JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i2

Constitutional Guarantees of the Right to Privacy of Personal Data of Citizens in the Era of Government Digitalization

Aprilia Dwi Rahmawati[1*], Dodi Jaya Wardana[2]
[1]Faculty of Law, Muhammadiyah University of Gresik, Indonesia, apriliadwi@umg.ac.id
[2]Faculty of Law, Muhammadiyah University of Gresik, Indonesia, apriliadwi@umg.ac.id

[*]Corresponding Author : apriliadwi@umg.ac.id

Abstract: The advancement of digital technology and the transformation toward electronic-based governance have brought new challenges to the protection of citizens' privacy rights, particularly concerning personal data. In the digital era, personal data has become increasingly vulnerable to misuse and data breaches, while Indonesia's legal framework is still in the process of adapting to these issues. This study aims to analyze the extent to which the right to privacy and personal data is constitutionally protected, and how the state is obligated to ensure such protection. This research uses normative legal methods with a juridical- conceptual approach. The findings indicate that the right to privacy is constitutionally guaranteed in the 1945 Constitution of the Republic of Indonesia, particularly in Article 28G paragraph (1) and Article 28H paragraph (4), although personal data is not explicitly mentioned. The enactment of Law No. 27 of 2022 on Personal Data Protection marks a significant step in strengthening legal safeguards for digital privacy. It must be supported by the establishment of an independent supervisory authority, adaptive policy formulation, and increased digital literacy among the public.

Keyword: Privacy Rights, Personal Data, Constitution, Digitalization, Legal Protection

INTRODUCTION

In the digital age, developments in information and communication technology have brought about major changes in human life. In the process, personal data has become increasingly important and sensitive because many activities are carried out online. Personal data includes information such as names, addresses, identity numbers, financial information, medical history, and other sensitive information related to individuals. In the midst of this rapid digital era, individuals' personal data is increasingly vulnerable to potential misuse and privacy violations. The security of personal data is a human right that must be guaranteed and respected. Indonesia, as a developing country with rapid technology adoption, has a responsibility to protect personal data as a right to privacy. In this context, the right to privacy is an urgent issue that must be addressed. The right to privacy is the fundamental right of every individual to maintain the confidentiality and security of their personal data. With the increasing number of privacy violations and misuse of personal data, it is important for every country to have effective legislation to protect the privacy rights of its citizens (Anggen Suari & Sarjana, 2023).

Cases of personal data leaks in Indonesia have occurred several times and caused public unrest. For example, in 2011 there was a data breach incident that affected around 25 million Telkomsel customers, followed by data leaks involving Lion Air and Batik Air passengers in September 2019. Sensitive data such as National Identity Cards (KTP) and passport numbers stored on Amazon Web Services (AWS) cloud computing services were found to be publicly accessible through backup files containing tens of millions of passenger data. This leak has great potential for misuse, both for identity theft and online fraud, which will certainly have a material and immaterial impact on society (Mahameru et al., 2023).

The increasing demand for information and communication technology and the growing number of internet users have led to a higher risk of data leaks. The rapid and easy dissemination of information has made the issue of personal data protection increasingly urgent to be regulated comprehensively (Komparatif & Indonesia, 2023).

The principle of personal data protection emphasizes that every individual has the right to determine the fate of their personal data, including the right to share or withhold such information. If someone decides to share their personal data, they also have the right to determine the conditions for its use. However, in practice, various digital services often request personal information such as full name, email address, social media accounts, or account numbers for identity verification purposes. Unfortunately, there is no absolute guarantee that this data is protected from the risk of misuse. (Anggen Suari & Sarjana, 2023).

The absence of specific regulations that comprehensively govern personal data protection in Indonesia has resulted in scattered regulations in various partial and sectoral laws and regulations, which do not fully emphasize the principles of data protection. According to Donny B. U, an expert advisor to the Minister of Communication and Information Technology in the field of Digital Literacy and Internet Governance, there are at least thirty-two (32) laws that generally contain provisions on personal data protection. One example is the Law on Banking, which regulates the protection of customer personal data. However, these regulations do not provide optimal and effective protection because they are scattered and not integrated. As a result, criminal acts arising from the dissemination of personal data still frequently occur, both online, such as fraud through social media or data misuse in cloud computing, and offline, such as mass collection of personal data (digital dossiers), direct selling, and other forms of misuse. (Priscyllia, 2019)

METHOD

This study uses a normative legal method, which is research that focuses on literature studies of written legal norms, both those contained in legislation and court decisions. The analysis was conducted on the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, and other sectoral regulations. In addition, the study is reinforced with scientific literature and legal doctrine to examine constitutional guarantees of personal data privacy rights in the digital age. The approach used is qualitative with descriptive normative analysis techniques.

RESULTS AND DISCUSSION

Constitutional Guarantees of the Right to Privacy of Personal Data in the Context of Digitalization eks Digitalisasi

The Unitary State of the Republic of Indonesia guarantees the right to privacy as part of human rights. For example, Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia (“1945 Constitution”) states that every person has the right to protection of their personal life, family, honor, dignity, and property under their control, and has the right to feel safe and protected from the threat of fear of doing or not doing something that is a human right (Wahyu Destanti & Aris Yuni Pawestri, 2025).

Advances in digital technology have had a major impact on personal data protection, where sensitive information such as identity, location, and biometric data can now be collected and disseminated without the owner's permission. This situation raises concerns about an increased risk of data breaches that can lead to cybercrime, such as identity theft, online fraud, and misuse of personal information for commercial gain (Mahameru et al., 2023). The phenomenon of personal data misuse demonstrates weak control over digital privacy, especially amid the rapid flow of information and global connectivity facilitated by internet technology. The speed and breadth of data distribution in cyberspace make threats to privacy increasingly difficult to control without a robust and comprehensive legal system (Komparatif & Indonesia, 2023).

More broadly, digitization has changed the way modern humans live. Governments, businesses, and even the education sector now rely on information technology to improve efficiency and expand the reach of their services. The presence of various platforms such as social media, e-commerce, and cloud-based storage has become part of everyday activities (Wijaya et al., 2024). Although it brings convenience and speed to public services, this development also creates new responsibilities in protecting personal data from misuse by unauthorized parties (Muin, 2023).

In Indonesia, public awareness of the importance of personal data protection has begun to increase, but the implementation of such protection still faces serious obstacles. One of the main obstacles is the unpreparedness of national regulations to adapt to the rapid development of information technology. Although Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) contains provisions on personal data, its substance is not yet comprehensive enough to regulate the mechanisms for collecting, processing, storing, and protecting data in a comprehensive manner (Mahameru et al., 2024).

In recent years, various data breaches in the public and private sectors have further highlighted the weakness of Indonesia's legal protection system. Several major cases, such as the leakage of telecommunications operator customer data, airline passenger data, and government agency data, point to significant gaps in information security oversight and management (Komparatif & Indonesia, 2023). This situation shows that the applicable regulations are still general in nature and unable to respond to the complex challenges of the digital age.

In addition to regulatory aspects, problems also arise from low digital literacy and a lack of understanding among public and private institutions of the basic principles of personal data protection. Many institutions have not implemented adequate security standards for data collection and storage, and are not transparent in their use of user data (Wijaya et al., 2024). This low level of understanding is partly due to the suboptimal dissemination and implementation of Law No. 27 of 2022 on Personal Data Protection (Muin, 2023)

Personal data is any information relating to a person that can identify or be identified, either directly or indirectly, through electronic or non-electronic systems. This definition is clearly stated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) as the main legal basis for the regulation and protection of personal data in Indonesia (Kusnadi & Wijaya, 2021). The law classifies personal data into two categories, namely specific personal data and general personal data, in order to determine the level of protection and appropriate legal handling for each type of data (Mahameru et al., 2023).

Specific personal data is highly sensitive and has the potential to cause significant harm if misused. Based on Article 4 paragraph (2) of the PDP Law, specific data includes information such as health data, biometrics, genetics, criminal records or history, child data, personal financial data, and other data regulated by laws and regulations (Wijaya et al., 2024). The processing of this type of data must obtain explicit consent from the data subject and must be carried out with the utmost care and protection, given its high potential for misuse, especially

in the health, finance, and security sectors (Mahameru et al., 2023). In the context of positive law in Indonesia, the processing of specific personal data must obtain explicit consent from the data subject as a form of protection for the privacy rights and autonomy of individuals over their personal information. The application of these principles is not only an ethical imperative, but also a legal obligation aimed at preventing potential violations and strengthening public trust in data governance in the digital age (Penelitian, 2024).

Meanwhile, general personal data includes basic information that can be used to identify a person, such as full name, gender, nationality, religion, and marital status (Saputra, 2023). Although its sensitivity level is lower than specific data, general data must still be properly protected because it can be used as a gateway for digital crimes, including identity theft or hacking of personal data (Komparatif & Indonesia, 2023). This situation shows that the protection of public data should not be neglected, because even the smallest security breach can be exploited by irresponsible parties to gain access to more sensitive information (Penelitian, 2024). This is reflected in cybercrime practices, where perpetrators use seemingly "non-critical" basic data as a gateway to carry out phishing attacks, social engineering, or identity theft, and subsequently access or sell much more valuable data (Satrio Pangarso Wisanggeni, 2020).

The increasingly complex development of digital technology requires a personal data protection system that is not only legally robust, but also based on the principles of fairness, transparency, and accountability at every stage of data management. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is the main foundation for protecting individuals' rights to their personal data, whereby the process of collecting, storing, and using data must be carried out legally and openly to the data owner (Setiawan, 2018). The PDP Law also regulates various important principles, including accuracy, purpose limitation, and accountability, which ensure that personal data may only be used in accordance with the original purpose of its collection, and that the data controller is fully responsible for its security (Komparatif & Indonesia, 2023). In addition, the principles of integrity and confidentiality require digital service providers to protect data from illegal access and implement reliable security systems to prevent data leaks or misuse (Putra et al., 2024)

The application of these principles is highly relevant in the context of digital transactions and e-commerce, where users are often asked to submit personal data such as their full name, email address, phone number, and official identification as part of the account verification process. Although this step is intended to ensure the validity of transactions, practices in the field show that user data is often misused and even sold illegally on dark web sites without the owner's knowledge (Ham et al., 2025). The impact of personal data leaks is multidimensional, ranging from financial risks due to account hacking and identity fraud, to data misuse for political campaigns and manipulative advertising on social media. This phenomenon proves that without the implementation of effective basic data protection principles, people's privacy rights easily be violated by digital criminals (Ham et al., 2025).

As a result, leaks and misuse of personal data such as full names, email addresses, telephone numbers, and official identities lead to financial vulnerability through account hacking and identity fraud, as well as the potential misuse of such data for political campaigns and manipulative advertising on social media. This explanation is relevant because in digital transactions and e-commerce, users are often asked to submit personal data as part of the account verification process, which aims to ensure the validity of transactions. The context is that practices in the field show that even though user verification is intended for security purposes, user data is often misused or even sold illegally, including on dark web sites, without the owner's knowledge. Therefore, the application of basic data protection principles is very important in the digital ecosystem to ensure that people's privacy rights are not easily violated by cybercriminals (Supeno et al., 2025).

Without consistent application of data protection principles and appropriate technical mechanisms, users' privacy rights in the digital ecosystem will be easily eroded by uncontrolled data flows. to elaborate, principles such as data minimization, data security (confidentiality, integrity, availability) and accountability must be accompanied by technical mechanisms such as encryption, access control, audit logs, as well as organizational mechanisms such as internal policies and employee training to control risks; in the current context of digitalization where data moves quickly, across platforms and national borders, many studies show that technical and organizational frameworks are still weak in many organizations (Singh & Singh, 2018).

The Personal Data Protection Bill (PDP Bill) emerged as the state's response to a major challenge in the digital age, namely the increasing risk of privacy violations due to the massive and uncontrolled collection of personal data. This regulation shifts the paradigm from the protection of physical space to the protection of digital traces as part of a person's identity (Sadillah Ahmad et al., 2025). The main issue addressed by the PDP Bill is the lack of transparency in data management practices by many electronic system operators, whereby users are often not informed about how data is collected, processed, used, and stored. However, the principles of data sovereignty and consent-based processing require that every individual have the right to know, control, and consent to the use of their data (Komparatif & Indonesia, 2023).

The effectiveness of regulations depends heavily on the digital literacy of the public. In Indonesia, most citizens do not yet understand risks such as identity theft, misuse of digital documents, and data exploitation, for example, sharing photos of identity documents on social media or giving applications access to contact and location data. These seemingly trivial matters actually open up serious loopholes for digital crime (Sadillah Ahmad et al., 2025). Global data breaches, such as those on Facebook, show that personal data protection requires a strong and internationally synchronized legal framework. Many developing countries, such as Indonesia, are in a weak position when facing giant corporations in lawsuits over user losses (Sadillah Ahmad et al., 2025)

Therefore, the PDP Bill is not only a legal instrument, but also a constitutional basis that reinforces the role of the state in protecting citizens' rights in the digital space. Although Law No. 27 of 2022 on Personal Data Protection has been passed, its implementation must be accompanied by concrete steps such as the establishment of an independent supervisory agency, operational derivative regulations, capacity building for officials, and public education in order to develop safe and fair personal data governance (Firdaus, 2022).

The State's Constitutional Obligation to Protect Personal Data in the Era of Digital Government

The rapid development of information technology in the digital age has brought about major changes in Indonesia's constitutional law. Digital transformation, which has reached various sectors of life such as communication, government, economy, and public participation, has created new challenges in protecting human rights in the digital space. One of the main challenges is maintaining a balance between freedom of expression and the right to privacy, two constitutional rights guaranteed in the 1945 Constitution. On the one hand, freedom of expression is the foundation of digital democracy, which allows people to freely voice their opinions through online platforms. However, on the other hand, this development also increases the risk of individual privacy violations, especially in the form of personal data dissemination, hacking, digital surveillance, and unauthorized misuse of personal information (Hanafi, 2022)

In response to this, the constitutional legal system needs to be reformed so that it can adapt to the ever-changing social and technological realities. These changes should not only include the formulation of new regulations, but also adjustments to existing constitutional

norms, including explicit recognition that the protection of personal data is part of the human rights guaranteed by the constitution (Mahardika, 2021). In addition, future legal approaches must strengthen the principles of data sovereignty, responsible information transparency, and the active role of the state in preventing the misuse of technology by both public and private parties. The state has a constitutional obligation to ensure open and accountable governance, while still guaranteeing the protection of individual rights in the digital space (Anggen Suari & Sarjana, 2023).

The rapid development of information technology has brought about major changes in political participation and public decision-making processes. Nowadays, people can express their opinions directly through social media, online forums, and other digital channels, allowing voices that were previously unheard to influence public policy (Mannayong et al., 2024). This transformation has created more inclusive and dynamic public participation, but it has also given rise to legal challenges, particularly in the constitutional system. Legal norms are needed to revise the framework for digital participation so that the constitution can guarantee freedom of expression in the digital space while also establishing ethical and legal boundaries to prevent disinformation, hate speech, and manipulation of public opinion (Mudha'i Yunus, 2024).

On the other hand, the digital age has made privacy rights and individual freedoms increasingly vulnerable to abuse. The collection of personal data without consent, digital surveillance, and access to personal information by private entities or the state without clear controls reinforce the urgency of constitutionalizing the protection of personal data as a human right (Pramudito, 2020).

The rapid development of information technology, if not balanced with adequate legal protection, can open up huge loopholes for human rights violations, especially the right to privacy and personal data protection. In everyday practice, personal data is often taken for granted in digital interactions: people voluntarily share information such as their name, address, identity, transaction history, and biometric data on social media or applications without considering the long-term consequences. Public awareness of the potential for data exploitation by irresponsible parties is still very low. Constitutionally, the 1945 Constitution provides the basis for personal data protection: Article 28G paragraph (1) guarantees protection of the individual and a sense of security; Article 28H paragraph (4) affirms the right to protection of privacy, honor, dignity, and property rights. These provisions emphasize that privacy is an integral part of constitutionally protected human rights (Moh Bagas Fadhli Dzil Ikrom, 2024).

As a concrete measure, Indonesia passed Law No. 27 of 2022 on Personal Data Protection (PDP Law). This law stipulates that all personal data processing must be based on a legitimate legal basis, such as explicit consent from the data subject (Article 20). Furthermore, Article 27 mandates that the collection, storage, and processing of data must be carried out carefully, in a limited manner, and transparently in order to respect individual privacy (Media Hukum Indonesia, 2025). Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) emphasizes the important obligation of every Personal Data Controller to ensure the accuracy, completeness, and consistency of the personal data being managed. This is stipulated in Article 29, which requires personal data to be updated regularly to ensure it remains relevant and not misleading, thereby preventing harm to data subjects or other parties. Additionally, Article 31 of the PDP Law also regulates the obligation for Personal Data Controllers to record each stage of personal data processing as a form of transparency and legal accountability, enabling such activities to be audited and fully accountable (Theresa & Marlyna, 2024).

Article 36 of the PDP Law emphasizes that maintaining the confidentiality of personal data is an absolute obligation that must not be violated, both in electronic and non-electronic contexts. This provision is reinforced by Article 37, which requires Personal Data Controllers to supervise all parties involved in data processing, including Personal Data Processors and other third parties. Such supervision may be carried out through work contracts, periodic audits,

and the implementation of technical and administrative security standards to prevent data misuse (Safira Widya Attidhira & Yana Sukma Permana, 2022).

The establishment of the Personal Data Protection Authority (LPPDP) is a strategic step in realizing the mandate set out in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This institution was formed to ensure the effective implementation of personal data protection principles while strengthening legal governance in an increasingly complex digital era. The existence of the LPPDP shows that the state does not only view law as a set of written norms, but also as an institution and process that serves to realize substantive justice in society, in line with Mochtar Kusumaatmadja's thinking regarding the essence of law as a means of social renewal (law as a tool of social engineering) (Safira Widya Attidhira & Yana Sukma Permana, 2022).

Articles 59 and 60 of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) establish comprehensive authority for the Personal Data Protection Agency (LPPDP), including the formulation of national policies, supervision of data controllers and processors, and the enforcement of administrative law against data protection violations. With these powers, the LPPDP has a strategic role not only as a supervisor of policy implementation, but also as an authority that directs digital privacy governance and guarantees the protection of citizens' constitutional rights in cyberspacer (Setiawan, 2018).

Convergence efforts in privacy and personal data protection are very important to be realized immediately in Indonesia in order to create equal data protection standards with other countries, especially countries with more advanced economies (Suwadi et al., 2025). The implementation of personal data protection is not only related to the fulfillment of human rights to privacy, but also a strategic necessity in strengthening global cooperation, particularly in the fields of the digital economy, electronic commerce (e-commerce), and cross-border data flow (Judijanto et al., 2024).

The drafting and enactment of the Personal Data Protection Bill (RUU PDP) into law is expected to provide a comprehensive national legal framework that is in line with international practices, such as the General Data Protection Regulation (GDPR) in the European Union, the sectoral approach in the United States, and strict regulations in Japan and South Korea (Riswandi, 2023). The enactment of the Personal Data Protection Law (PDP Law) has the potential to strengthen Indonesia's position in the global arena and increase the confidence of investors and international partners in the government's commitment to protecting the security of information and privacy of citizens (BDO Indonesia, 2024). In the era of globalization and digital economic integration, personal data protection has become one of the main indicators in assessing the credibility and investment climate of a country (Hukumonline, 2024). In addition, the PDP Bill is also expected to address various threats of personal data misuse, especially against consumers who are increasingly active in the digital ecosystem. The existence of a strong legal umbrella will provide a sense of security to the public in conducting digital activities, including e-commerce transactions, the use of digital financial services, and interactions through social media (Xynexis, 2023).

Comprehensive regulations on personal data have the potential to generate positive economic impacts for Indonesia, as they can increase the confidence of businesses and international partners in domestic data governance (Rahmatullah et al., 2025). This trust is an important factor in increasing digital investment, expanding cross-border cooperation, and promoting sustainable technology-based economic growth. Legal certainty in personal data protection can create a secure and transparent digital ecosystem, thereby strengthening Indonesia's position in global trade and innovation (Abdullah et al., 2025). However, the legislative process for the PDP Bill experienced delays due to political and technical challenges. The urgency of this regulation is increasingly pressing as cases of personal data leaks and misuse in Indonesia continue to rise (Judijanto et al., 2024).

The delay in the ratification of the PDP Bill, which was not originally included in the 2018 National Legislation Program (Prolegnas), shows a gap between the legal needs of the community and the political response of the legislative body (Riswandi & Gultom, 2023). As a result, national data protection standards are not yet fully aligned with global practices, which risks leaving Indonesia behind in its efforts to guarantee the digital rights of its citizens (Hukumonline, 2024). As a result, Indonesia experienced a vacuum in substantive norms specifically regulating personal data governance amid increasing digital activities involving cross-sector and cross-border information exchange. This condition resulted in weak national data protection standards that were not fully in line with global practices, such as the General Data Protection Regulation (GDPR) in the European Union, which has become an international benchmark in guaranteeing the digital privacy rights of citizens (Abdullah et al., 2025).

This gap not only affects the protection of citizens' rights, but also Indonesia's position in the global digital economy ecosystem. The lack of domestic regulations that meet international standards poses the risk of low foreign investor confidence and potential barriers to cross-border data flow. The delay in harmonizing privacy regulations has made it challenging for Indonesia to create a secure and globally competitive digital environment. Accelerating the implementation and harmonization of the PDP Law with international data protection principles is crucial so that Indonesia can not only protect the digital rights of its citizens, but also compete in a digital economy based on trust and transparency (Laelaturramadani, 2025).

Through Constitutional Court Decision Number 5/PUU-VIII/2011, the Court affirmed that the right to privacy is part of human rights that falls under the category of derogable rights, namely rights that can be restricted under certain conditions in accordance with legal provisions (Mahkamah Konstitusi Republik Indonesia, 2011). The ruling also explains that the right to privacy includes protection of personal information, known as the right to information privacy, which in the modern context is synonymous with data privacy or data protection (Mahkamah Konstitusi Republik Indonesia, 2011). The protection of personal data in Indonesia has begun to be accommodated through derivative regulations of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), one of which is through Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions. Article 1 point 27 of the regulation states that personal data is specific personal data that is stored, maintained, kept accurate, and protected for confidentiality (Peraturan Pemerintah Nomor 82 Tahun 2012). This definition emphasizes the importance of storage, accuracy, and security in the management of personal data through electronic systems (Riswandi & Gultom, 2023)

This Constitutional Court ruling provides a strong legal basis that personal data is not merely ordinary information, but rather part of a constitutional right that must be protected by the state. The ruling affirms that the protection of personal data is an integral part of the right to personal protection as referred to in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees the right of every person to protection of their personal self, family, honor, dignity, and property (Mahkamah Konstitusi Republik Indonesia, 2011). The state has an obligation to ensure maximum protection of citizens' personal data as part of the human rights guaranteed by the constitution. As a result, regulations related to personal data protection in Indonesia are still scattered across various sectoral regulations that are not yet fully comprehensive and integrated. Prior to the enactment of Law No. 27 of 2022 on Personal Data Protection, regulations on the management and processing of personal data were only partially regulated in a number of laws such as the ITE Law, the Health Law, and the Banking Law without a comprehensive national legal umbrella (Saghara Luthfillah Fizara, 2022). However, to date, regulations related to personal data protection in Indonesia are still

scattered across various sectoral regulations that are not yet fully comprehensive and integrated (Judijanto et al., 2024).

Several regulations containing provisions on personal data protection include: Law No. 7 of 1992 on Banking, which was amended by Law No. 10 of 1998 on customer data confidentiality; Law No. 36 of 1999 concerning Telecommunications, which regulates the privacy of communication service users; and Law No. 11 of 2008 concerning Electronic Information and Transactions, which was later revised through Law No. 19 of 2016, which emphasizes the protection of electronic data and individual privacy rights (Peraturan Pemerintah Nomor 82 Tahun 2012). In addition, there is Law No. 36 of 2009 concerning Health, which regulates the confidentiality of medical data, as well as Law No. 23 of 2006 concerning Population Administration, which provides a legal basis for the protection of population data such as NIK and residents' addresses (Rahmatullah et al., 2025).

Although a number of these regulations govern certain aspects of data privacy, the approach is still sectoral in nature and does not yet form a comprehensive protection system. This situation creates legal gaps and weaknesses in the enforcement of data protection in the digital age, which demands higher standards of security and privacy (Hukumonline, 2024). Therefore, an umbrella regulation is needed to regulate personal data protection in an integrated and comprehensive manner as a form of implementing human rights in the context of information technology development (BDO Indonesia, 2024).

CONCLUSION

The protection of privacy rights over personal data in Indonesia is a constitutional issue that is becoming increasingly important amid the rapid pace of global digitalization. Advances in information technology bring enormous benefits in terms of the efficiency of public services, governance, and the digital economy, but they also pose a serious threat to the security of personal data. The phenomenon of data leaks and misuse of information shows that the national legal system is still weak and fragmented across sectors, without a comprehensive protection framework.

Legally, Constitutional Court Decision Number 5/PUU-VIII/2011 has confirmed that the right to privacy is part of the human rights guaranteed by the constitution and includes the protection of personal data. This is an important basis for the state to guarantee the security of its citizens' information. The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) is a major milestone in the establishment of an integrated data protection legal system based on the principles of fairness, transparency, and accountability.

However, the effectiveness of the PDP Law still depends heavily on consistent implementation through the establishment of a Personal Data Protection Supervisory Agency (LPPDP), increased digital literacy among the public, and synergy between state institutions and the private sector. In addition, harmonization with international standards such as the General Data Protection Regulation (GDPR) is also necessary so that Indonesia can guarantee the privacy rights of its citizens while strengthening global confidence in national data governance.

Constitutional guarantees of the right to personal data privacy must be realized not only in the form of formal regulations, but also through the application of the principles of data sovereignty, consent-based processing, and responsibility by design, so that the digital rights of citizens are effectively protected in an era of increasingly open digital government and economy.

REFERENCE

Abdullah, C., Durand, N., & Moonti, R. M. (2025). Transformasi Digital dan Hak atas Privasi: Tinjauan Kritis PelaksanaanUU Perlindungan Data Pribadi (PDP) Tahun 2022 di Era Big

Data. *Politik Dan Hukum Indonesia*, *2*(3), 233–241. https://doi.org/10.62383/amandemen.v2i3.1073

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

BDO Indonesia. (2024). *Pengenalan Undang-Undang Perlindungan Data Pribadi Resmi (UU PDP)*. Bdo Indonesia.

Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, *4*(2), 23–31. https://doi.org/10.52005/rechten.v4i2.98

Ham, D. P., Asthi, M., Ari, S., Hakim, A., & Baihaqy, A. (2025). *ANALISA DAMPAK KEBOCORAN DATA PUSAT DATA NASIONAL (PDN) Andhika Pratama Adhi Surya M . Asif Nur Fauzi*. *4*(156), 31–37.

Hanafi. (2022). Urgensi Pengaturan Hukum Tentang Perlindungan Data Pribadi Pada Sistem Digital Dalam Pemenuhan Hak Privasi Di Indonesia. *SULTAN ADAM: Jurnal Hukum Dan Sosial*, *1*(1), 13–23. https://doi.org/10.71456/sultan.v1i1.143

Hukumonline. (2024). *Strategi dan Tantangan Implementasi UU Pelindungan Data Pribadi di Perusahaan*. Hukumonline.

Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*, *3*(01), 20–29. https://doi.org/10.58812/eslhr.v3i01.351

Komparatif, P., & Indonesia, S. (2023). *Akuntabilitas Dalam Kebijakan Perlindungan*. *8*, 89–102.

Laelaturramadani. (2025). Tinjauan Terhadap Efektivitas Regulasi Perlindungan Data Pribadi di Indonesia. *Mandalika Law Journal*, *3*(1), 38–48. https://ojs.cahayamandalika.com/index.php/mlj/article/view/5469/4034

Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal, M., & Rahmadia, M. H. (2023). *Implementasi Uu Perlindungan Data*. *5*(20), 115–131.

Mahardika, A. G. (2021). Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi Dalam Sistem Ketatanegaraan Indonesia. *Jurnal Hukum Unissula*, *37*(2), 101–118. https://doi.org/10.26532/jh.v37i2.16994

Mahkamah Konstitusi Republik Indonesia, 1 ========== 1 (2011). http://ridum.umanizales.edu.co:8080/jspui/bitstream/6789/377/4/Muñoz_Zapata_Adriana_Patricia_Artículo_2011.pdf

Mannayong, J., S, M. R., & Faisal, M. (2024). Transformasi Digital dan Partisipasi Masyarakat : Mewujudkan Keterlibatan Publik yang Lebih Aktif Digital Transformation and Community Participation : Realizing More Active Public Engagement. *Jurnal Administrasi Publik*, *XX*(1), 51–72.

Moh Bagas Fadhli Dzil Ikrom, T. B. (2024). Perlindungan Hukum Hak Privasi Warga Negara terhadap Kebocoran Data Pribadi di Indonesia Legal Protection Of Citizens' Privacy Rights Against Personal Data Leaks In Indonesia. *Contitution Jurnal*, *3*(2), 139–154.

Mudha'i Yunus, H. S. (2024). *JURNAL RENVOI : Jurnal Hukum dan Syariah vol 1 No. 2 January 2024*. *1*(2), 75–89.

Muin, I. (2023). Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia. *MJP Journal Law and Justice (MJPJLJ)*, *1*(2), 81–91. https://jurnalilmiah.co.id/index.php/MJPJLJ

Penelitian, A. (2024). *VOLUME 7 ISSUE 3 MARET 2024 Perlindungan Hukum Data Pribadi Pengguna Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi di Indonesia Legal Protection of Personal Data of Information Technology- Based Lending and*

Borrowing Service Users in Indonesia. *7*(3), 1320–1325. https://doi.org/10.56338/jks.v7i3.4644

Pramudito, A. P. (2020). Kedudukan dan Perlindungan Hak Atas Privasi di Indonesia. *Jurist-Diction*, *3*(4), 1397. https://doi.org/10.20473/jd.v3i4.20212

Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara*, *34*(3), 239–249. https://doi.org/10.29303/jtsw.v34i3.218

Putra, R. K., Idris, M. F., & Widhiati, G. (2024). Perlindungan Data Pribadi Dalam Era Big Data : Implikasi Hukum Di Indonesia. *Jaksa : Jurnal Kajian Ilmu Hukum Dan Politik*, *2*(4), 31–44. https://journal.stekom.ac.id/index.php/Jaksa/article/view/2260

Rahmatullah, I., Suwadi, P., Purwadi, H., & Laehseng, R. (2025). Legal uncertainty in cross-border data transfers in Indonesia: A call for reform. *Towards Resilient Societies: The Synergy of Religion, Education, Health, Science, and Technology*, *Casarosa 2020*, 573–579. https://doi.org/10.1201/9781003645542-92

Riswandi, B. A., & Gultom, A. M. (2023). Protecting Our Mosts Valuable Personal Data: a Comparison of Transborder Data Flow Laws in the European Union, United Kingdom, and Indonesia. *Prophetic Law Review*, *5*(2), 179–206. https://doi.org/10.20885/PLR.vol5.iss2.art3

Sadillah Ahmad, R., Puspaningtyas, D. A., & Ismariy, M. N. K. Al. (2025). Perlindungan Hukum Terhadap Privasi Data Pribadi Di Era Digital. *The Juris*, *9*(1), 15–23. https://doi.org/10.56301/juris.v9i1.1307

Safira Widya Attidhira, & Yana Sukma Permana. (2022). Review of Personal Data Protection Legal Regulations in Indonesia. *Awang Long Law Review*, *5*(1), 280–294. https://doi.org/10.56301/awl.v5i1.562

Saghara Luthfillah Fizara, S. . (2022). *Perkembangan Regulasi Perlindungan Data Pribadi*. SIPLAWFIRM. https://siplawfirm.id/perkembangan-regulasi-perlindungan-data-pribadi/?lang=id&utm_source=c

Saputra, D. F. (2023). Literasi Digital untuk Perlindungan Data Pribadi. *Jurnal Ilmu Kepolisian*, *17*(3), 1–8.

Satrio Pangarso Wisanggeni. (2020). *AWAS, PENJAHAT SIBER MENGINCAR DATA PRIBADIMU*. https://interaktif.kompas.id/baca/awas-penjahat-siber/?

Setiawan, A. B. (2018). Revolusi Bisnis Berbasis Platform Sebagai Penggerak Ekonomi Digital Di Indonesia. *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *9*(1), 61. https://doi.org/10.17933/mti.v9i1.118

Singh, N., & Singh, A. K. (2018). Data Privacy Protection Mechanisms in Cloud. *Data Science and Engineering*, *3*(1), 24–39. https://doi.org/10.1007/s41019-017-0046-0

Supeno, S., Rosmidah, R., & Iqbal, S. M. U. (2025). Personal Data Protection in Review of Legal Theories and Principles. *Journal of Law and Legal Reform*, *6*(3), 1349–1376. https://doi.org/10.15294/jllr.v6i3.10252

Theresa, G., & Marlyna, H. (2024). Pelindungan Data Pribadi pada Layanan Pendanaan Berbasis Teknologi Informasi Pasca Undang-Undang Nomor 27 Tahun 2022 dan Undang-Undang Nomor 4 Tahun 2023. *Jurnal Hukum & Pembangunan*, *54*(2). https://doi.org/10.21143/jhp.vol54.no2.1631

Wahyu Destanti, R. S., & Aris Yuni Pawestri. (2025). Perlindungan Hak Konstitusional Pemilik Data Pribadi Berupa Nomor Telefon Yang Dicantumkan Sebagai Nomor Darurat Secara Ilegal Pada Pinjaman Online (Dalam Perspektif Undang-Undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi). *Indonesian Journal of Law and Justice*, *3*(1), 12. https://doi.org/10.47134/ijlj.v3i1.4573

Wijaya, J., Nursanthy, A. T. R., & Thamrin, M. A. (2024). Perlindungan Terhadap Data Pribadi Dalam Berselancar Di Dunia Maya. *The Juris*, *8*(2), 638–644. https://doi.org/10.56301/juris.v8i2.1477

Xynexis. (2023). *UU PDP: Langkah Awal Melindungi Data Pribadi*. Xynexis.Com.