1*(2). https://doi.org/10.30560/les.v1n2p43