

Law Enforcement Against Violations Of Privacy Rights Resulting From The Use Of Personal Data Without Consent In Electronic Media To Create Legal Awareness In Society

Yenny Febrianty¹; Dina Nur Maulidiah Jamil ²; Fauzan Azima Faturachman ³.

Doctor of Law Program, Graduate School Pakuan University, Indonesia¹,

Faculty of Economics & Business Pakuan University, Indonesia²

Faculty of Law Pakuan University, Indonesia³.

Jalan Pakuan, Tegallega, Central Bogor District, Bogor City, West Java 16143.

E-mail: yenny.febrianty@unpak.ac.id, dina.nmj@unpak.ac.id, fznazima3@gmail.com.

Manuscripts received : 01/07/2026. Revision and Review : 20/07/2026. Approved 04/08/2026

Abstract

The development of information technology has increased the intensity of the use of personal data in various activities through electronic media, but on the other hand, it has also given rise to various violations of privacy rights due to the use of personal data without the owner's consent. Although Indonesia has Law Number 27 of 2022 concerning Personal Data Protection and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, the effectiveness of law enforcement still faces various challenges. This study aims to analyze law enforcement against violations of privacy rights due to the use of personal data without consent in electronic media, based on Indonesian positive law, and to formulate an ideal concept of law enforcement to realize public legal awareness. This study uses an empirical juridical legal research method with a statutory approach, a conceptual approach, and an empirical approach. Data were obtained through literature studies and interviews with academics and law enforcement practitioners, then analyzed qualitatively using Lawrence M. Friedman's legal system theory, Soerjono Soekanto's theory of legal effectiveness and legal awareness, and Hans Kelsen's theory of legal norms. The results of the study indicate that law enforcement against violations of privacy rights has an adequate normative basis, but its implementation is not optimal due to the lack of harmonization of regulations, the limited capacity of law enforcement officers, the complexity of electronic evidence, and low public legal awareness. This study offers an ideal concept of law enforcement through strengthening legal substance, legal structure, and legal culture in an integrated manner as a law enforcement model that is not only oriented towards enforcement, but also on building public legal awareness in protecting personal data in the digital era.

Keywords: Law Enforcement, Privacy Rights, Personal Data, Personal Data Protection, Legal Awareness.

A. Introduction

Digital transformation has transformed nearly every dimension of modern society. The development of information and communication technology, marked by the massive use of the internet, social media, *cloud computing*, *big data*, the *Internet of Things* (IoT), and artificial intelligence (AI), has given rise to a digital space that enables the exchange of information to occur quickly, massively, and without national jurisdictional boundaries.

Digitalization has not only changed people's communication patterns but also transformed economic activities, government, education, public services, and financial transaction systems, which are increasingly dependent on the processing of personal data. In this digital ecosystem, personal data has developed into a strategic asset (*new oil*) that has economic, social, and political value, making it highly vulnerable to various forms of abuse. This condition means that personal data protection is no longer seen as a mere administrative or technical issue, but has developed into a legal issue closely related to respect for human rights, cybersecurity, and guaranteeing legal certainty in a democratic state based on the rule of law.¹

The right to privacy is a fundamental right inherent in every individual as an inseparable part of human rights. From a modern legal perspective, the right to privacy is not only defined as a person's right to be free from interference by others in their private life, but also includes the right to determine how information about them is collected, used, processed, stored, and disseminated. With the development of digital technology, the scope of personal data is no longer limited to basic identities such as name, address, or national identity number, but has also included photographs, voice recordings, fingerprints, biometric data, geographic location, digital activity, and biological characteristics that can specifically identify an individual. Therefore, any form of processing of personal data without the data owner's consent is essentially a violation of the right to privacy that has the potential to cause material and immaterial losses, including loss of security, damage to reputation, misuse of identity, digital discrimination, and violations of human dignity.²

The urgency of personal data protection is increasingly prominent with the rise in cases of personal data misuse in Indonesia. The phenomena of data breaches, the distribution of photos without consent, identity theft, doxing, *image manipulation through deepfake* technology, and the misuse of biometric data demonstrate that threats to privacy rights are no longer hypothetical but have become real issues in the digital society.³ This condition is reflected in the increasing public attention to the issue of personal data protection. According to a report from the Directorate General of Digital Space Supervision at the Ministry of Communication and Digital, from October 2024 to November 2025, 342 complaints were received through personal data protection services, with approximately 41% of them directly related to alleged personal data protection violations. In addition, there were 483 consultation requests, of which approximately 89% discussed personal data protection issues. This data indicates that the issue of personal data protection has become a digital law issue that is gaining increasing public attention and emphasizes the growing need for legal certainty and effective protection mechanisms.⁴

The increasing number of privacy violations demonstrates that the development of digital technology is not always accompanied by increased public legal awareness regarding respecting the privacy rights of others. The ease of accessing, duplicating, modifying, and

¹ Dian Sudiantini, et al, "Digital Transformation: Impact, Challenges, and Opportunities for Digital Economic Growth", *Trending: Journal of Economics, Accounting and Management*, published by Universitas 45 Surabaya, (Vol. 1 No. 3, 2023): 21-30.

² Nur Azizah Qurrotuaini, "The Right to Privacy as a Constitutional Right in the Digital Era: A Juridical Study from a Cyber Law Perspective", *Staatsrecht: Journal of Islamic State and Political Law*, published by the Faculty of Law, UIN Sunan Kalijaga, (Vol. 4 No. 2 of 2024): 236-254.

³ Yusuf Daeng, et al, "Personal Data Protection in the Digital Era: A Review of the Legal Framework for Privacy Protection", *Innovative: Journal of Social Science Research*, published by Pahlawan Tuanku Tambusai University, (Vol. 3 No. 6 of 2023): 2898-2905.

⁴ Detikinet, "Komdigi Receives Hundreds of Complaints about Personal Data Protection", available at: <https://inet.detik.com/law-and-policy/d-8281251/komdigi-terima-ratusan-aduan-soal-perlindungan-data-pribadi>, accessed May 29, 2026.

disseminating information through electronic media has created various new forms of violations that are difficult to address using conventional legal approaches. In practice, the distribution of a person's photo without consent, the use of faces for commercial purposes, the publication of personal data through social media, and the use of facial recognition technology *are* often carried out without considering the aspect of consent *or* the rights of personal data subjects. ⁵In fact, in many cases, these violations are considered commonplace due to low digital literacy and the public's lack of understanding of the legal consequences of using personal data without consent. This phenomenon demonstrates that the main problem of personal data protection is not only related to regulatory aspects, but also concerns the legal culture *of* society, which has not fully recognized the right to privacy as a right that must be respected and protected.

As a state of law (*rechtstaat*), Indonesia has actually built a normative foundation that is adequate enough to provide protection for the right to privacy and personal data. Recognition of these rights is constitutionally reflected in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees protection for the individual, family, honor, dignity, and sense of security for every citizen, ⁶and Article 28H paragraph (4) guarantees the right of every person to own personal property that may not be taken arbitrarily. ⁷In subsequent developments, protection of personal data was emphasized through Article 26 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law), which emphasizes that the use of any information concerning a person's personal data must be carried out with the consent of the person concerned. ⁸The state's commitment was further strengthened by the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which establishes a specific legal regime concerning the rights of personal data subjects, the obligations of data controllers and processors, data processing principles, legal accountability mechanisms, and the imposition of administrative and criminal sanctions for personal data violations. The PDP Law marks a paradigm shift from personal data protection, previously scattered across various sectoral regulations, to a more comprehensive and integrated protection system.

Although Indonesia has a relatively comprehensive legal framework through the Personal Data Protection Law (PDP), this regulation has not fully addressed the complexity of privacy violations, which continue to evolve with advances in digital technology. The main problem currently lies not in the absence of legal frameworks, but rather in the effectiveness of their implementation in practice. Law enforcement against privacy violations still faces various challenges, ranging from low public legal awareness, suboptimal inter-agency coordination, limited capacity of law enforcement officers to handle electronic evidence, and the cross-jurisdictional nature of cybercrime. Consequently, the legal protections that have been normatively guaranteed through various laws and regulations have not fully provided a sense of security and legal certainty for the public as subjects of personal data.

The enactment of the Personal Data Protection Law (PDP) is indeed a significant advancement in the Indonesian legal system, but its implementation still faces various

⁵ Nur Azizah Qurrotuaini, "The Right to Privacy as a Constitutional Right in the Digital Era: A Juridical Study from a Cyber Law Perspective", *Staatsrecht: Journal of Islamic State and Political Law*, published by the Faculty of Law, UIN Sunan Kalijaga, (Vol. 4 No. 2 of 2024): 236-254.

⁶ Indonesia, *Constitution of the Republic of Indonesia*, 1945 Constitution, Article 28G (1).

⁷ Indonesia, *Constitution of the Republic of Indonesia*, 1945 Constitution, Article 28H (4).

⁸ Indonesia, *Law on the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions*, Law Number 1 of 2024, LN No. 1 of 2024, TLN No. 6905, article 26.

obstacles, including low public awareness, weak oversight, suboptimal law enforcement, and the lack of a truly independent oversight body. Another equally important challenge is the need for synchronization between laws and regulations to avoid overlapping authority and legal uncertainty in practice. This perspective demonstrates that the effectiveness of personal data protection is not only determined by the quality of regulations, but also influenced by institutional readiness and the legal culture of society in respecting the right to privacy as part of human rights.⁹

These findings align with Lawrence M. Friedman's perspective, which explains that the functioning of a legal system is determined by the integration of legal structure, legal substance, and legal culture. In ¹⁰ In the context of personal data protection in Indonesia, the legal substance has essentially undergone significant development through the establishment of the Personal Data Protection Law. However, the legal structure still faces various limitations, particularly in terms of institutional coordination, the capacity of law enforcement officers, and the readiness of digital forensic infrastructure. On the other hand, the legal culture of society has not yet demonstrated an adequate level of compliance with the principle of respect for the right to privacy, as reflected in the continued widespread use of photos, videos, and personal data without consent. Thus, the issue of personal data protection is actually a problem of the legal system as a whole, not merely a matter of establishing new legal norms.

In law enforcement practice, handling personal data breach cases still faces various obstacles, both technical and legal. These obstacles include the difficulty of identifying perpetrators, the ease with which electronic evidence can be deleted or manipulated, the limited availability of digital forensic experts, and jurisdictional issues when the perpetrators and servers are located outside of Indonesia. In fact, he said, the success of the prosecution process depends heavily on the ability of authorities to maintain *the chain of custody*, *conduct metadata* analysis, utilize *digital forensic* results, and ensure that electronic evidence is obtained through legal procedures according to criminal procedure law. This fact shows that the effectiveness of law enforcement against violations of privacy rights in the digital era is no longer solely determined by the existence of criminal provisions, but also by the readiness of human resources, technological support, and electronic evidence mechanisms that are adaptive to the development of cybercrime.¹¹

From the perspective of the theory of legal effectiveness put forward by Soerjono Soekanto, this condition shows that law enforcement against violations of privacy rights is influenced by various interrelated factors, namely the law itself, law enforcement officials, supporting facilities or infrastructure, society, and culture. ¹²Thus, the success of personal data protection cannot be measured only by the number of regulations established or the number of cases processed through the judicial mechanism, but also by the extent to which the law is able to shape public behavior to respect the right to privacy as part of the legal culture. In this context, increasing public legal awareness is one of the main prerequisites for the realization of effective personal data protection.

Many researchers have previously conducted studies on personal data protection. Some studies focus on normative analysis of the provisions on personal data protection in

⁹Desy Maryani, Lecturer in Criminal Law Faculty of Law, Daehasen University, Bengkulu, *Interview*, June 15, 2026

¹⁰ Lawrence M. Fredman, *The Legal System: A Social Science Perspective*, (New York: Russell Sage Foundation, 1975), p. 5-6.

¹¹Rima Eka Hardiyani, Head Subsection Pre-prosecution Sexy General Crimes, Cilegon District Attorney's Office, *Interview*, June 22, 2026

¹² Soerjono Soekanto, *Factors Influencing Law Enforcement*, (Jakarta: Rajawali Press, 2010), p. 8.

the ITE Law and the PDP Law. Others focus more on criminal liability, human rights protection, or comparisons of personal data protection legal systems across countries. While these studies have made important contributions to the development of legal science, they generally still position personal data protection as a normative issue, resulting in few studies examining the effectiveness of legal implementation from a holistic legal system perspective that integrates regulatory, institutional, and legal culture dimensions.

Based on these conditions, this study has a different position from previous research. This study not only examines law enforcement against privacy rights violations from the perspective of Indonesian positive law, but also integrates analysis using Lawrence M. Friedman's legal system theory, Hans Kelsen's legal norm theory, Soerjono Soekanto's legal awareness theory, and empirical data obtained through interviews with academics and law enforcement practitioners. This integration of the normative approach and empirical data is expected to provide a more comprehensive picture of the factors influencing the effectiveness of law enforcement against privacy rights violations in the digital space.

Based on this, the novelty of this research lies in the formulation of an integrative model for enforcing personal data protection laws based on strengthening the legal system and public legal awareness, namely a concept that positions the effectiveness of law enforcement as a result of synergy between strengthening legal substance, optimizing law enforcement structures, developing digital forensic capacity, institutional harmonization, increasing digital literacy, and establishing a legal culture in society that respects the right to privacy. This model is expected not only to contribute to the development of legal science but also to become a conceptual recommendation for the formation of personal data protection policies that are more adaptive to developments in information technology.

Based on these various problems, the author believes that research is important to conduct. The urgency of this research is not only based on the increasing number of forms of personal data violations in the digital era, but also on the need to evaluate the effectiveness of law enforcement from the perspective of positive Indonesian law and to formulate an ideal concept that can answer the challenges of information technology development. Through a normative approach strengthened by empirical data from interviews, this research is expected to be able to provide theoretical contributions to the development of personal data protection laws while offering conceptual recommendations for policymakers, law enforcement officers, and the public in realizing a personal data protection system that is effective, fair, and oriented towards increasing public legal awareness. On that basis, this research is focused on answering two main problems, namely: (1) how to enforce the law against violations of the right to privacy due to the use of personal data without consent on electronic media from the perspective of positive Indonesian law; and (2) what is the ideal concept of law enforcement against violations of the right to privacy due to the use of personal data without consent on electronic media to raise public legal awareness.

B. Research methods

This study employs a normative legal research method supported by empirical data. This method was chosen because the primary objective of this study is the legal norms governing the protection of privacy rights regarding the unauthorized use of personal data in electronic media, as stipulated in various laws and regulations in Indonesia. Empirical data is used to support the analysis, providing a clear picture of the implementation of law enforcement in practice. Therefore, the resulting analysis is not only normative but also reflects the actual conditions occurring in society.

The research approaches used include the statute approach, the conceptual approach, and the case approach. The statutory approach is used to examine various legal provisions related to the protection of privacy rights and personal data, including the 1945 Constitution of the Republic of Indonesia, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, the Criminal Code, the Criminal Procedure Code, and various other laws and regulations related to personal data protection. The conceptual approach is used to analyze various theories that form the basis of the research, namely Lawrence M. Friedman's legal system theory, the theory of legal effectiveness, Soerjono Soekanto's legal awareness theory, and Hans Kelsen's legal norm theory. The case approach is used to analyze various forms of violations of privacy rights due to the use of personal data that occur through electronic media as an illustration of the implementation of legal norms in practice.

The data sources in this study consist of primary legal materials, secondary legal materials, and primary data from interviews. Primary legal materials include laws and regulations related to the protection of privacy rights and personal data. Secondary legal materials were obtained from law books, scientific articles, national and international journals, research results, and various literature relevant to the research object. Primary data were obtained through interviews with legal academics and law enforcement agencies to gain perspectives on the implementation of law enforcement against violations of privacy rights due to the use of personal data in practice.

The legal material collection technique was conducted through library research, reviewing various laws and regulations, literature, and research findings related to the research object. Furthermore, primary data collection techniques were conducted through structured interviews with informants selected based on their competence and relevance to the research theme. The results of these interviews were used as supporting data to strengthen the normative analysis regarding the effectiveness of law enforcement against violations of privacy rights regarding the use of personal data in electronic media.

The analysis of legal materials and research data was conducted qualitatively using descriptive-analytical methods. All legal materials and interview data were analyzed systematically through a process of inventory, classification, interpretation, and legal argumentation, then linked to Lawrence M. Friedman's legal system theory, Soerjono Soekanto's theory of legal effectiveness and legal awareness, and Hans Kelsen's theory of legal norms. Through this approach, it is hoped that a comprehensive analysis will be obtained regarding the effectiveness of law enforcement against violations of privacy rights due to the use of personal data without consent in electronic media, as well as the ideal concept of law enforcement that is able to realize public legal awareness.

C. Results and Discussion

1. Law Enforcement Against Violations of Privacy Rights Due to the Use of Personal Data Without Consent on Electronic Media from the Perspective of Indonesian Positive Law

The development of information technology has brought significant changes to the way people communicate, transact, and exchange information through electronic media. Despite these conveniences, new legal issues have emerged, including the increasing misuse of personal data without the owner's consent. Personal data, once viewed solely as identity information, has now evolved into a legal right to privacy that carries legal value and must be protected by the state. Therefore, the use of personal

data without consent not only harms the individual concerned but also violates citizens' constitutional right to personal protection.

In the Indonesian legal system, protection of the right to privacy has a strong legal basis through Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees the right of every person to protection of themselves, their families, their honor, their dignity, and their sense of security.¹³ This constitutional guarantee is then implemented in Article 26 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, which requires the use of personal data based on the consent of the data subject,¹⁴ and is strengthened through Law Number 27 of 2022 concerning Personal Data Protection, which regulates the rights and obligations of the parties, personal data processing mechanisms, and sanctions for any violations.¹⁵ The presence of these regulations demonstrates the state's commitment to building a more comprehensive personal data protection system in the digital era.

However, the existence of these legal instruments has not been fully accompanied by effective law enforcement. Numerous cases of unauthorized dissemination of personal data, identity theft, data leaks by electronic system administrators, and the use of personal data for commercial purposes continue to demonstrate that people's privacy rights are not yet optimally protected. This situation indicates that the primary issue no longer lies in the availability of legal norms, but rather in how those norms are consistently implemented by law enforcement officials, electronic system administrators, and the public as users of digital technology.

Protection Law represents a significant advancement in the national legal system, but its effectiveness remains fraught with regulatory harmonization, institutional strengthening, oversight mechanisms, and public understanding of the right to personal data.¹⁶ Similarly, the practical handling of personal data breach cases still faces challenges, particularly in the areas of electronic evidence, digital forensics, and inter-institutional coordination, particularly when the cases involve cross-jurisdictional issues. These empirical findings demonstrate that the effectiveness of law enforcement is determined not only by the quality of the legal substance but also by the readiness of the authorities and supporting systems to implement applicable provisions.¹⁷

Based on this description, discussions regarding law enforcement against privacy violations related to the use of personal data cannot be conducted solely through a normative approach. They also require analysis based on current law enforcement practices in Indonesia. This analysis is crucial for assessing the extent to which existing legal mechanisms are capable of protecting people's privacy rights and for identifying various factors that influence the effectiveness of law enforcement in realizing personal data protection in the digital age.

Law enforcement against violations of privacy rights regarding the use of personal data in Indonesia is implemented through administrative, civil, and criminal mechanisms, depending on the nature of the violation. This approach demonstrates that personal data protection is not solely focused on imposing sanctions on

¹³ Indonesia, *Constitution of the Republic of Indonesia*, 1945 Constitution, Article 28G (1).

¹⁴ Indonesia, *Law on the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions*, Law Number 1 of 2024, LN No. 1 of 2024, TLN No. 6905, article 26.

¹⁵ Indonesia, *Law on Personal Data Protection*, Law Number 27 of 2022, LN No. 196 of 2022, TLN No. 6820.

¹⁶ Desy Maryani, *log cit*

¹⁷ Rima Eka Hardiyani, *log cit*.

perpetrators but also aims to restore the rights of affected data subjects. In practice, administrative mechanisms are applied to violations related to the data controller's obligations, while civil and criminal mechanisms are used when the misuse of personal data results in losses or meets the elements of a criminal offense as stipulated in laws and regulations.¹⁸

Law enforcement involves various institutions with varying authorities. Law enforcement officers play a role in the investigation, inquiry, prosecution, and court hearings, while ministries or agencies authorized to protect personal data carry out oversight and enforce administrative sanctions. This ¹⁹The multi-institutional law enforcement pattern essentially reflects the state's efforts to provide comprehensive legal protection. However, inter-institutional coordination is crucial for the successful handling of any personal data breach case.

The effectiveness of law enforcement can be seen in several cases that have occurred in Indonesia. One example that has received widespread public attention is the personal data leak at the Temporary National Data Center (PDNS) in 2024, which disrupted various public services and demonstrated the significant risks posed by data management systems not supported by adequate cybersecurity governance. Furthermore, numerous cases of identity theft and the dissemination of personal data through social media processed under the ITE Law also demonstrate that privacy violations are no longer incidental but have become a real legal issue in the digital age. These cases demonstrate that despite the availability of legal instruments, effective law enforcement still faces challenges in providing swift, appropriate protection and optimally restoring victims' rights.²⁰

Handling personal data breach cases differs from conventional criminal offenses. The evidentiary process relies heavily on electronic evidence, the authenticity of which and its connection to the criminal event must be verified through digital forensic examination. Furthermore, many cases involve digital platforms or perpetrators located outside of Indonesia's jurisdiction, necessitating cross-agency coordination and even collaboration with international parties. This often results in law enforcement requiring greater time and resources than handling typical criminal offenses.²¹

These empirical findings demonstrate that the effectiveness of law enforcement is determined not only by the availability of legal instruments but also by the capacity of law enforcement officials, support for digital evidence, and inter-agency coordination. In other words, the success of protecting the right to privacy regarding the use of personal data cannot be measured solely by the number of regulations in place, but rather by the legal system's ability to effectively implement those regulations to provide legal certainty, justice, and protection for the public.

Although the Indonesian legal system provides administrative, civil, and criminal mechanisms to address privacy violations related to the use of personal data, its

¹⁸ Predderics Hockop Simanjuntak, "Legal Protection of Personal Data in the Digital Era in Indonesia: A Study of the Personal Data Protection Law and the General Data Protection Regulation (GDPR)", *Jurnal Esensi Hukum*, published by the Master of Law, Veteran National Development University, Jakarta, (Vol. 6 No. 2 of 2024): 105-124.

¹⁹ Kurniawan Nduru, M. Yusuf Daeng, and Rudi Pardede, "Law Enforcement on Misuse of Personal Data on Social Media", *Lancang Kuning Law Journal*, published by Lancang Kuning University, (Vol. 2 No. 2 of 2025): 127-135.

²⁰ Syarifa Tommy, and Muhammad Irwan Padli Nasution, "Evaluation of Cybersecurity Risk Management in Government Digital Infrastructure", *Kampus Akademik Publishing: Scientific Journal of Economics and Management*, published by CV. Kampus Akademik Publishing, (Vol. 3 No. 6 of 2025): 330-346.

²¹ Rima Eka Hardiyani, *log cit*

implementation still faces various obstacles that impact the effectiveness of law enforcement. These obstacles relate not only to normative aspects but also to institutional issues, evidentiary issues, technological developments, and the level of public legal awareness. Consequently, the legal protection expected by personal data owners has not been fully realized.

One of the main obstacles is the complexity of proving evidence in cases involving electronic data. Unlike conventional crimes, personal data breaches rely on electronic evidence, which must meet procedural requirements and be authenticated through digital forensic examination. This situation requires the availability of technically competent human resources, support from digital forensic laboratories, and strong coordination between agencies. Furthermore, rapid technological developments often outstrip the ability of regulators and authorities to anticipate various modes of personal data misuse.²²

The electronic evidence process, the need for digital forensic examinations, and the handling of cases involving perpetrators or operators of electronic systems outside Indonesian jurisdiction are challenges frequently encountered in law enforcement practices.²³ Meanwhile, the effectiveness of the PDP Law is also influenced by regulatory harmonization, institutional strengthening, and oversight mechanisms that can keep pace with developments in information technology. This perspective demonstrates that successful law enforcement requires synergy between regulatory quality, institutional capacity, and human resource readiness.²⁴

Beyond institutional factors, low public legal awareness is also a significant challenge. Many people still don't understand that personal data is a legally protected right, so the use of another person's photo, identity, phone number, or other personal information without their consent is often considered acceptable. Furthermore, some victims are also unaware of the legal mechanisms available when their privacy rights are violated. This situation results in many violations going unreported or not being pursued through available legal mechanisms, thus preventing the goal of personal data protection from being fully achieved.

Based on this description, it can be understood that the obstacles to law enforcement against privacy violations do not stem from a single factor, but rather are the accumulation of various interrelated issues, ranging from regulatory, institutional, evidentiary, and societal legal culture. Therefore, a more in-depth analysis of these factors is needed using the perspectives of legal system theory, legal effectiveness theory, and legal norms theory to identify the root of the problem and formulate a more effective law enforcement concept.

Based on the practice of law enforcement and the various obstacles that have been described, it can be understood that the effectiveness of the protection of privacy rights regarding the use of personal data is determined not only by the existence of laws and regulations, but also by the ability of the legal system to implement these norms consistently. Lawrence M. Friedman explains that the operation of a legal system is influenced by three main elements, namely legal substance, legal structure, and legal culture. These three elements must work harmoniously for the law to be able to achieve

²² Putu Khan'ha Khilana Putra Bukian, Ni Luh Wayan Yasmiati, Seni Kamalia Rizki Fathullah, "The Emptiness of Digital Forensic Norms in Handling Natural Resource Crimes (SDA): Analysis of the State's Constitutional Responsibility Post-Law 1/2024", *Aliansi: Jurnal Hukum Pendidikan dan Sosial Humaniora*, published by the Indonesian Legal Research and Teaching Association, (Vol. 3 No. 3 of 2026): 31-43.

²³ Rima Eka Hardiyani, *log cit*.

²⁴ Desy Maryani, *log cit*

the desired goals. In the context of personal data protection in Indonesia, these three elements have not yet fully demonstrated integration, so the effectiveness of law enforcement still faces various obstacles.²⁵

From a legal substantive perspective, Indonesia already has a relatively adequate legal basis through the Privacy Law (PDP), the Electronic Information and Transactions (ITE) Law, and various other supporting regulations. The existence of these legal instruments demonstrates the state's commitment to providing legal certainty for the protection of people's privacy rights. However, the effectiveness of these norms still requires harmonization between regulations and technical arrangements that can keep pace with developments in information technology. Therefore, the problem no longer lies in the absence of legal norms, but rather in the consistency and synchronization of their application in practice.²⁶

From a legal structural perspective, law enforcement against personal data breaches involves various institutions with varying authorities. Although this division of authority is regulated in the national legal system, electronic evidence, limited digital forensic capabilities, and the complexity of cases involving perpetrators or electronic systems across jurisdictions remain real challenges for law enforcement. This situation demonstrates that the success of law enforcement is determined not only by the quality of regulations but also by the readiness of human resources, supporting facilities, and inter-agency coordination in handling information technology-based crimes.²⁷

Meanwhile, from a legal culture perspective, the low level of public awareness of the importance of protecting personal data indicates that respect for the right to privacy has not yet fully become part of society's legal culture. There is still a perception that distributing photos, identities, or other people's personal information through electronic media is a normal action as long as it does not cause direct harm. However, the use of personal data without consent is essentially a violation of individual rights guaranteed by the Constitution, laws, and regulations. This situation demonstrates that the success of law enforcement depends not only on law enforcement officials but also requires increasing legal awareness among the public as both subjects and objects of legal protection.

These findings align with Soerjono Soekanto's theory of legal effectiveness, which states that the success of law enforcement is influenced by five factors: the law, law enforcement, facilities and infrastructure, society, and culture. ²⁸In the context of personal data protection, these five factors are interrelated and influence each other. Adequate regulations will be difficult to implement effectively without the support of competent officials, adequate digital evidence facilities, and a public that understands their rights and obligations regarding the processing of personal data. Therefore, efforts to strengthen the effectiveness of law enforcement must be carried out comprehensively through regulatory reform, increasing the capacity of law enforcement officers, strengthening digital forensic infrastructure, and providing legal education to the public.

Furthermore, from Hans Kelsen's perspective, the existence of legal norms regarding personal data protection has provided a clear legal basis for the state to

²⁵ Izzy Al Kautsar and Danang Wahyu Muhammad, "Lawrence M. Friedman's Modern Legal System: Legal Culture and Social Change in Society from Industrial to Digital", *Sapientia et Virtus Journal*, published by the Faculty of Law, Darma Cendika Catholic University, (Vol. 7 No. 2, 2022): 84-99.

²⁶Desy Maryani, *log cit*

²⁷Rima Eka Hardiyani, *log cit*

²⁸ Soerjono Soekanto, *Op.Cit.* , p. 35.

protect the public's right to privacy. However, a legal norm is not only measured by its formal validity but also by its ability to be effectively implemented in society.²⁹ Therefore, the PDP Law is not solely assessed by its existence as a legislative product, but also by the consistency of its implementation, the compliance of electronic system administrators, and the effectiveness of law enforcement in providing legal certainty, justice, and benefits to the public.

Based on this overall analysis, it is clear that law enforcement against privacy violations related to the use of personal data in Indonesia has a fairly strong normative foundation, but its effectiveness still requires strengthening of the legal structure and legal culture. Therefore, improving the law enforcement system cannot be achieved simply by improving regulations; it must also be accompanied by increased institutional capacity, strengthened inter-agency coordination, and fostered public legal awareness to optimally protect privacy rights.

2. The Ideal Concept of Law Enforcement against Violations of Privacy Rights due to the Use of Personal Data Without Consent in Electronic Media to Create Public Legal Awareness

Based on the analysis in the previous discussion, it is clear that the Indonesian legal system essentially has an adequate normative foundation for protecting the right to privacy regarding the use of personal data. However, the effectiveness of law enforcement is still affected by various obstacles stemming from legal substance, institutional structure, and societal legal culture. This situation indicates that the establishment of legislation alone is insufficient to guarantee the protection of privacy rights if it is not accompanied by a law enforcement system that can adapt to developments in information technology and changing patterns of societal interaction in the digital space.

Therefore, the ideal concept of law enforcement against privacy violations cannot be adequately understood as a repressive effort by imposing sanctions on perpetrators after the violation occurs. Law enforcement must be directed towards a more comprehensive approach, integrating prevention, monitoring, enforcement, and victim restoration functions in a balanced manner. This approach is necessary so that personal data protection not only provides legal certainty but also builds public trust in the implementation of electronic systems and encourages the formation of a culture of respect for privacy rights.

The effectiveness of personal data protection cannot rely solely on the existence of the Personal Data Protection Law. Regulatory harmonization, institutional strengthening, effective oversight mechanisms, and increased public legal literacy are required to ensure optimal implementation of personal data protection. This perspective demonstrates that the ideal concept of law enforcement must be built through comprehensive system reform, not simply the addition of new legal norms.³⁰

Thus, the ideal concept of law enforcement against privacy violations needs to be formulated by strengthening all components of the legal system: legal substance, legal structure, and legal culture. These three components must work synergistically so that law enforcement not only provides a deterrent effect on perpetrators but also raises public legal awareness regarding respecting and protecting personal data as a human right.

²⁹Hans Kelsen, *General Theory of Law and State* (New York: Russell and Russel, 1971), p. 29-30.

³⁰Desy Maryani, *log cit*

The ideal concept of law enforcement against privacy violations must begin with strengthening the legal substance as the primary foundation of the personal data protection system. From Lawrence M. Friedman's perspective, legal substance is the totality of norms, principles, and regulations that serve as guidelines for the implementation of the legal system.³¹ Therefore, the success of law enforcement is determined not only by the existence of a law, but also by the quality of norms that can provide legal certainty, respond to societal developments, and be implemented effectively. Although Indonesia already has the PDP Law as its primary regulation, the dynamics of information technology developments indicate that the legal substance still requires refinement to accommodate the ever-evolving forms of violations.

Strengthening legal substance does not necessarily mean creating new laws, but rather ensuring harmonization between the PDP Law and various sectoral regulations related to electronic systems, telecommunications, digital financial services, healthcare, and electronic-based government administration. This harmonization is crucial to avoid overlapping authorities, differing data protection standards, and uncertainty in the application of sanctions for privacy violations. This ensures that every electronic system operator has uniform legal guidelines for processing and protecting people's personal data.³²

In addition to regulatory harmonization, strengthening the legal substance also needs to be realized through the development of more operational implementing regulations, particularly regarding data security standards, reporting mechanisms for data breach incidents, procedures for restitution of victims' rights, and simple and accessible dispute resolution procedures. Clarity in these regulations will provide legal certainty not only for law enforcement officials but also for electronic system administrators and the public as data subjects. From Hans Kelsen's perspective, legal norms will be meaningful if they are formulated systematically, consistently, and can serve as clear guidelines for every legal subject in their actions.³³

The urgency of strengthening the legal substance aligns with the assertion that the effectiveness of personal data protection does not solely depend on the existence of the PDP Law, but also requires regulatory harmonization and the establishment of more effective oversight mechanisms. This perspective demonstrates that the ideal concept of law enforcement must be developed through continuous improvement of the regulatory system to keep pace with developments in digital technology without compromising the protection of the public's right to privacy.³⁴

Thus, strengthening legal substance is a strategic step in building a law enforcement system that is adaptive, consistent, and oriented toward protecting human rights. Harmonious and implementable legal substance will serve as the foundation for strengthening the legal structure and fostering a legal culture within society, ensuring that the goal of protecting personal data is achieved not only at the normative level but also in the practical implementation of electronic systems.

³¹ Lawrence M. Friedman, *Loc. Cit.*

³² Ghufon Rosadi Hidayah, Ha. Djazim Ma'shum, and Muhammad Awaluddin, "Comparative Study of Personal Data Protection in the 2024 ITE Law and the 2022 PDP Law", *Journal of Social, Political and Humanities Research Cluster*, published by the National Research and Innovation Center of the Lecturer Performance Development Institute, (Vol. 4 No. 4 of 2025): 62-70.

³³ Ranti Fadillah, et al, "The Spirit and Contribution of Hans Kelsen in the Development of Legal Science", *Das Sollen: Journal of Contemporary Studies of Law and Society*, published by FORIKAMI (Forum for Scientific Research on Indonesian Society Studies), (Vol. 2 No. 1 of 2023): 1-25.

³⁴ Desy Maryani, *log cit*

In addition to strengthening legal substance, the ideal concept of law enforcement against violations of privacy rights due to the use of personal data must also be directed at strengthening the legal structure as the primary implementer of established norms. From Lawrence M. Friedman's perspective, the legal structure encompasses all institutions that carry out law enforcement functions and the resources they possess.³⁵ Thus, the effectiveness of personal data protection is determined not only by the quality of laws and regulations, but also by the ability of law enforcement officials and related institutions to implement these norms professionally, adaptively, and with a focus on protecting public rights.

Strengthening the legal structure needs to be realized through increased human resource capacity, particularly in handling cases related to electronic evidence and cybercrime. The characteristics of personal data breaches, which mostly occur through electronic systems, require law enforcement officers to have competence in digital investigations, electronic evidence analysis, and an understanding of developments in information technology. Therefore, ongoing education and training in *digital evidence*, *digital forensics*, and personal data protection governance are essential for achieving effective law enforcement.³⁶

The evidentiary process in personal data misuse cases often faces technical challenges, ranging from the authentication of electronic evidence and digital forensic examinations to the handling of cases involving perpetrators and electronic system operators outside of Indonesian jurisdiction. These findings demonstrate that law enforcement challenges are no longer solely legal but also technical and cross-border. Therefore, strengthening the legal structure must be accompanied by the provision of adequate supporting facilities, improving the competence of officers, and developing inter-institutional and international cooperation mechanisms in handling cyber cases.

³⁷

In addition to increasing the capacity of law enforcement agencies, the ideal concept of law enforcement also requires a more integrated coordination system across agencies. Handling personal data breaches involves various actors, from the police, prosecutors, courts, ministries responsible for personal data protection, to electronic system administrators. If this coordination is not effective, the law enforcement process could potentially experience delays, overlapping authority, and differing interpretations of regulations.³⁸ Therefore, a clear coordination mechanism is needed through shared operational standards, a secure information exchange system, and a measurable division of authority so that each institution can carry out its functions synergistically.

Strengthening the legal structure ultimately aims not only to improve the ability of law enforcement officers to handle cases but also to build public trust in the law enforcement system. A professional, responsive legal structure supported by adequate technology will provide legal certainty and expedite the resolution of personal data breach cases. Therefore, strengthening the legal structure is a crucial prerequisite for realizing a law enforcement system that is adaptive to developments in digital

³⁵Lawrence M. Friedman, *Loc. Cit.*

³⁶ Abdul Sakti, "The Influence of Digital Forensic Education and Training on the Quality of Handling Cybercrime Cases" *Popular: Student Research Journal*, published by AMNI Maritime University Semarang, (Vol. 4 No. 1 Year 2025): 104-109.

³⁷Rima Eka Hardiyani, *log cit*

³⁸ Kurniawan Nduru, M. Yusuf Daeng, and Rudi Pardede, *Loc.Cit.*

technology and capable of providing effective protection for the public's right to privacy.

The ideal concept of law enforcement against violations of privacy rights due to the use of personal data must ultimately lead to strengthening the legal culture of society. From Lawrence M. Friedman's perspective, legal culture is a determining factor in whether or not a legal rule is accepted in society.³⁹ Good regulations and professional law enforcement officers will not result in effective law enforcement if the public lacks the awareness to respect and protect the privacy rights of others. Therefore, developing a legal culture is an integral part of efforts to create a sustainable personal data protection system.

The urgency of strengthening legal culture becomes even more relevant when linked to Soerjono Soekanto's theory of legal awareness, which places legal knowledge, legal understanding, legal attitudes, and legal behavior as the main indicators of legal effectiveness in society.⁴⁰ In the context of personal data protection, the public is not sufficient to simply be aware of the PDP Law; they must also understand their rights and obligations as both subjects and controllers of data. This awareness must be reflected in concrete behavior, such as not disseminating photos, identities, telephone numbers, or other personal information of others without their consent, and having the courage to use available legal mechanisms if their privacy rights are violated. Thus, compliance with the law grows not out of fear of sanctions, but out of an understanding that personal data protection is part of respect for human rights.

The public's lack of understanding of the importance of personal data protection remains a major obstacle to the implementation of the Personal Data Protection Law. Therefore, improving legal and digital literacy must be part of the national strategy for personal data protection. Education should be aimed not only at the public as users of electronic media, but also at electronic system administrators, business actors, and state officials who process personal data in the delivery of public services. This way, a culture of personal data protection can develop equitably across all sectors of life.⁴¹

Strengthening legal culture also requires the active involvement of various stakeholders. The government plays a role in developing sustainable educational policies, educational institutions play a role in instilling an understanding of ethics and personal data protection from an early age, while mass media and digital platforms have a responsibility to support the dissemination of accurate information regarding privacy rights in the electronic space. Synergy between these actors will create a legal ecosystem that focuses not only on taking action after violations occur but also on prevention by increasing public legal awareness.

Thus, the ideal concept of law enforcement against violations of the right to privacy due to the use of personal data must be understood as a system that integrates the strengthening of legal substance, legal structure, and legal culture in a balanced manner. These three components complement each other in creating law enforcement that not only provides legal certainty and a deterrent effect on perpetrators, but also fosters a society with a high level of legal awareness and respect for the right to privacy as part of human rights. Through this comprehensive approach, the goal of personal data protection is realized not only through repressive law enforcement but also

³⁹Lawrence M. Friedman, *Loc. Cit.*

⁴⁰ Nur Fitriyani Siregar, "Legal Effectiveness", *Al-Razi: Journal of Science and Society*, published by UIN Sultan Syarif Kasim, (Vol. 18 No. 2 of 2018): 1-16.

⁴¹Desy Maryani, *log cit*

through the development of a legal culture that encourages conscious and sustainable compliance.

The ideal model of law enforcement against violations of privacy rights over the use of personal data is built through the integration of three components of the legal system of Lawrence M. Friedman: legal substance, legal structure, and legal culture, which are implemented effectively according to the legal effectiveness factors of Soerjono Soekanto and supported by the validity of legal norms as stated by Hans Kelsen. This model places public legal awareness as the ultimate goal of law enforcement, so that the protection of personal data is not only realized through action, but also through prevention and the formation of a sustainable legal culture.

D. Conclusion and Recommendations

Based on the results of the research and discussion that have been carried out, the following conclusions can be drawn:

1. Law enforcement against violations of privacy rights due to the use of personal data without consent in electronic media in Indonesia essentially has an adequate legal basis through Law Number 27 of 2022 concerning Personal Data Protection, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, and various other supporting regulations. However, the effectiveness of law enforcement is not yet fully optimal because it is still influenced by various obstacles, including the lack of optimal harmonization of regulations, the complexity of electronic evidence, limited digital forensic capacity, ineffective inter-agency coordination, and low public legal awareness of the importance of personal data protection. Based on an analysis using Lawrence M. Friedman's legal system theory, these obstacles indicate that legal substance, legal structure, and legal culture have not worked in an integrated manner. This finding is reinforced by the results of interviews with academics and law enforcement practitioners, which indicate that challenges to law enforcement stem not only from normative aspects but also from implementation, institutional capacity, and community readiness to face developments in digital technology.
2. The ideal concept of law enforcement against violations of the right to privacy due to the use of personal data must be built through an integrated strengthening of legal substance, legal structure, and legal culture. Strengthening legal substance is carried out through the harmonization of regulations and refinement of implementing regulations that are adaptive to developments in information technology. Strengthening the legal structure is realized through improving the competence of law enforcement officers, developing digital forensic capabilities, providing adequate supporting facilities, and strengthening inter-institutional coordination and cross-jurisdictional cooperation. Strengthening legal culture is carried out through increasing legal literacy and digital literacy that can shape public knowledge, understanding, attitudes, and behavior in respecting the right to privacy as part of human rights. This concept demonstrates that effective law enforcement is not only oriented towards imposing sanctions on perpetrators, but also on building public legal awareness as the primary goal of protecting personal data in the digital era.

Based on the results of this study, the author provides several recommendations as follows:

1. Based on findings that law enforcement against privacy violations related to the use of personal data has not been optimal, the Government, along with law enforcement officials, needs to strengthen the implementation of Law Number 27 of 2022 concerning

Personal Data Protection through regulatory harmonization, increased human resource capacity in the field of electronic evidence and digital forensics, and strengthened inter-agency coordination in handling personal data violation cases. These steps are necessary to ensure that existing legal instruments not only provide legal certainty in normative terms but also can be effectively implemented in law enforcement practices.

2. Based on the ideal concept generated in this research, efforts to raise public legal awareness regarding personal data protection need to be carried out sustainably through an integrated strengthening of legal substance, legal structure, and legal culture. The government, educational institutions, electronic system providers, and the public need to work together to improve legal and digital literacy to foster an understanding, attitudes, and behaviors that respect the right to privacy as a fundamental human right. Thus, law enforcement should not only focus on imposing sanctions on perpetrators but also foster a preventative and sustainable legal culture within society.

References

A. Legislation

- Indonesia. *The Constitution of the Republic of Indonesia (The 1945 Constitution)*.
Indonesia. *Law Number 27 of 2022 concerning Personal Data Protection*. LN No. 196 of 2022, Supplement to LN No. 6820.
Indonesia. *Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions*. LN No. 1 of 2024, TLN No. 6905.

B. Books

- Fredman, Lawrence M. *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 1975.
Kelsen, Hans. *General Theory of Law and State*. New York: Russell and Russell, 1971.
Soekanto, Soerjono. *Factors Influencing Law Enforcement*. Jakarta: Rajawali Press, 2010.

C. Journal Articles

- Al Kautsar, Izzy, and Danang Wahyu Muhammad. "Lawrence M. Friedman's Modern Legal System: Legal Culture and Social Change in Society from Industrial to Digital." *Sapientia et Virtus Journal* 7, no. 2 (2022).
Bukian, Putu Khan'ha Khilana Putra, Ni Luh Wayan Yasmiati, and Seni Kamalia Rizki Fathullah. "The Vacuity of Digital Forensic Norms in Handling Natural Resource Crimes (SDA): Analysis of the State's Constitutional Responsibility Post-Law 1/2024." *Alliance: Journal of Educational Law and Social Humanities* 3, no. 3 (2026).
Daeng, Yusuf, et al. "Personal Data Protection in the Digital Era: A Review of the Legal Framework for Privacy Protection." *Innovative: Journal of Social Science Research* 3, no. 6 (2023).
Fadillah, Ranti, et al. "The Spirit and Contribution of Hans Kelsen in the Development of Legal Science." *Das Sollen: Journal of Contemporary Studies of Law and Society* 2, no. 1 (2023).
Hidayah, Ghufon Rosadi, Ha. Djazim Ma'shum, and Muhammad Awaluddin. "Comparative Study of Personal Data Protection in the 2024 ITE Law and the 2022 PDP Law." *Journal of Social, Political, and Humanities Research Cluster* 4, no. 4 (2025).
Nduru, Kurniawan, M. Yusuf Daeng, and Rudi Pardede. "Law Enforcement of Personal Data Misuse on Social Media." *Lancang Kuning Law Journal* 2, no. 2 (2025).
Qurrotuaini, Nur Azizah. "The Right to Privacy as a Constitutional Right in the Digital Era: A Juridical Study from a Cyber Law Perspective." *Staatsrecht: Journal of Islamic State and Political Law* 4, no. 2 (2024).
Sakti, Abdul. "The Influence of Digital Forensic Education and Training on the Quality of Cybercrime Case Handling." *Popular: Student Research Journal* 4, no. 1 (2025).
Simanjuntak, Predderics Hockop. "Legal Protection of Personal Data in the Digital Era in Indonesia: A Study of the Personal Data Protection Law and the General Data Protection Regulation (GDPR)." *Journal Esensi Hukum* 6, no. 2 (2024).
Siregar, Nur Fitriyani. "The Effectiveness of Law." *Al-Razi: Journal of Science and Society* 18, no. 2 (2018).
Sudiantini, Dian, et al. "Digital Transformation: Impacts, Challenges, and Opportunities for Digital Economic Growth." *Trending: Journal of Economics, Accounting and Management* 1, no. 3 (2023).

Tommy, Syarifa, and Muhammad Irwan Padli Nasution. "Evaluation of Cybersecurity Risk Management in Government Digital Infrastructure." *Kampus Akademik Publishing: Scientific Journal of Economics and Management* 3, no. 6 (2025).

D. Online News

Detikinet. "Komdigi Receives Hundreds of Complaints about Personal Data Protection." Accessed May 29, 2026.

E. Interviews

Hardiyani, Rima Eka. Head of the Pre-Prosecution Subsection of the General Crimes Section of the Cilegon District Attorney's Office. Interview, June 22, 2026.

Maryani, Desy. Lecturer in Criminal Law, Faculty of Law, Daehasen University, Bengkulu. Interview, June 15, 2026.