

LEGAL DEVELOPMENT AND URGENCY OF PERSONAL DATA PROTECTION IN INDONESIA

Yohanes Leonardus Ngompat^{1*}, Mary Grace Megumi Maran²

^{1,2}Fakultas Hukum, Universitas Katolik Widya Mandira, Kupang, Indonesia

lleonardnk@gmail.com^{1*}, meggymarygrace@gmail.com²

Abstract

This research aims to know and analyze the development of personal data protection law and to know and analyze the urgency of personal data protection in Indonesia. This research is normative juridical research using secondary data. The approaches used are legislative and historical approaches. The data collected is then analyzed qualitatively. Based on the results of the research, it is known that the laws and regulations on personal data protection continue to develop from time to time. The regulation begins with the inclusion of Article 28 G Paragraph (1) in the 1945 Constitution which becomes the legal basis in guaranteeing the rights of every person or owner of personal data and reaches the peak where a special regulation has been formed that specifically regulates the protection of personal data, namely in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Previously, the regulation on personal data protection was regulated partially and sectorally, so with the enactment of the PDP Law, there is a special regulation related to personal data protection. In relation to the urgency of personal data protection, personal data is important to protect because along with the development of technology and information, it is easier for violations to occur, including the misuse of personal data. Violations of personal data should be prevented and handled seriously because personal data is very important data related to one's privacy. Protection of personal data can ultimately increase public confidence in providing personal data to support government policies in fulfilling public interests without violating people's personal rights.

Keywords: Legal Development; Urgency; Personal Data Protection; Indonesia

INTRODUCTION

Legal protection of personal data is the most crucial thing today. The protection is the answer to the rapid development of information technology. The development of technology and information also touches the country of Indonesia, where at this time Indonesia has entered the era of digital economy and industry 4.0 which has resulted in an increase in internet users. Based on the data obtained, out of a total population of 262 million people, there are 140 million people who use the internet in their daily lives (Sinaga & Putri, 2020). The development of information technology has both positive and negative impacts. The positive impact of the development of information technology certainly provides convenience and comfort for the community, for example in the aspect of electronic-based trading or often called e-commerce. If previously people needed a long time to buy goods, then with the sophistication of technology it is easy with one click through the e-commerce platform, the purchased goods will be sent to their destination. Meanwhile, the negative impact of the development of information technology can threaten the security of consumer personal data in electronic-based trading if the e-commerce platform leaks personal data.

Various kinds of electronic platforms are currently emerging and have many benefits such as providing convenience in long-distance communication, providing electronic-based marketplaces such as shoppe to provide convenience in online buying and selling transactions. The platform provider provides an obligation to users or consumers to access the electronic platform must agree to the terms and conditions of the electronic platform. One of the conditions that must be met by users or consumers is to provide personal data and consent so that the provider or controller of personal data can manage the personal data. Personal data controllers also have the obligation to protect personal data belonging to users or consumers so that no leakage occurs which results in harm to users or consumers for their personal data.

Personal data is data in the form of identity, code, symbol, letter or number of a person's personal marker that is private and confidential (Kusnadi, 2021). Personal data is a very valuable asset or commodity. Like the definition of personal data above, personal data is the privacy owned by each person. So that if data is referred to as personal data if it is related to a person, it can be used to identify that person as the owner of the data. An identifiable person is someone who can be recognized or identified directly or indirectly based on an identification number or based on one or more specific factors of physical, psychological, mental, cultural or social identification (Ngompat, 2023). Protection of the owner of personal data is an obligation to maintain its confidentiality, because it is privacy for the owner of personal data. This means that the personal data of a person is an inherent part of him, so that no one is allowed without obtaining the rights of the owner of the personal data to manage or use the personal data.

Personal data protection is linked to the concept of privacy. This concept requires the protection of personal integrity and dignity. Through the concept of privacy, everyone is given the right to determine who holds information about them and has the right to determine the use of that information (Priliyasi, 2019). Discussions on personal data protection have been conducted at the international, regional and national levels. In this case, there are recommendations issued by international and regional organizations that aim to serve as guidelines for member countries in providing protection to personal data. These recommendations also influence the formation of personal data protection regulations in each country. Among them is The OECD Privacy Framework published by the Organization for Economic Co-Operation and Development (OECD) in 1980 which was revised in 2013. In addition, ASEAN as a regional organization in Southeast Asia has also issued a Framework on Personal Data Protection agreed upon at the ASEAN Telecommunications and Information Technology Ministers Meeting (Telmin) (Yuniarti, 2019).

These recommendations then become one of the guidelines for countries to ensure the protection of personal data in a legal regulation. The regulation of personal data protection in

Indonesia is not a new thing. This is because legal provisions regarding personal data protection have been included in the Constitution, namely in Article 28 G paragraph (1) of the 1945 Constitution. This article calls for the protection of every person for themselves, including their family, honor, dignity, and property under their control, as well as the right to security and protection from threats of fear to do or not do something which is a human right.

As we know, lately there are often targets of personal data theft carried out by hackers by breaking into or hacking software. Apart from being caused by hackers, in certain circumstances personal data leakage is also caused by the negligence of personal data controllers of personal data due to the weak functioning of electronic systems. Therefore, it is very important to understand together the development of personal data protection law in Indonesia so that everyone becomes aware of the legal basis for personal data protection in Indonesia and can become a guideline or guide for everyone who needs protection of their personal data. Based on this explanation, in this paper the author wants to analyze how the development of personal data protection law in Indonesia and the urgency of personal data protection in Indonesia.

RESEARCH METHODS

This research is a normative juridical research. Normative juridical research is research that uses positive legal norms as the object of research. The data source used in normative juridical research is secondary data consisting of primary legal materials and secondary legal materials. Primary legal materials are the main legal materials such as laws and regulations. Secondary legal materials are legal materials derived from literature studies such as books, legal journals and articles related to this study. The approach method used in this research is a statutory approach by examining both laws and regulations related to this study and a historical approach to examine the development of personal data protection law. The data that has been collected is analyzed using qualitative techniques.

RESULT AND DISCUSSION

Personal data is always closely related to a person's characteristics. Personal data is often identified with identity, code, symbol, letter or number as a marker for someone who has personal and confidential nature (Windriani et al., 2023). Personal data is classified into two types, namely general personal data and specific personal data. General personal data such as full name, gender, nationality, religion, occupation and place of residence (Meher et al., 2023). Meanwhile, specific personal data consists of data related to health, biometric data, genetic data, sexual life or orientation, political views, criminal records, child data, financial data and other data in accordance with statutory provisions (Marzuki, 2021). This personal data is a right owned by the owner of the personal data and it is not allowed to process or utilize the personal data without the knowledge or permission of the owner of the personal data. To ensure the protection of privacy, the state is obliged to protect as mandated by the constitution in Article 28 G Paragraph (1) which guarantees the protection of personal, family, honor, dignity and all property under its control.

Developments in the world of information technology currently provide convenience for the community. However, there are other implications of advances in information technology that can also harm the community. Seeing the things experienced by the community, the state, through authorized institutions must formulate a regulation to provide protection to personal data owners. As we know, the regulation on personal data protection was previously regulated partially and sectorally until the enactment of a special regulation on personal data protection. In this regard, the following will describe the development of regulations governing personal data protection in Indonesia.

Development of Personal Data Protection Law

1. The 1945 Constitution of the Republic of Indonesia (UUD 1945).
The Constitution is the highest law in the order of legislation in Indonesia. This makes the Constitution referred to as the source of all sources of law. Therefore, every regulation under the Constitution must not conflict with the Constitution in the formulation of article by article. If a regulation under the Constitution contradicts the Constitution, then the regulation has no binding legal force. The preamble of the Constitution guarantees the independence of all nations. Then explicitly in the preamble, it also requires the establishment of a government to protect all Indonesian people. This then results in the state, through the government, being obliged to provide protection, including in relation to personal data. Such protection is regulated in Article 28 G Paragraph (1). In the context of personal data protection, this article has become the legal basis and guarantees rights for every person or owner of personal data.
2. Law Number 8 of 1997 on Company Documents.
Basically, this law comes as a response to the influence of economic and information globalization due to the rapid development of the economy and trade both nationally and internationally. These developments have implications for the use of documents in the business world by utilizing technological advances to increase effectiveness and efficiency in the management of company documents. In the management of company documents in accordance with the provisions of this law, it still prioritizes the protection of the interests of the parties in legal relations. This means that all processes of making, storing, transferring, destroying and releasing company documents must not violate the provisions of this law because it can harm the parties who have legal relations. One of the government's efforts in establishing this law is to provide protection for company documents owned by the parties, because in fact these documents are an inseparable part of a person's personal data.
3. Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking.
Banking law has realized the protection of customers by giving banks the obligation to keep information about customers confidential, although with some exceptions. This has been regulated in Article 40 Paragraph (1). Even when there is a violation committed by the bank, it can be subject to administrative sanctions for not fulfilling its obligations in the form of revocation of business license. The enactment of this law can certainly increase customer confidence in banks because it has regulated protection including the protection of personal data for customers.
4. Law Number 36 of 1999 concerning Telecommunications.
The development of technology today requires everyone to adapt or adjust to existing developments. Telecommunication is an integral part that cannot be separated from current information technology. One of the obligations of telecommunications is to protect the interests and security of the state. It can be interpreted that the interests and security of the state are the interests and security of society, because without society the state cannot exist. Protection related to personal data regulated in Law Number 36/1999 on Telecommunication can also be seen in Article 40 which regulates the prohibition of tapping activities on information transmitted through telecommunications networks in any form. Tapping activities are prohibited in this law because through tapping other people's information can be obtained illegally. This information is a personal right that must be protected. The telecommunications law has ensured legal certainty and provided protection for both telecommunications providers and users.
5. Law Number 1 Year 2008 on Electronic Information and Transactions, which was last amended by Law of the Republic of Indonesia Number 1 Year 2024 on the Second

Amendment to Law Number 1 Year 2008 on Electronic Information and Transactions (UU ITE).

UU ITE is one of the regulations that provide protection for personal data. This can be seen in Article 26 paragraph (1) which requires that the use of any information through electronic media concerning a person's personal data must be done with the consent of the person concerned. This aims to prevent personal data from being misused for negative purposes, considering that the right to protection of personal data is also one of the human rights that should be protected. This regulation also reiterates that personal data protection is an integral part of personal rights. This personal right implies, among other things: the right to monitor access to information about one's personal life and data. Therefore, the use of information and technology is expected not to harm a person's personal data.

6. Law Number 43 of 2009 concerning Archives.

The archive creator or archive manager in Article 44 can close access to the archive if it reveals secrets or personal data. This allows for the protection of personal data.

7. Law No. 24 of 2013 on the Amendment to Law No. 23 of 2006 on Population Administration.

As stipulated in the 1945 Constitution, it is obligatory to provide protection for both personal and others. In the context of population administration, the protection is related to population data. This law guarantees protection to both Indonesian citizens and foreigners residing in Indonesia. The amendment of Law No. 23/2006 on Population Administration is an effort to improve services by utilizing the development of information technology and still paying attention to the protection of population data.

8. Law Number 17 of 2023 concerning Health.

The development of information technology has encouraged services in the health sector, seeing that health services are currently integrated into health information systems. The health information system is a system that integrates all processing, reporting and use of information to improve health organization effectively and efficiently. Article 351 requires health information system organizers to ensure the protection of individual health data and information. Furthermore, in Paragraph 2, data processing must be done with the consent of the owner of the personal data. This provision aims to maintain the privacy rights of individuals.

9. Law Number 27 Year 2022 on Personal Data Protection (UU PDP).

UU PDP is a regulation that specifically regulates the protection of personal data. Previously, regulations regarding the guarantee of personal data protection were regulated partially and sectorally, so with the enactment of the PDP Law, there is a special regulation related to the protection of personal data. The PDP Law regulates the types of personal data, the rights of personal data subjects, the processing carried out by personal data controllers or processors as well as their obligations and most importantly, sanctions for perpetrators who violate the provisions in the PDP Law. According to the PDP Law, a personal data subject is a person to whom personal data is attached (Article 4 of the PDP Law). Personal data subjects have rights, one of which is as stipulated in Article 5, personal data subjects have the right to obtain information related to the clarity of identity, the basis of legal interests, the purpose of requesting and using personal data and the accountability of the party requesting personal data. Meanwhile, the obligations of the personal data controller must have a basis for processing personal data, then one of the obligations is also in Article 20 Paragraph (2) letter a, with the valid consent of the subject or owner of personal data. In the PDP Law, there are types of sanctions such as administrative sanctions and criminal sanctions. If you violate the provisions regarding the obligations of personal data managers, you will be subject to administrative sanctions (Article 57). Then there are prohibitions on the use of personal data which are regulated in Articles 65 and 66. The legal consequences

of violating the prohibition will be subject to imprisonment, fines and additional criminal sanctions (Articles 67 to 73 of the PDP Law). However, the administrative sanctions for private and government agencies stipulated in UU PDP have not been effectively implemented because the institution authorized to impose administrative sanctions on perpetrators of personal data theft has not been regulated in government regulations.

The Urgency of Personal Data Protection

The development of personal data protection law has been accommodated in the previously described laws. The laws and regulations described above have also considered all the increasingly massive developments in globalization and information technology. Basically, the law is dynamic, because of its dynamic nature, legal development must adjust to existing developments. It is no secret that the development of information technology provides great benefits to society. All aspects of life today have utilized information technology as a support to make all activities more effective and efficient. The obvious benefits of information technology such as in the fields of economy, education, government and in matters relating to the development of science (Lesmana et al., 2021). The use of digital-based technology in relation to trade, various applications or digital platforms such as shoppe, Tokopedia and others have emerged. Using these applications can help people who want to buy goods. Moreover, nowadays it has become a habit to do online shopping that connects sellers with buyers through electronic applications or platforms. The implications of the development of information technology have changed the traditional trading culture, because electronic-based trading does not prevent sellers and buyers from exchanging goods whenever and wherever they are (Siahaan, 2022). The role of information technology is also very convenient for the world of education. Conventional learning usually requires teachers and students to meet face-to-face in a classroom to carry out the teaching and learning process. However, the existence of information technology has changed this paradigm with the emergence of various channels or facilities that can be used in the electronic-based learning process (e-education) without having to meet physically (Husaini, 2017). The use of e-education is the only solution and a very practical method when the COVID virus hits the whole world because it must maintain distance (social distance). In addition to the benefits of technology in the fields of trade and education, information technology is also very useful for government in providing public services to the community (e-government). The Indonesian government has implemented electronic-based services, because it is considered to provide convenience in public services. Furthermore, according to Pudjiatno et al in the journal (Rachmatullah & Purwani, 2022) e-government is a means to improve government interaction with citizens.

After knowing the benefits of information technology in providing convenience in human activities. It should also be noted that the impact of the development of information technology can bring harm to society. As explained in the background of the problem related to electronic-based trading, users of electronic platforms in conducting transactions must agree to the terms and conditions of the platform that provides goods. These terms and conditions include submitting personal data to be managed by the personal data controller. The obligation of the personal data controller is to protect the personal data belonging to platform users, although the electronic system is decisive in controlling the integration of personal data with information technology (Ginancar & Lubis, 2022).

Problems that occur today often experience losses for owners of personal data. There are many causes of these losses, such as as a result of data leaks which are then utilized by irresponsible parties, data theft carried out by hackers who attack software systems so that there are very significant losses for personal data owners. According to the author, personal data leaks and breaches carried out by hackers occur for two reasons, namely that personal data managers are negligent in maintaining security and reducing the risk of leaking personal data

and weak software systems that need to be optimized. Another because that causes data leakage is due to human error, here the role of users such as awareness determines the security of personal data, then the weakness of the system makes it vulnerable to breaches and the use of malware and various cyber attacks by hackers (Hapsari & Pambayun, 2023). In fact, maintaining the security of personal data is the most crucial thing because it involves the right to privacy that has been determined by law.

Cases of personal data theft in Indonesia often occur, starting from the Tokopedia, Bukalapak and Bihneka applications and many others experiencing data leaks. About 91 million Tokopedia user data were sold to dark web sites (Samin, 2024). Other cases have also occurred due to the lack of attention of government agencies in maintaining personal data security, such as the case of hacking by hackers (Brain Chipher) against the national data center system. This case certainly poses a huge threat to state secrets, especially for the personal data of the Indonesian people.

Violations of personal data should be prevented and handled seriously because basically personal data is very important data related to everyone's privacy. Therefore, personal data should not be disseminated or misused, let alone causing harm to the owner of personal data. The protection of personal data is also one of the human rights, therefore it must be optimally protected. The protection of personal data can ultimately increase public trust in providing personal data to support government policies in fulfilling the interests of the community without being misused or violating people's personal rights.

Violations of personal data also require the strengthening of electronic systems and the ability of personal data managers to maintain data security by both private and government agencies. These efforts are a way to overcome the occurrence of leaks and theft of personal data. In addition, to realize legal certainty related to personal data protection, the provisions that have been regulated in various regulations governing personal data, especially in Law No. 27 of 2022 concerning Personal Data Protection, also need to be implemented in a real and optimal manner. The PDP Law is ultimately expected to make a major contribution to the creation of order and progress in society in relation to the use and utilization of information.

CONCLUSIONS

Laws and regulations on personal data protection continue to develop from time to time. The regulation began with the inclusion of Article 28 G Paragraph (1) in the 1945 Constitution which became the legal basis in guaranteeing the rights of every person or owner of personal data. Over time, the law on personal data protection is increasingly included in various legislative products, namely in Law Number 8 of 1997 concerning Company Documents, Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, Law Number 36 of 1999 concerning Telecommunications, Law Number 1 of 2008 concerning Information and Electronic Transactions which was last amended by Law. Law of the Republic of Indonesia No. 1 of 2024 on the Second Amendment to Law No. 1 of 2008 on Electronic Information and Transactions, Law No. 43 of 2009 on Archives, Law No. 24 of 2013 on the Amendment to Law No. 23 of 2006 on Population Administration, and in Law No. 17 of 2023 on Health.

In essence, these regulations want to create maximum protection for a person's personal data and can prevent the misuse of personal data that can cause harm to the owner of personal data. In 2022, the law on personal data protection developed even more rapidly with the enactment of Law Number 27 of 2022 on Personal Data Protection (UU PDP). UU PDP is a regulation that specifically regulates the protection of personal data. Previously, the regulation regarding the guarantee of personal data protection was regulated partially and sectorally, so with the enactment of the PDP Law, there is a special regulation related to personal data protection. The PDP Law regulates the types of personal data, the rights of personal data

subjects, the processing carried out by personal data controllers or processors as well as their obligations, and most importantly, the sanctions for perpetrators who violate the provisions in the PDP Law.

Personal data is important to protect because along with the development of technology and information, it is easier for violations to occur, including the misuse of personal data of each person. Violations of personal data should be prevented and handled seriously because basically personal data is very important data related to everyone's privacy. Therefore, personal data should not be disseminated or misused, let alone causing harm to the owner of personal data. The protection of personal data is also one of the human rights, therefore it must be optimally protected. Protection of personal data can ultimately increase public confidence to provide personal data to support government policies in fulfilling the interests of the community without being misused or violating people's personal rights. In addition, to realize legal certainty related to personal data protection, the provisions that have been regulated in various regulations governing personal data, especially in Law No. 27 of 2022 concerning Personal Data Protection, also need to be implemented in a real and optimal manner. The PDP Law is ultimately expected to make a major contribution to the creation of order and progress of society in relation to the use and utilization of information.

REFERENCES

- Ginanjari, D., & Lubis, A. F. (2022). Urgensi perlindungan data pribadi dalam menjamin keamanan data. *Jurnal Hukum Dan HAM Wara Sains*, 1(01), 21–26.
- Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen*, 5(1), 1–17.
- Husaini, M. (2017). Pemanfaatan teknologi informasi dalam bidang pendidikan (e-education). *MIKROTIK: Jurnal Manajemen Informatika*, 2(1).
- Kusnadi, S. A. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *AL WASATH Jurnal Ilmu Hukum*, 2(1), 9–16.
- Lesmana, C. S. A. T., Elis, E., & Hamimah, S. (2021). Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, 3(2), 1–6.
- Marzuki, A. A. (2021). Urgensi Perlindungan Data Pribadi Dalam Aktivitas Ad Tracking Di Ruang Siber. *Resam*, 7(2), 73–88.
- Meher, C., Sidi, R., & Risdawati, I. (2023). Penggunaan Data Kesehatan Pribadi Dalam Era Big Data: Tantangan Hukum dan Kebijakan di Indonesia. *Jurnal Ners*, 7(2), 864–870.
- Ngompat, Y. L. (2023). *KETIDAKSETARAAN SANKSI DALAM UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI*. Universitas Atma Jaya Yogyakarta.
- Priliyasi, E. (2019). Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online. *Majalah Hukum Nasional*, 49(2), 1–27.
- Rachmatullah, N., & Purwani, F. (2022). Analisis pentingnya digitalisasi & infrastruktur teknologi informasi dalam institusi pemerintahan: E-Government. *Jurnal Fasilkom*, 12(1), 14–19.
- Samin, H. H. (2024). Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif. *Jurnal Ilmiah Research Student*, 1(3), 1–15.
- Siahaan, A. L. S. (2022). Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi. *Majalah Hukum Nasional*, 52(2), 209–223.
- Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 9(2), 237.
- Windriani, N. P. W., Putri, P. I. D., & Wiraatmaja, I. P. P. (2023). Pendampingan Pengolahan

Data Pribadi Pelanggan Terkait Perlindungan Hukum pada Perumda Air Minum Tirta Sewakadarma Denpasar. *Jurnal Pengabdian UntukMu NegeRI*, 7(1), 17–23.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, 1(1), 147–154.