Journal of International Islamic Law, Human Right and Public Policy

Journal of International Islamic Law, Human Rights, and Public Policy
(JISHUP Journal) | ISSN(e): 3031-2280
Website https://jishup.org/index.php/ojs/index | Volume 4 No. 3 (2026)

PROTECTION OF DIGITAL PRIVACY RIGHTS AS A HUMAN RIGHT AGAINST PERSONAL DATA MISUSE IN INDONESIA

Faisal Fachri[1], Ariy Khaerudin[2], Nourma Dewi[3]
Fakultas Hukum Universitas Islam Batik Surakarta
faisalfchri@gmail.com, ariykhaerudin@gmail.com, nourmadewi03@gmail.com

Received: 05/06/2026 | **Revised:** 11/06/2026 | **Accepted:** 25/06/2026 | **Published:** 05/07/2026

Abstract

The rapid development of information technology and internet usage has increased the risk of misuse of personal information in the digital space, in the form of data theft, dissemination, and utilization. This study aims to determine the form of protection of the right to privacy as a human right against misuse of personal data in Indonesia based on the Personal Data Protection Law. Using normative legal research with a legislative approach and a conceptual approach, the study results show that the Personal Data Protection Law has provided a legal basis for the rights of personal data subjects, the obligations of data controllers, and administrative and criminal sanctions for personal data violations. However, the implementation of the Personal Data Protection Law still faces various obstacles, such as low public awareness, weak supervision, and the persistently high number of personal data leaks. Therefore, it is necessary to strengthen supervision, law enforcement, and improve the digital literacy of the public to realize effective personal data protection in Indonesia.

Keywords: personal data protection, misuse of personal information, internet, Personal Data Protection Law, right to privacy.

INTRODUCTION

The development of information technology has transformed nearly all patterns of social, economic, and administrative relations in society. Activities previously conducted in person have now largely shifted to the digital space, from public services and financial transactions to education and e-commerce, to personal communications. These changes provide convenience and efficiency, but at the same time, they open up new avenues for cybercrime. Technology abuse can take various forms, such as identity theft, account hacking, unauthorized data sales, digital fraud, and the use of personal information for purposes detrimental to the data owner. This situation places personal data protection beyond mere technical issues, but also as a legal and human rights issue (Ukurta, 2022).

Threats to personal data are increasingly serious because most digital activities leave a trail of information. Names, addresses, ID numbers, telephone numbers, email addresses, location data, transaction records, and even biometric data can be stored in various systems. If this data is not managed carefully, data owners can experience economic loss, reputational damage, discrimination, blackmail, or psychological distress due to a loss of sense of security. Therefore, personal data protection aims not only to maintain information confidentiality but also to protect the dignity, freedom, and autonomy of individuals in determining how their information is used.

In the context of a state governed by the rule of law, the state has a responsibility to provide a protection framework that can address changes in digital society. The existence of specific regulations regarding personal data protection demonstrates the recognition that personal information is an inherent human right. These regulations essentially govern the relationship between data owners, those who manage data, and those who process it. These regulations cover the principles of lawful processing, the obligation to maintain information security, the right of data owners to know and control the use of their data, and redress mechanisms in the event of a violation. Thus, personal data protection is a crucial tool for creating legal certainty and building public trust in the digital ecosystem.

The issue of personal data protection in Indonesia has received widespread attention as various public and private services increasingly rely on digital identity systems. Electronic population administration programs, the use of identity numbers for service registration, and the use of biometric data demonstrate that the government and businesses are collecting public data on a large scale. While this data collection offers administrative benefits, it also carries risks if not accompanied by robust security governance. Several cases of misuse of identity numbers and family data in communication service

registration demonstrate that security gaps and weak verification can lead to unauthorized use of personal data (Siswanto & Ismawati, 2025). In addition to individual abuse, large-scale data breaches have also attracted public attention. One frequently discussed example is the leak of e-commerce platform user data, which impacted millions of accounts. The leaked data can include user identities, email addresses, phone numbers, dates of birth, and account credentials, which could potentially be exploited for further criminal activity. Incidents like these demonstrate that failure to protect data not only harms users personally but can also undermine public trust in electronic system providers (Christmas, 2025).

Personal data misuse can also occur in simpler forms, such as using another person's identity to register a communication card, open a digital account, or obtain certain benefits. While seemingly limited, such actions remain dangerous because they can place victims at legal, financial, and social risk. In law enforcement practice, identity misuse demonstrates that personal data has strategic value and can be used as a tool for unlawful acts. Therefore, a data protection approach must encompass prevention, enforcement, redress of victims' rights, and increased public awareness. In terms of accountability, personal data breaches can have varying consequences, depending on the nature of the act and the losses suffered by the victim. Under certain circumstances, the perpetrator can be held criminally liable for their actions, which involve intentional misuse, unauthorized use, and harm to others. On the other hand, victims can also pursue civil remedies to recover their losses. Therefore, personal data protection has two orientations: providing a deterrent effect against violations and restoring the rights of affected data subjects (Aji, 2023).

Personal data protection, as part of the right to privacy, is also a key issue in constitutional discourse. Debates over the effectiveness of regulations, the role of oversight bodies, and protection for small-scale digital businesses demonstrate that personal data regulation still requires strengthening. In a society increasingly reliant on electronic transactions, data transfer can occur rapidly and involve multiple parties. If data owners lack adequate control, their constitutional rights can be threatened. Therefore, studies on personal data protection need to be placed within the framework of respect for basic human rights (Wijaya, 2022). Based on this description, this study discusses the protection of digital privacy rights as part of human rights against the misuse of personal data in Indonesia. The discussion focuses on the relationship between personal data, privacy rights, human rights principles, and the challenges of implementing data protection in people's digital lives. This study is important because the misuse of personal data not only causes individual harm but also illustrates the urgent need for a more accountable legal system and digital culture.

LITERATURE REVIEW

Personal data is information that identifies an individual and can be used to identify them, either directly or through combination with other information. This data can include administrative identification, contact information, transaction data, digital activity records, biometric information, or other forms of information related to a person's personal life. In modern society, personal data has economic, social, and legal value. This value makes personal data frequently the object of collection, use, and even misuse by certain parties. Therefore, personal data protection must be understood as part of efforts to maintain human dignity. The right to privacy allows individuals to determine the boundaries of their personal lives. This right encompasses the authority to determine when, how, to what extent, and to whom their personal information can be disclosed. When personal data is collected or used without a legitimate basis, the data owner loses control over their information. This loss of control can impair individual freedom, create feelings of insecurity, and open the door to harm. Therefore, misuse of personal data constitutes a violation of the right to privacy because it robs an individual of the ability to control their digital identity.

From a human rights perspective, privacy does not stand alone but is closely linked to honor, freedom, security, and equality before the law. Protecting privacy allows individuals to live their private lives without unauthorized interference. In the digital space, this interference can take the form of excessive surveillance, unauthorized use of data, the dissemination of personal information, or non-transparent profiling. Therefore, protecting digital privacy rights is integral to safeguarding human dignity in an ever-changing technological environment. Weaknesses in data protection systems can have far-reaching consequences. Victims of data breaches can experience material losses, such as fraud, account misuse, and illegal transactions. Victims can also experience immaterial losses, such as fear, embarrassment, loss of trust, or damage to their reputation. In some cases, personal data can even be used to discriminate or manipulate behavior. This demonstrates that personal data protection cannot be left solely to the technical policies of electronic system providers. Such protection requires legal support, oversight, corporate responsibility, and public digital literacy.

Internationally, the right to privacy has long been recognized as a fundamental human right. Global human rights instruments place privacy, family life, residence, and communication as areas that should not be arbitrarily disturbed. This principle has evolved in the context of personal data protection, along with the use of computers and electronic systems to manage population information. Technological advancements mean that privacy violations are no longer limited to physical searches or conventional wiretapping, but also encompass massive and covert data processing. Privacy rights can generally be restricted under certain circumstances, for example for law enforcement, public safety, or the protection of others' rights. However, such restrictions must be based on clear rules, a legitimate purpose, and proportionate measures. Restrictions

should not be used as a justification for unlimited surveillance or excessive data collection. In human rights thinking, restrictions on rights can only be justified if they respect human dignity and do not diminish the essence of the right itself. This view aligns with the idea that the law should function to protect people, not simply be a tool of power (Asshiddiqie, 2018). Satjipto Rahardjo positions law as a means to bring justice and protection to humans. In the context of personal data protection, this idea is relevant because the law cannot simply contain prohibitions and sanctions; it must also address the needs of people living in a digital environment. Technological change demands that the law be adaptive, responsive, and pro-human protection. Without effective updates and implementation, regulations regarding personal data will remain mere normative texts that are unable to prevent real harm (Rahardjo, 2012). In the Indonesian legal system, protection of privacy rights and personal data is developed through various policies and regulations. This legal framework essentially recognizes that personal data is information related to an individual and must be processed responsibly. Personal data protection is intended to ensure that all processes of data collection, storage, use, transmission, disclosure, and deletion are carried out with respect for the data owner's rights. This regulation also places the data manager as the party responsible for the security and legality of data processing (Rahardjo, 2006).

METHOD

This research employs normative legal research methods with regulatory, conceptual, and case-based approaches. The regulatory approach is used to examine the legal framework governing personal data protection and privacy rights. The conceptual approach is used to understand the concepts of human rights, privacy rights, personal data, and the relationship between data owners and data managers. Meanwhile, the case-based approach is used to examine how personal data misuse occurs in practice and how the principles of legal protection can be applied to such incidents. Normative legal research is prescriptive in nature because it not only explains applicable norms but also provides arguments regarding the direction in which protection should be developed. In this research, the data used are sourced from legal materials and scientific literature, such as law books, journal articles, expert opinions, policy documents, and decisions or cases relevant to the issue of personal data protection. All of this material is analyzed qualitatively, emphasizing the consistency of norms, the purpose of protection, and the alignment of legal regulations with the needs of the digital society (Marzuki, 2016). The analysis was conducted through several stages. First, it identified the basic concepts of personal data and privacy rights. Second, it examined the relationship between personal data protection and human rights principles. Third, it outlined the forms of personal data misuse and their impact on victims. Fourth, it assessed the challenges of implementing legal protection in Indonesia. Through these stages, this research seeks to generate a more comprehensive understanding of digital privacy rights protection amidst the development of information technology (Soekanto & Mamudji, 2007).

RESULTS AND DISCUSSION

In practice, personal data protection rests on several basic principles. First, data must be collected lawfully and without misleading intent. Second, the purpose of data collection must be clearly stated from the outset. Third, processed data must be relevant to that purpose and must not be overused. Fourth, data must be kept accurate, secure, and not easily accessible to unauthorized parties. Fifth, data owners must be given the opportunity to learn about, correct, limit, or withdraw consent to the processing of their data. These principles demonstrate that personal data protection places the individual at the center of the entire information management process. Data owner consent is a crucial foundation for processing personal data. Consent should not be understood as a mere formality, but rather must be given consciously, freely, clearly, and based on adequate information. In digital services, users often agree to privacy policies without reading them due to overly technical language or difficult-to-understand information placement. This situation renders consent less meaningful. Therefore, data managers need to compile privacy information in a simple, transparent, and easily accessible manner so that data owners fully understand the consequences of their consent.

In addition to consent, control by data owners is also central to privacy protection. Data owners should have the right to obtain information about who processes their data, for what purposes it is used, how long it is retained, and with whom it is shared. Data owners should also be given the opportunity to correct inaccurate data, request the cessation of processing, request the deletion of certain data, and obtain a copy of the data in a usable format. These rights are important because they give individuals an active role, rather than simply making them objects of information collection activities. The responsibility of data managers extends beyond fulfilling administrative requirements and includes establishing adequate security systems. Data managers must implement the precautionary principle through technical safeguards, access restrictions, regular audits, recording of processing activities, and procedures for handling incidents. When a breach or protection failure occurs, data managers must act quickly to mitigate the impact, provide clear notification to affected parties, and provide a complaint or redress mechanism. Accountability is key, as data protection cannot be effective without concrete responsibility from those who benefit from data processing.

In the event of a breach, the data protection system must provide effective redress instruments. Redress can take the form of stopping unauthorized processing, deleting data, improving security systems, providing compensation, or imposing sanctions on violators. Administrative sanctions are necessary to encourage compliance by electronic system operators, while criminal mechanisms can be used as a last resort for serious, intentional, and detrimental acts against victims. With this approach, law enforcement not only pursues punishment but also ensures victims receive adequate protection and redress. Comparison with international standards shows that some types of information require stronger protection. Data relating to health, biometrics, beliefs, ancestry, specific views, or highly personal aspects of an individual's life are at higher risk of misuse. If such data is leaked or used unauthorizedly, the impact can be far more severe than a general information leak. Therefore, managing sensitive data requires stricter restrictions, clearer processing bases, and higher levels of security (Purnamasari, 2021).

Historically, attention to personal data protection has grown as the use of computers to store citizen information has become widespread. Countries that were earlier in developing computer-based administrative systems faced a new challenge: how to prevent the overuse of citizen data by both the government and the private sector. From this experience, data protection principles emerged, emphasizing collection limitations, data quality, clarity of purpose, use limitations, security, openness, individual participation, and accountability. These principles remain important references in personal data governance (Suari & Sarjana, 2023). The principle of collection limitation requires that requested data be truly necessary and obtained through legitimate means. The principle of data quality emphasizes that the data used must be accurate, relevant, and updated when changes occur. The principle of clarity of purpose requires data managers to disclose the purpose of processing from the outset to prevent data from being used for other purposes unilaterally. Meanwhile, the principle of security requires protection from loss, alteration, unauthorized access, and unauthorized dissemination. These four principles serve as the foundation for preventing excessive data collection and data use beyond legitimate purposes.

The principles of openness and individual participation are also crucial in realizing democratic protection. Openness requires data managers to clearly explain their data processing policies and practices. Individual participation allows data owners to learn about the existence of their data, request access, submit corrections, and object to processing deemed detrimental. The principle of accountability places the responsibility on data managers to demonstrate that all processing activities have been carried out in accordance with applicable protection standards. Therefore, data protection does not stop at the promise of a privacy policy but must be testable in practice (Shofiyah & Fogar, 2019). The concept of human rights provides a philosophical foundation for the protection of personal data. Human rights arose from the recognition that every human being possesses inherent rights due to their human dignity. These rights do not depend on the state granting them, but must be respected and protected by the state. The history of human rights thinking shows that the concept of fundamental rights has evolved since the conception of natural law, including Aristotle's view of humans as social beings living in political communities. The state is understood as a vehicle for realizing the common good, not as a power free to ignore the interests of its citizens (Latumahina, 2014).

In Aristotle's thought, the state was formed from the human need to live together and achieve prosperity. Prosperity does not merely mean the fulfillment of economic needs, but also encompasses justice, security, dignity, and the opportunity to develop. When viewed in today's digital context, the state is obligated to ensure that technological developments do not compromise the security and freedom of its citizens. Personal data protection is one form of state responsibility to create a digital space that is safe, just, and respectful of human dignity. The development of modern human rights was marked by the birth of various important documents in world history that affirmed the limitations of power and the recognition of individual rights. Following experiences of war and widespread violence, the international community increasingly placed human rights protection as a universal standard. This recognition influenced various countries, including Indonesia, in formulating guarantees for citizens' rights. Over time, the right to privacy and personal data protection has become an extension of human rights protection, as human life no longer takes place solely in physical space but also in digital space (Yuniarti, 2019).

In Indonesia, human rights protection is firmly grounded in the constitution and various national legal instruments. Guarantees for personal privacy, family, honor, dignity, communication, and security form the foundation for the development of privacy protection. As information technology advances, this protection has been extended to encompass personal data and digital activities. Thus, privacy protection encompasses not only the prohibition of physical intrusions into private life but also protection from unauthorized use of personal information (Pratama, 2024). The Indonesian personal data protection framework normatively incorporates many important elements, such as recognition of data owner rights, data manager obligations, processing bases, security, transparency, and law enforcement mechanisms. Conceptually, these regulations align with international data protection standards, which place individuals in control of their personal information. However, the existence of norms does not automatically guarantee effective protection. The success of data protection is largely determined by supervisory institutions, the compliance culture of electronic system administrators, the capabilities of law enforcement, and public awareness of the risks of data misuse (Bunyamin, 2020).

One of the main challenges is the need for an independent, professional, and clearly authorized oversight body. Such an institution is needed to monitor data managers' compliance, receive complaints, conduct investigations, and take corrective action in the event of violations. Without strong oversight, personal data protection will depend on the voluntary awareness of businesses and electronic system operators. In practice, however, business interests often drive the collection of as much data as possible for analysis, marketing, or service development. The next challenge relates to the harmonization of data protection regulations with criminal and civil law. Many personal data breaches occur through rapidly evolving new methods, such as identity theft, social engineering, creating fake accounts, database hacking, or selling data on illegal forums. Law enforcement officials need a clear technical understanding and legal framework to distinguish between administrative violations, civil disputes, and crimes requiring criminal prosecution. Without such harmonization, victims risk experiencing difficulties in obtaining protection and redress (Wiraguna, 2025). In addition to institutional and law enforcement factors, public digital literacy also plays a crucial role. Many digital service users don't understand the risks of sharing identity numbers, verification codes, document photos, or other personal information. Some people are also unfamiliar with reading privacy policies, managing account security, or reporting suspected data misuse. This literacy gap makes the public more vulnerable to fraud and identity theft. Therefore, personal data protection must be supported by ongoing public education.

Electronic system providers must also change their perspective on personal data. User data should not be treated simply as a business asset, but rather as information inherent in human dignity. Data minimization principles need to be implemented to prevent service providers from requesting information irrelevant to the service's purpose. Furthermore, security must be designed from the outset through a privacy-by-design and security-by-design approach. With this approach, data protection is not a default after the system is operational but rather becomes part of the service design from the outset. Ultimately, protecting digital privacy rights requires collaborative efforts between the state, businesses, and the public. The state is responsible for providing clear regulations, effective oversight, and consistent law enforcement. Businesses are obligated to manage data responsibly and transparently. The public needs to increase their vigilance and understand their rights as data owners. If these three elements are balanced, personal data protection can be a crucial instrument in realizing a digital space that is safe, equitable, and respects human rights.

CONCLUSION

The misuse of personal data in the digital space constitutes a violation of the right to privacy, which is directly related to the protection of human rights. Advances in information technology have expanded the range of privacy risks, from identity theft and database leaks to unauthorized dissemination of information, to the use of data for purposes detrimental to its owner. In these circumstances, personal data cannot be viewed as ordinary information, as it inherently compromises an individual's identity, dignity, and security.

Normatively, Indonesia has a personal data protection framework that recognizes the rights of data owners, the obligations of data managers, the principles of lawful processing, redress mechanisms, and enforcement against violations. This framework demonstrates the country's commitment to adapting human rights protection to the development of a digital society. However, the effectiveness of this protection still faces several challenges, particularly related to strengthening oversight institutions, consistent law enforcement, electronic system security, and the public's digital literacy level.

Strengthening the protection of digital privacy rights requires independent and professional oversight, stronger security standards for electronic system administrators, and accessible complaint and redress mechanisms for victims. Furthermore, the public needs to be equipped with an understanding of the right to personal data, how to maintain information security, and what to do in the event of misuse. With such strengthening, personal data protection can function not merely as an administrative regulation, but as a concrete manifestation of respect for human dignity and rights in the digital age.

REFERENCES

Ade Hari Siswanto and Yulia Ismawati, Legal Protection against Misuse of Personal Data in Prepaid SIM Card Registration (Study of Decision Number 78/Pid.Sus/2024/PN Tng), Arus Jurnal Sosial dan Humaniora (AJSH), Vol.5, No.2 (2025)

Anggeen Suari, KR, & Sarjana, IM (2023). Maintaining Privacy in the Digital Age: Personal Data Protection in Indonesia. Journal of Legal Analysis, 6 (1), 132-42. https://doi.org/10.38043/jah.v6iL4484.

Bunyamin, 2020 in Ibid Praxis: Journal of Applied Philosophy

Daniar Supriyadi, Personal Data and Two Legal Basis for Its Use, 2017. Accessed May 21, 2026

Darmodihardji and Shidarta, 1995 in Vanny Elvahira, Elga Suci Anjani, Nanda Puspita DP, Muhammad Alvi Pratama, "Aristototle's Concept of Natural Law". Praxis: Journal of Applied Philosophy (2024) 1:2, 1-25 ISSN 1111-1111. Published by FORIKAMI (Indonesian Society Study Scientific Research Forum) Online – March 2024

Deni Bagus Prastyo Aji, Personal Data Protection in Online Transactions: A Study of Decision Number 235/Pdt.G/2020/Pn.jkt.Pst. Journal of Law POSTULAT. February, 2023. Vol. 01 No. 01, pp. 36-44
GraceChristmas, Leakage of 91 Million Personal Data of Tokopedia Application Consumers: Normative and Responsible Study, PERAHU (Legal Information): Journal of Legal Studies, Vol.13, No.1 (2025).
Jimly Asshiddiqie, The Indonesian Constitution and Constitutionalism, Jakarta: Sinar Grafika, 2018, pp. 123–125
Considerations Regarding the PDP Law
LG. Saraswati et al. Human Rights. Philosophy UI Press. December 2006
Nadya Nurhamdiah Purnamasari, "Legal Protection of Personal Data of Marketplace Users," (Thesis, Department of Civil Law, Faculty of Law, Hasanuddin University, 2021), p. 16.
Nita Octaviana Rahmadani, Gischa Adelia Fitri, and Sidi Ahyar Wiraguna, "Personal Data Protection as a Human Right: A Legal Perspective Based on Law Number 27 of 2022." PESHUM: Journal of Education, Social and Humanities. Vol. 5, No. 1 December 2025.
Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems
Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions
Peter Mahmud Marzuki, Legal Research Revised Edition, 9th Edition, Jakarta: Kencana Prenada Media Group, 2016. P. 133
Press_2739_14.4.23 Release 108. 110.PUU.XX.2022 Personal Data Protection Law https://www.mkri.id/public/content/infoumum/press/pdf/press_2739_14.4.23%20Rilis%20108.110.PUU.XX.2022%20UU%20Pelindungan%20Data%20Pribadi-%20VI-%20PUTUSAN%20FY.pdf Accessed May 21, 2026
Rosalinda Elsina Latumahina, "Legal Aspects of Personal Data Protection in Cyberspace," Jurnal Gema Aktualita – Fhuph Surabaya, Vol. 3, 2014, p. 16
Satjipto Rahardjo, Legal Studies, Seventh Edition, Citra Aditya Bakti, Bandung 2012. Page 206
Satjipto Rahardjo, Legal Studies, Bandung: Citra Aditya Bakti, 2006, pp. 206–208
Shofiyah, EN, & Indri Fogar, S. (2019). Misuse of personal data of loan recipients in Peer To Peer Lending Novum: Journal of Law, 6(2), pp. 2-3.
Siti Yuniarti, Legal Protection of Personal Data in Indonesia, Becoss Journal, Vol. 1, 2019, p. 151
Law Number 27 of 2022 concerning Personal Data Protection
Wijaya, Alvian Dwiangga, Legal Protection of Personal Data in the Use of Applications on Smartphones, Inicio Legis, Vol. 3, No. 1 (2022), p. 63-72
Regina Ukurta, "Administrative and Criminal Sanctions Following the Enactment of Law Number 27 of 2022 Concerning Personal Data Protection," Jurnal Kertha Desa 11, no. 4 (2022).