

Personal Data Protection Through Law Number 27 Of 2022: Challenges Of Cybercrime in The Era of Globalization and Digital

Setyo Utomo

doctorsetyojpu@gmail.com

STIH Sumpah Pemuda, Palembang, Indonesia

Article Info

Received: 2024-10-11

Revised: 2024-12-30

Accepted: 2024-12-31

Keywords:

Tax, Mining, Environment,
Legal Certainty

Abstract

This research was compiled based on the urgency of massive technological and information developments in Indonesia. Due to this development, it is also accompanied by negative impacts in the form of cybercrime targeting people's personal data. The implementation of the law must be in accordance with the reality of the development of the times. The formulation of the problem taken and discussed in this study is how the development of personal data protection through Law Number 27 of 2022 and how urgent Law Number 27 of 2022 is in meeting the demands of the community for personal data protection. The method used is normative juridical which uses primary data. The search for literature sources uses library studies. The results of this study are that the Government of the Republic of Indonesia through Law Number 27 of 2022 guarantees the right to privacy and personal data of citizens as one of the protections of human rights. Furthermore, this personal data protection law becomes a law that aligns Indonesian personal data protection regulations with international standards. Sanctions for violations of personal data protection provisions are also stated more firmly in this law.

I. Introduction

The development of information and communication technology has progressed rapidly throughout the world, including Indonesia.¹ The current era of globalization demands that people move quickly, precisely, and dynamically in order to face increasingly tight competition. The era of globalization accompanied by the acceleration of digitalization has made elements of information and communication technology enter every aspect of life. Information technology (as one of the impacts of digitalization) has become an integral part of society in various aspects of life such as education, government, security, trade, social, politics, and so on.

¹ Hari Mulyanto et al., "The Importance of Implementing Pancasila Values in Technological Development Among the Millennial Generation," Proceedings of the National Seminar on Law, Business, Science, and Technology 4, no. 1 (2024): 637.

Indonesia is one of the countries that is involved in the flow of digital globalization. This is an effort to realize Indonesia as a developed and prosperous country. The development of technology from globalization has many impacts, both positive and negative. Positive impacts such as making daily work easier and increasing daily productivity are added value for humans who are competing in the era of the Industrial Revolution 4.0. However, these positive impacts are also accompanied by other negative impacts, namely cybercrime.

Cybercrime or also called cybercrime is one form of modern crime (digitalization era) caused by the rapid development of information technology. This crime is a dark side of the progress of information technology in the world, therefore there are many large-scale losses. In a narrow sense, cybercrime is an unlawful act using internet media based on sophisticated information technology².

Cybercrime or cybercrime in the digital era targets many aspects. However, the most common target targeted by cybercrime perpetrators is data. The data here concerns personal data, organizational or institutional data, and other important data. Data is defined as information that is processed through infrastructure that has an automatic function to respond to commands given with its purpose and is stored so that it can be processed³.

Data is an important thing and is used according to its needs in accordance with the owner's consent. Nowadays, data misuse crimes or cybercrimes have reached an alarming level. Even Indonesia has the highest number of cybercrime cases in the world, third after Ukraine. Recent data leaks due to cybercrime include Tokopedia data leaks, BPJS data, BRI Life data, Bank Jatim user data, KPAI data, POLRI database, Indihome customer data, PLN user data, and several other cases⁴.

Information technology crime cases are an important issue in the corridor of Indonesian legal regulation. Do not let it happen that when a criminal act of information technology crime occurs, the law that regulates it does not exist. This will create a *rechtsvacuum* and legal chaos can occur. In addition, personal data is one of the human rights that need to be protected. Thus, laws related to the protection of personal data and anticipation related to cybercrime must be drafted properly.

² Raodia, "The Influence of Technological Developments on Cybercrime," *Jurisprudentie* 6, no. 2 (2019): 235, <https://doi.org/https://doi.org/10.24252/jurisprudentie.v6i2.11399>.

³ Data Protection Act, UK, 2018

⁴ Jeane Neltje Saly et al., "Analysis of Personal Data Protection Related to Law No. 27 of 2022," *Jurnal Serina Humaniora* 1, no. 3 (2023): 148.

The government has gradually begun to pay attention to the importance of legal regulations governing the protection of personal data. This can be seen through the efforts of the Indonesian Government in drafting and ratifying Law Number 27 of 2022. The government is gradually starting to pay attention to the importance of regulations governing the protection of personal data, as reflected in their efforts to draft and ratify Law Number 27 of 2022 concerning Personal Data Protection.⁵ The legislation that was ratified on October 17, 2022 aims to protect the personal data of the community managed by PSE (electronic system organizers). The next goal is to prevent misuse by irresponsible individuals/individuals⁶.

In relation to the protection of personal data from cybercrime, there is a need for the development of competent human resources and qualified skills in the field of cybersecurity. The state needs to facilitate this realization by strengthening human resources who understand cyber and improving state security production facilities. This can be done by involving adequate training and education for cybersecurity experts and improving technological infrastructure that can identify, protect, and respond to cyber attacks effectively and quickly.⁷

Based on the description that has been presented, there is an urgency of implementing Law Number 27 of 2022 effectively and comprehensively. Moreover, the relationship between personal data protection is the protection of human rights which is also protected by law. The problems that will be discussed in this study are how the development of personal data protection through Law Number 27 of 2022 and how urgent Law Number 27 of 2022 is in meeting the demands of the community for personal data protection.

This study was compiled for the purpose of providing an explanation of the development of personal data protection through the legal standing of Law Number 27 of 2022. Furthermore, this study is to determine the urgency of the personal protection law as a response to the challenges of digital globalization, whether it can answer the demands of society regarding personal data protection and cybercrime.

⁵ Albert Lodewyk Sentosa Siahaan, "The Urgency of Personal Data Protection on the Marketplace Platform Against Technological Progress," *National Law Magazine* 52, no. 2 (2022): 210–22, <https://doi.org/https://doi.org/10.33331>.

⁶ Dirgantara Muhammad, "Legal Responsibility of PT Tokopedia for Personal Data Leaks" (State Islamic Institute of Palopo, 2023).Page 56

⁷ Ineu Rahmawati, "The Analysis of Cyber Crime Threat Risk Management to Increase Cyber Defense," *Journal of Defense & National Defense* 7, no. 2 (2017): 51–66.

2. Research Method

This research in the form of a scientific article was compiled using library research techniques with a normative legal method approach. The normative legal method is considered appropriate to answer the legal issues faced through the process of discovering legal rules, legal principles, and legal doctrines⁸. The normative legal method is also called doctrinal legal research which conceptualizes law as law in book.⁹ The legal basis for this research, the researcher uses Law Number 27 of 2022 concerning Personal Data Protection as relevant legal material. Other literature sources as primary data are also used as additional compilers of this research.

3. Results and Discussion

Development of Personal Data Protection Through Law Number 27 of 2022

Personal data protection is important because it is related to the protection of fundamental human rights. As a result of the development of information technology (IT) and the increasing potential of Indonesia's digital economy, there are various negative impacts in the form of threats to the privacy rights and personal data of citizens.¹⁰ The threat certainly makes citizens uncomfortable in carrying out daily activities on social media. In addition, the public will also always be afraid if personal data that has been given to the state or private sector is leaked and can harm themselves in the future.

Protection of personal data has been internationally recognized as a human right. Protection of personal data is one of the intersections of the right to information and the right to privacy in The Universal Declaration of Human Rights in 1948.¹¹ Specifically, the protection of individual privacy rights is regulated in Article 12 of the UDHR, namely "No one shall be subjected to arbitrary interference with his privacy, family, or correspondence, nor to attack upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".

Indonesia in its constitution, guarantees and recognizes the right to personal protection. As stated in Article 28 letter G which emphasizes that the government guarantees, protects personal rights and is obliged to provide a sense of security to its citizens for their actions in accordance with human rights.

⁸ Peter Mahmud Marzuki, *Legal Research: Revised Edition* (Jakarta: Kencana, 2005).Page 47

⁹ Jonaedi Efendi and Johnny Ibrahim, *Normative and Empirical Legal Research Methods*, First Edition (Jakarta: Kencana, 2016).Page 124

¹⁰ Ananthia Ayu D, Titis Anindyajati, and Abdul Ghoffar, "Protection of Privacy Rights to Personal Data in the Digital Economy Era" (Jakarta, 2019).Page 6.

¹¹ Elfian Fauzi and Nabila Alif Radika Shandy, "The Right to Privacy and the Legal Politics of Law Number 27 of 2022 Concerning Personal Data Protection," *Lex Renaissance Journal* 7, no. 3 (2022): 453, <https://doi.org/10.20885/jlr.vol7.iss3.art1>.

From this article, it is very clear that the government is obliged to participate in the problem of protecting personal data from cybercrime attacks. Therefore, Law Number 27 of 2022 concerning Personal Data Protection was born.

Law Number 27 of 2022 has the main objective of protecting individual personal data and regulating the collection, use, storage, security and deletion of personal data by parties authorized to manage it.¹² This law consists of 16 chapters with 76 articles with the main content providing regulations regarding personal data in the scope of types, rights, data processing, obligations of personal data controllers and processors, transfer of personal data, administrative sanctions, criminal provisions, and prohibitions on the use of personal data. Furthermore, the PDP Law also regulates the institutional role of the implementation of personal data protection, international cooperation, community participation, and dispute resolution along with procedural law if there are legal problems from personal data protection.

In terms of implementation, if there is a case of personal data leaking, the PDP Law will apply the normative implementation aspects. These aspects include the obligations of the data manager, notification obligations, data transfer regulations, and sanctions and responsibilities. This is implemented in accordance with applicable legal principles and aims to create order for the wider community.

The obligation of the data manager in the PDP Law is to instruct the data manager to be able to create data protection measures. Both protection in the form of technical measures and organizational standards that are considered adequate to protect personal data. This protection is intended to be able to defend or resist unauthorized attempts to access, use or manage data.

When a data leak occurs that has been detected and verified correctly, the person in charge of the data is required to provide notification to the affected parties. The notification is intended primarily for the parties whose data has been leaked. This is useful so that the parties whose data has been leaked can take anticipatory steps from changing passwords or other steps. This anticipation is intended so that other data is not leaked or misused by irresponsible parties.

Personal data protection regulations also regulate data transfers. The PDP Act can instruct (in a mandatory connotation) to ensure that data transfers between countries are carried out securely. The person in charge of the data must ensure that the destination country of the data transfer has good cybersecurity before transmitting data there. The person in charge of the data must use a

¹² Saly et al., "Analysis of Personal Data Protection Related to Law No. 27 of 2022."Page 147

security mechanism so that when transferring data, the personal data transmitted remains secure.

The provisions of sanctions and responsibilities are also regulated in the PDP Law. Data custodians who are proven to have violated the law will be subject to significant sanctions in the form of fines and/or lawsuits in accordance with applicable regulations. Victims of misuse or negligence in safeguarding personal data governance can sue for compensation for financial losses and reputation restoration. These demands are the rights of victims due to losses from misuse of personal data which are included in the right to compensation which is the responsibility of the data custodian.

The legal classification of personal data consists of two, namely specific and general personal data. Specific personal data is all personal data belonging to an individual which includes health information data, biometric data, genetic data, criminal records, child data, personal financial data, and/or other data in accordance with statutory provisions.¹³ In addition, general personal data includes individual data regarding full name, gender, nationality, religion, marital status, and personal data combined to identify a person.¹⁴

The Indonesian government through the PDP Law stipulates sanctions for violations of personal data protection rules through administrative sanctions and criminal sanctions. In Article 57, provisions on administrative sanctions are imposed on violations of the articles as referred to in paragraph (1). Administrative sanctions can be in the form of written warnings, temporary suspension of personal data processing activities, deletion or destruction of personal data, and/or administrative fines.

The provisions of criminal sanctions as referred to in the PDP Law Article 67 to Article 73 by imposing criminal sanctions of imprisonment and/or fines. The imposition of criminal sanctions is carried out in accordance with the provisions of the violations listed in the criminal provisions of the PDP Law. Corporations are also still subject to criminal sanctions, but only in the form of criminal fines. The criminal fines imposed on corporations can be imposed at most ten times the maximum fine threatened in the Law¹⁵.

The Urgency of Law Number 27 of 2022 in Meeting Public Demands for Personal Data Protection

¹³PDP Law Article 4 paragraph (2)

¹⁴PDP Law Article 4 paragraph (3)

¹⁵ Rina Rahma Ornella Angelia, Rahmi Erwin, and Andi Desmon, "Sanctions Against Corporations as Electronic System Organizers Due to Leaks and Misuse of Personal Data," *Ensklopedia of Journals* 6, no. 2 (2024): 362, <https://doi.org/https://doi.org/10.33559/eoj.v6i2.2226>.

The rampant cases of personal data leaks that have occurred have made the public restless about the protection of their personal data. With the PDP Law, the government can provide a sense of security and legal certainty for the protection of personal data. In addition to carrying out its responsibilities, the Indonesian Government through the PDP Law has provided comprehensive digital regulatory needs. This can provide trust and also increase the digital economy.

The presence of the PDP Law can answer the issue of harmonizing international regulations on data protection with national regulations. The international world certainly has its own standards in protecting personal data. The PDP Law allows Indonesia to align international personal data protection principles and standards, such as the General Data Protection Regulation (GDPR) in the European Union. This has implications for increasing global trust in Indonesia regarding the security of the data provided.

Elements of society are also involved in the PDP Law. With the presence of the PDP Law, the community can participate in controlling data leaks in cyberspace. In addition, through the PDP Law, the community can also be given clear rights to the authority to know, access, change, or delete their data. Increased knowledge and awareness of personal data protection by the community can also occur and anticipation of sustainability risks can also be applied from the implementation of this PDP Law.

The determination of administrative sanctions and criminal penalties becomes clearer. The PDP Law explicitly regulates administrative and criminal sanctions that can be imposed on individuals and corporations. The imposition of sanctions can also be applied appropriately, because there are special rules regarding personal data that have been implemented. Criminalization is carried out so that there is a deterrent effect and a precautionary effect on organizers and those responsible for personal data in implementing its governance.

The Personal Data Protection Law, which is a mandate regulation of Article 28G of the 1945 Constitution of the Republic of Indonesia, is expected to create security and peace in society. For corporations, the Personal Data Protection Law can be used as a reference regulation to increase the security of personal data management, both data owned or collected from the public. Thus, the urgency of the Personal Data Protection Law is said to be very important in order to create a protected society and increase global trust in Indonesia. This global trust in the future will have implications for investment and digital businesses that will or are currently running in Indonesia.

4. Conclusion

The development of personal data protection in Indonesia is heading towards a better direction. Due to various existing urgencies, the Indonesian Government issued Law Number 27 of 2022 to implement personal data protection through normative provisions. This regulation is considered a balancing rule for the progress of the times and the rampant cybercrime targeting personal data. This law is the answer to public concerns about the security of their personal data amidst the rapid development of the digital era of globalization.

Law Number 27 of 2022 concerning Personal Data Protection explicitly regulates the protection and strict sanctions of those responsible for data. This PDP Law has great urgency for aligning Indonesian regulations with other international laws relating to the protection of privacy and personal data. The provisions of this personal data protection law also strengthen the protection of human rights in Indonesia.

Acknowledgments

This research is supported by the STIHPADA Palembang, and the Institute for Research and Community Empowerment as well as the parties who have supported this research. All of research material, data verification and research activity belong to author.

References

- Angelia, Rina Rahma Ornella, Rahmi Erwin, and Andi Desmon. "Sanctions Against Corporations as Electronic System Organizers Due to Leakage and Misuse of Personal Data." *Ensklopedia of Journal* 6, no. 2 (2024): 362. <https://doi.org/https://doi.org/10.33559/eoj.v6i2.2226>.
- D, Ananthia Ayu, Titis Anindyajati, and Abdul Ghoffar. "Protection of Privacy Rights to Personal Data in the Digital Economy Era." Jakarta, 2019.
- Efendi, Jonaedi, and Johnny Ibrahim. *Normative and Empirical Legal Research Methods*. Edition I. Jakarta: Kencana, 2016.
- Fauzi, Elfian, and Nabila Alif Radika Shandy. "The Right to Privacy and Legal Politics of Law Number 27 of 2022 Concerning Personal Data Protection." *Lex Renaissance Journal* 7, no. 3 (2022): 453. <https://doi.org/10.20885/jlr.vol7.iss3.art1>.
- Marzuki, Peter Mahmud. *Legal Research: Revised Edition*. Jakarta: Kencana, 2005.
- Muhammad, Dirgantara. "Legal Responsibility of PT Tokopedia for Personal Data Leaks." *State Islamic Institute of Palopo*, 2023.
- Mulyanto, Hari, Mayda Nur Rohmani, Muh Alvian Bagus Prasetya, and Aris Prio Agus Santoso. "The Importance of Implementing Pancasila Values in the Development of Technology Among the Millennial Generation." *Proceedings*

of the National Seminar on Law, Business, Science, and Technology 4, no. 1 (2024): 637.

Rahmawati, Ineu. "The Analysis of Cyber Crime Threat Risk Management to Increase Cyber Defense." *Journal of Defense & National Defense* 7, no. 2 (2017): 51–66.

Raodia. "The Influence of Technological Developments on Cybercrime." *Jurisprudentie* 6, no. 2 (2019): 235. <https://doi.org/https://doi.org/10.24252/jurisprudentie.v6i2.11399>.

Saly, Jeane Neltje, Halena Artamevia, Kendelif Kheista, Barnabas Juni, Saputra Gulo, Evellyn Abigael Rhemrev, and Michelle Christie. "Analysis of Personal Data Protection Related to Law No. 27 of 2022." *Serina Humaniora Journal* 1, no. 3 (2023): 148.

Siahaan, Albert Lodewyk Sentosa. "The Urgency of Personal Data Protection on the Marjetplace Platform Against Technological Advances." *National Law Magazine* 52, no. 2 (2022): 210–22. <https://doi.org/https://doi.org/10.33331>.

Legislation

Law Number 27 of 2022 concerning Personal Data Protection (State Gazette of the Republic of Indonesia 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6820)

Data Protection Act, 2018, United Kingdom.