Jurnal Notariil

Jurnal Notariil, Vol. 9, No. 2, 2024; 71-75 P ISSN 2540 - 797X
Available Online at https://ejournal.warmadewa.ac.id/index.php/notariil E ISSN 2615 - 1545

LEGAL PROTECTION OF PERSONAL DATA OF INDONESIAN CITIZENS BASED ON ACT NUMBER 27 OF 2022

Ni Made Dwi Gayatri Putri[1*], Dewa Gede Wibhi Girinatha[2]
1. Master of Law, Universitas Warmadewa, Indonesia
2. Associate Notary, Indonesia
*Email : pgayatri11@yahoo.com

How To Cite:
Putri, N, M, D, G., Girinatha, D, G, W. (2024). Legal Protection of Personal Data of Indonesian Citizens Based on Act Number 27 of 2022. *Jurnal Notariil*, 9 (2), 71-75, Doi: https://doi.org/10.22225/jn.9.2.2024.71-75

Abstrak

The purpose of this research is to analyze personal data, which is private and must be protected. Numerous cases of personal data breaches in Indonesia have had detrimental effects on society. The lack of comprehensive legislation results in inadequate legal protection against data breaches. Due to the frequent occurrence of personal data breaches, the government enacted the Personal Data Protection Law Number 27 of 2022. This research employs normative methods with a legislative and conceptual approach. The findings reveal that legal protection against personal data breaches is comprehensive under Law Number 27 of 2022. Preventive efforts to protect personal data include not sharing data by the public and avoiding illegal platforms prone to cybercrime. There is also a need for public awareness to safeguard personal data. Meanwhile, the government will conduct compliance testing and take repressive protective measures. If a personal data breach occurs, the sanctions outlined in the Personal Data Protection Law include criminal penalties under Articles 67 and 68, which stipulate fines and imprisonment, and Article 70 for corporate violations.

Keywords: law number 27 of 2022; legal protection; personal data

1. INTRODUCTION

Era of globalization, the development of technology and the internet is happening at an incredibly rapid pace. Human activities are now closely tied to technology and the internet. Human existence is inherently intertwined with specific evolving patterns that mature, gain consensus, and serve as societal norms. The development of technology and information allows for the rapid distribution of information and data. One example is the ability to search for information and communicate through mobile phones. With mobile phones, people can quickly access various media using advanced technology, making it easier to obtain and share information without being hindered by time and distance. Today, Electronic information and communication systems have permeated nearly every facet of society, giving rise to emerging markets. Consequently, the societal economic landscape has shifted from traditional manufacturing-based economies to what is now termed the "digital economy" or the "Creative Economy," emphasizing information, intellectual ingenuity, and knowledge.

Era of globalization, human activities are closely related to technology and the internet. Human interaction is inherently bound by particular evolving patterns that expand, evolve, gain consensus, and serve as guiding principles in people's lives (Mahendrawati Made Ni Luh, 2021). The advancement of technology and information applied in various aspects of society is always closely related Safeguarding personal data is essential, considering it a valuable asset. Indonesian law, as outlined in the Constitution of the Republic of Indonesia Year 1945 Article 28G paragraph (1), asserts the right to privacy, family, honor, possessions, and the right to feel secure. Protecting these rights is fundamental to the advancement

of human values.

Throughout its evolutionary history, privacy has been a widely recognized and acknowledged concept in many countries, both formally through legislation and informally through moral norms (Rosadi Dewi, 2009). Frequent occurrences of breaches of personal data security often result in significant losses for society, especially for the data owners themselves. Several prominent cases, Instances involving breaches of personal data security leading to fraud or criminal activities, like pornography, highlight the pressing need for legal frameworks to safeguard personal data. (Djafar Wahyudi, 2014).

Personal data is integral to an individual's right to privacy, encompassing the entitlement to lead a private life devoid of unwarranted interference. The lack of comprehensive regulation leads to legal uncertainty, making it difficult for aggrieved parties to pursue their rights through legal means.

Indonesia, the protection of personal data is addressed through various laws, including the Human Rights Law, the Electronic Information and Transactions Law, the Population Administration Law, the Banking Law, the Health Law, the Consumer Protection Law, the Public Information Disclosure Law, and the Telecommunications Law. However, these regulations only offer partial coverage and do not provide a comprehensive framework for personal data protection.

The current regulations inaccurately only impose administrative sanctions such as warnings, oral or written reprimands, temporary cessation of activities, and/or announcements on websites, with procedures governed by ministerial regulations. However, there are still unresolved issues regarding leaks of personal data. The authorized institutions often hesitate to impose penalties related to the misuse of personal data, resulting in legal unfairness and difficulties for aggrieved parties to pursue their rights.

After observing numerous cases concerning personal data, on September 20, 2022, the House of Representatives and the President approved the Draft Law (RUU) concerning Personal Data Protection, which was later enacted as Law Number 27 of 2022. This PDPA Law is designed to be applicable to all parties processing personal data of the public, including individuals, companies, governments, private entities, as well as various institutions providing services in Indonesia, both domestically and internationally. Based on this background, several issues are formulated as follows: How is the regulation of personal data protection governed according to Law Number 27 of 2022, and what are the legal aspects protecting the confidentiality of Indonesian citizens' personal data in the context of widespread dissemination.

2. METHOD

This research method uses normative legal methods, statute approach, and conceptual approach. It focuses on the analysis of legal materials and relevant issues. The main aim is to identify solutions to emerging legal problems, thereby producing recommendations regarding normative principles that must be applied.(Soetrisno Hadi, 1995)

The success of a research greatly depends on how the research is conducted. The selection of research methods is based on considerations regarding the suitability with the research subject, the objectives of the research, the variables to be investigated, and the problems to be solved. Research methods are efforts to discover, develop, and test the truth of knowledge through scientific approach.(Peter Mahmud Marzuki, 2011)

This research seeks to delve into the legal mechanisms established for safeguarding the personal data of Indonesian citizens, as outlined in Law Number 27 of 2022.

3. RESULT AND DISCUSSION

Regulation of Personal Data Protection According to Law Number 27 of 2022

Personal information can be considered something of great economic value (Makarim Edmon, 2003). The safeguarding of personal data encompasses the practice of ensuring the confidentiality of individuals' information, whether processed electronically or otherwise within society. The Personal Data Protection (PDP) Law was officially enacted and announced in the Republic of Indonesia on October 17, 2022. Comprising 26 chapters and 76 articles, this law comprehensively regulates various aspects pertaining to the protection of personal data. It delineates the rights of personal data subjects, the procedures for personal data processing, the responsibilities of data controllers and

processors, as well as the prohibitions and associated administrative and criminal penalties for infringements on personal data protection measures.

The Personal Data Protection (PDP) Law applies to all individuals, institutions, and international groups who commit violations within or outside the jurisdiction Indonesia, that have legal consequences. Thus, personal data protection covers those residing within the jurisdiction of RI as well as Indonesian citizens (WNI) living abroad.

Under the Personal Data Protection (PDP) Law, protected personal data pertains to information concerning individuals that can be identified directly or indirectly through electronic or non-electronic means. This law categorizes personal data into two main types: specific and general. Specific personal data comprises details like health records, biometric information, genetic data, criminal records, information regarding children, personal characteristics, and other data specified by law. On the other hand, general personal data includes publicly accessible information such as full names, gender, religion, marital status, and data combinations that facilitate individual identification.

In the process of personal data processing, two key roles are identified: data controllers and data processors. A data controller refers to an individual, institution, or organization responsible for processing personal data, often on behalf of the data subject. Conversely, a data processor is an individual, public authority, or organization tasked with handling personal data, which encompasses various stages such as acquisition, collection, storage, correction, updating, dissemination, as well as the deletion or destruction of personal data.

The Guidelines for Personal Data Protection in the personal data processing process are delineated in Article 16, paragraph (2), comprising eight points. Additionally, Article 18 specifies that personal data processing may involve two data controllers, subject to contractual agreements between them and interconnected purposes. Furthermore, Article 19 underscores that both data controllers and data processors may be individuals, public institutions, or international organizations. They are both mandated to uphold personal data protection obligations in alignment with the provisions outlined in Articles 20 through 54 of the Personal Data Protection Law.

Issues concerning personal data protection can be addressed through diverse methods, including arbitration, litigation, or alternative dispute resolution mechanisms as stipulated by legislation. Valid evidence in these resolution processes may take various forms, including those governed by procedural law, electronic information, and electronic documents, all in accordance with the provisions of the legislation.

The Personal Data Protection (PDP) Law delineates four types of violations across Articles 67, 68, and 70. For instance, Article 67 specifies that activities like illicitly acquiring personal data for personal benefit at the expense of the data subject, or the unauthorized use of personal data not belonging to oneself, may result in imprisonment for a maximum of five years and a fine of up to five billion. These articles also address various other violations, each accompanied by corresponding criminal penalties and fines.

Article 68 of the Personal Data Protection (PDP) Law stipulates that individuals who intentionally fabricate or alter personal data for personal gain can face imprisonment for up to six years and a fine of up to six billion. Additionally, Article 70 specifically addresses corporate violations outlined in Articles 67 and 68. In such instances, penalties may be imposed on directors, controlling shareholders, government officials, beneficial owners, and/or the corporation itself. Fines could potentially amount to ten times the maximum prescribed fine. For corporations, penalties might include fines, seizure of profits, business suspension, payment of damages, permit revocation, closure, or dissolution.

An independent supervisory entity, referred to as the "data protection authority," will be established to oversee the enforcement of personal data protection measures. This institution is charged with monitoring compliance with personal data protection regulations, administering administrative penalties for violations of the law, and facilitating alternative dispute resolution mechanisms outside of the judicial system. Furthermore, with the enactment of this legislation, the Ministry of Communication and Informatics (Kominfo) will be responsible for regulating the management of personal data by Electronic System Providers.

A two-year transition phase is mandated for the implementation of the Personal Data Protection (PDP) Act. Despite the law being enacted, its enforcement is currently stalled due to the absence of detailed implementing regulations directly derived from the PDP Act. It is emphasized that the formulation and guidance provided in the regulations should be approached with a perspective that fosters mutual synergy among stakeholders, prioritizing societal welfare, growth, and environmental considerations (Mahendrawati Made Ni Luh, 2020). Creating detailed implementing regulations demands specialized expertise and must be customized to suit the unique characteristics of each region.

Legal Protection Against the Disclosure of Personal Data Confidentiality of Indonesian Citizens

Legal Protection refers to efforts to ensure that individual rights are fulfilled and to provide assistance in feeling secure, especially for witnesses and/or victims of crimes. It is an integral part of efforts to protect the community as a whole and can be realized in various ways, such as through restitution, compensation, medical services, and legal support.

Meanwhile, Personal Data is information related to an individual's life. The safeguarding of personal data is integral to human rights and must be upheld. Individuals possess the right to dictate how their information is stored and managed by others.(Rosadi Dewi, 2015)

Safeguarding personal rights enhances humanitarian values, fosters stronger bonds within communities, empowers individuals with greater autonomy to assert and protect their rights, encourages tolerance, reduces the risk of discrimination, and serves to constrain government authority (Danrivanto Budhijanto, 2010). It's a common phenomenon to encounter numerous issues of personal data breaches that result in significant losses for individuals whose data is compromised.

The misuse of personal data can occur inadvertently due to society's negligence in everyday activities. For instance, when registering for a SIM card requiring an ID number, casually displaying phone numbers on billboards that can be misused, or when downloading applications that request personal data through forms. The use of email can also pose a risk if individuals do not understand how to secure it, as emails can store various personal information and can be accessed by others if login information is shared.

Although there are laws in place to protect personal data, such as the Personal Data Protection Act (PDPA), individual awareness is also crucial to safeguard their personal data. Measures such as using strong passwords, avoiding suspicious links, limiting privacy permissions on applications, using legal software, regularly backing up data (like storing data on Google Drive), and refraining from sharing personal information are also necessary.

Preventive efforts in personal data protection involve actions to avoid sharing data by the public and avoiding the use of unauthorized platforms that may lead to cybercrimes. Indeed, public awareness regarding the significance of safeguarding personal data is crucial. Meanwhile, the government will conduct compliance tests to ensure that electronic systems comply with the regulations established in the Personal Data Protection Act.

Repressive measures in cases of personal data breaches involve the application of sanctions stipulated in the Personal Data Protection Act (PDPA). Article 67 and Article 68 of the PDPA regulate penalties in the form of fines and/ or imprisonment for individuals who violate the law, while Article 70 provides sanctions for violations within corporations. If there is non-compliance with the PDPA and a personal data breach occurs, the sanctions outlined in the PDPA will be enforced.

4. CONCLUSION

Personal Data Protection Law (UU PDP) has been completely drafted, consisting of 26 chapters and 76 articles which regulate various aspects related to personal data protection. This law covers the rights of personal data subjects, the processing of personal data, the responsibilities of personal data controllers and processors, prohibitions, as well as administrative and criminal sanctions. To implement the PDP Law effectively, it is important to have supporting implementing regulations. Therefore, a 2 year transition period is needed to unify the implementation of the PDP Law. Preventive efforts such as avoiding sharing data on illegal platforms that can lead to cybercrime, as well as increasing public awareness about the importance of protecting personal data, are very important in protecting personal

data. Government is expected to carry out compliance tests with the regulations of the PDP Law in order to create compatibility between existing regulations and the obligations that must be fulfilled by electronic systems. In addition, repressive protection efforts are also carried out in cases of personal data violations, with sanctions including fines and imprisonment for individual violators, as well as sanctions for corporate violators as regulated in Article 70 of the PDP Law.

REFERENCES

Danrivanto Budhijanto, 2010, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi*, PT. Refika Aditama, Bandung.

Djafar Wahyudi, Komarudin Asep, 2014, *Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci,* Elsam, Jakarta.

Mahendrawati Made Ni Luh, 2021, *Journal Atlantis Press*, *The Principle of Balance to Realize Justice of The Parties in Standard Agreements for Business Format,* Volume 605, Universitas Warmadewa, Bali.

Mahendrawati Made Ni Luh, dan Maha Putra Agustya Gede I.B, 2020, *Management of Community Markets to Provide Well-Being to Community n The Badung District*, Warmadewa Press, Bali.

Makarim Edmon, 2003, *Kompilasi Hukum Telematika*, Raja Grafindo Perkasa, Jakarta.

Peter Mahmud Marzuki, 2011, *Penelitian Hukum*, Kecana Prenada Media Group, Jakarta.

Rosadi Dewi, Sinta, 2009, *Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasiona*l, Widya Padjadjaran, Bandung.

Rosadi Dewi, Sinta, 2015, *Aspek Data Privasi Menurut Menurut Hukum Internasional, Regional, dan Nasional*, *Cet. I*, Widya Padjajaran, Bandung.

Soetrisno Hadi, 1995, *Metode Research*, Yogyakarta: Andi Offset.