FR-FH-18.Rev.1

SURAT TUGAS

Nomor: 1189-D/1409/FH-UNTAR/X/2024

Pimpinan Fakultas Hukum Universitas Tarumanagara dengan ini menugaskan kepada:

Prof. Dr. Gunardi Lie, S.H., M.H.

Telah menjadi Penulis Jurnal dengan judul "*Personal Data Protection Law In Indonesi W In Indonesia: Challenges And Opportunities*".

Setelah 1 (satu minggu) acara dilaksanakan segera melaporkan kegiatan beserta dengan lampirannya.

Apabila tidak dilaporkan, maka penugasan kegiatan selanjutnya akan ditunda.

Demikian surat tugas ini diterbitkan untuk dilaksanakan dengan baik.

Jakarta, 29 Oktober 2024

Dekan

UNIVERSITAS TARUMANAGARA
DEKAN
FAKULTAS HUKUM

Prof. Dr. Amad Sudiro, S.H., M.H., M.Kn., M.M.

Tembusan:
1. Kaprodi dan Sekprodi Pascasarjana Doktor FH
2. Kabag. Tata Usaha FH
3. Bagian Personalia FH

Ca.

Indonesia Law Review

Volume 14 | Number 2 Article 4

8-31-2024

PERSONAL DATA PROTECTION LAW IN INDONESIA: CHALLENGES AND OPPORTUNITIES

Moody Rizqy Syailendra
Universitas Tarumanegara, moodys@fh.untar.ac.id

Gunardi Lie
gunardi.lie@fh.untar.ac.id

Ahmad Sudiro
ahmads@fh.untar.ac.id

¸Indonesia Law Review (2024) 4: 56 - 72
ISSN: 2088-8430 | e-ISSN: 2356-2129

PERSONAL DATA PROTECTION LAW IN INDONESIA: CHALLENGES AND OPPORTUNITIES

Moody Rizqy Syailendra*, Gunardi Lie **, Amad Sudiro***

*,**,*** Faculty of Law, Universitas Tarumanagara, Indonesia

Article Info

Received : 1 February 2024 | Received in revised form : 15 April 2024 | Accepted : 10 July 2024
Corresponding author's e mail : moodys@fh.untar.ac.id

Abstract

This research identifies challenges, obstacles and opportunities related to the issuance of Law No. 27 of 2022. Protection of personal data is crucial, especially in the use of information and communication technology in the current modern era. The contents of this article were analyzed using qualitative methods and secondary data in analyzing it. The research results show that: although the PDP Law was only implemented in 2022, regulations regarding PDP can actually be found in various pre-existing regulations, then there are principles and provisions that can be included in the PDP Law to better accommodate the need for protecting people's personal data, Furthermore, there are various challenges, obstacles and protections in implementing the PDP Law. The conclusion is that the passing of Law Number 27 of 2022 concerning Personal Data Protection in Indonesia marks a significant step in strengthening personal data protection for Indonesian citizens. However, implementing this law presents various challenges that the government must overcome.

Keywords*: Personal Data Protection, Challenges, Obstacles, Potential*

Abstrak

Penelitian ini mengindentifikasikan tantangan, hambatan dan kesempatan terkait diterbitkannya Undang-Undang Noor 27 Tahun 2022. Perlindungan data pribadi menjadi hal yang krusial, utamanya dalam pemanfaatan teknologi informasi dan koomunikasi di era modern saat ini. Isi artikel ini dianalisis dengan menggunakan metode kualitatif dan data sekunder dalam menganalisisnya. Hasil penelitian menunjukkan bahwa: walaupun UU PDP baru diberlakukan pada 2022 lalu, namun pengaturan mengenai PDP sebetulnya dapat ditemukan pada berbagai aturan yang sudah ada sebelumnya, selanjutnya terdapat asas dan ketentuan yang dapat dimuat di dalam UU PDP agar semakin mengakomodasi kebutuhan perlindungan data pribadi masyarakat, selanjutnya terdapat berbagai tantangan, hambatan, dan protensi dalam pemberlakuan UU PDP. Kesimpulan didapatkan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia menandai langkah signifikan dalam memperkuat perlindungan data pribadi bagi warga negara Indonesia. Namun penerapan undang-undang ini menghadirkan berbagai tantangan yang harus diatasi oleh pemerintah.

Keywords*: Perlindungan Data Pribadi, Tantangan, Hambatan, Potensi*

DOI : https://doi.org/10.15742/ilrev.v14n2.1

I. INTRODUCTION

Currently, the development of information technology is increasingly rapid and is much different from its initial existence. Information technology has changed the pattern of life in society globally, as well as causing rapid and significant changes in social, cultural, economic and legal frameworks.[1] Information and Communication Technology (ICT) can fundamentally change, reorganize and restructure working methods, and ultimately the sector itself.[2] ICT has provided many facilities that can be enjoyed by all users throughout the world which makes it easy for people to get access to various kinds of data, including other people's privacy data.[3] One example of the use of ICT in everyday life is the use of Big Data. Big data, is a general term for all data sets in very large, complex and unstructured amounts, making them difficult to handle if only using traditional data processing applications or systems.[4]

Big data is now familiar to software developers with large-scale projects.[5] Many data processing institutions require very large data capacities to store and process data. One example of the use of big data in everyday life is the recording of E-KTP, electronic driving licenses, Public Heatlh Service Provider (BPJS, JKN, etc) and the use of public application such as *pedulilindungan*, *e-Hac*, etc. The use of big data provides various assistance and benefits in various areas of daily life.

However, behind the convenience provided, there are also shortcomings regarding to an information system. Where the system can be exploited, so that it can bring disadvantage to society. This causes personal data held by service users to be accessed by people who are able to do so, unlawfully. So violations of privacy are very likely to occur. The most frequent personal data breaches that occur in Indonesia are the sale of personal data by data storage parties. The data that has been sold is then used to offer products, such as insurance or bank loans, by telemarketers. Apart from that, the problem that has become a topic of discussion is the leaking of personal data of eHac application users. Around 1.3 million eHac application user data was hacked and distributed unlawfully. The personal data that was allegedly leaked included names, addresses, telephone numbers, photos and the results of COVID-19 test users of the application. Moreover, the allegedly leaked database also contains personal information such as the names of parents or relatives of application users, including hotel details, travel destinations, and information about when the eHac account was created.[6] Another problem that is currently of particular concern is the leak of Covid-19 patient data which was revealed via the dark web site RaidForums.[7] Based

[1] Endang Sumardi, "The development of communication technology has changed every aspect of people's daily lives", available at https://portal.sukabumikota.go.id/4112/perkembangan-teknologi-komunikasi-telah-mengubah-setiap-aspek-kehidupan-masyarakat-sehari-hari

[2] *United Nations Conference on Trade and Development:* "Information and Communication Technology Development Indices", *ICT Development Indices*, New York and Geneva, 2003. p. 2

[3] Sinta Dewi, "*Cyber Law: Aspects of Data Privacy According to International, Regional and National Law*", Bandung: Refika Aditama, 2015, p.4.

[4] Narendra,, Albertus Pramukti. (2015), "Big Data, Data Analysis, and Librarian Competency Development", *Record and Library Journal*: Vol. 1: No. 2.

[5] Bagus Sudirman, "Get to know the meaning and function of BIG DATA", available at http://teknik-informatika-s1.stekom.ac.id/informasi/baca/Mengenal-Pengertian-Dan-Fungsi-BIG-DATA/bda947d7ccc3524999a0fabe36b3783a24bd510b

[6] Noam Rotem and Ran Locar, "Indonesian Government's Covid-19 App Accidentally Exposes Over 1 Million People in Massive Data Leak", available at https://regional.kontan.co.id/news/psbb-jakarta-berlaku-hari-ini-ingat-kembali-protokol-kesehatan-dan-sanksinya?page=all

[7] Alza Ahdira: "Hundreds of Thousands Covid-19 Patients Data Allegedly Leaked, sold by Hackers on Dark

on these problems, data privacy has become an issue that is discussed globally and is receiving more attention.

In order to overcome problems related to security in the implementation of ICT systems, a legal approach is absolute because without legal certainty, problems related to the use of ICT will not be optimal.[8] In this case, the state should be present to protect the personal data of its citizens. Based on welfare state theory, the state is obliged to be present and involved in meeting the economic and social welfare of its citizens.[9] This concept requires the state to be responsible for the welfare of its citizens by intervening in making rules and policies and being responsible in various areas of life related to the welfare of society. Personal data protection plays a central role in ensuring the well-being of citizens in this digital era. By preventing misuse of personal information, it can be ensured that individuals have control over their own privacy, reducing the risk of identity theft and financial fraud that can be financially detrimental. More than just protecting information, data security also helps maintain emotional security, reducing stress and worry arising from potential misuse of personal data. Additionally, by increasing consumer confidence in the digital economy, data protection supports sustainable economic growth. Furthermore, by providing individuals with a sense of security regarding their use of the internet and technology, data protection also encourages greater participation in online life, supporting freedom of speech and opinion which is one of the pillars of the prosperity of modern society. Thus, personal data protection is an important aspect in ensuring holistic well-being and individual freedom in today's digital society.

Personal data protection is closely related to the principle of the rule of law which demands justice, legal certainty and protection of individual rights. Within the framework of the Rule of Law, the state has the responsibility to create laws that are fair, transparent and accessible to all citizens, including regarding the protection of personal data. This ensures that individuals' privacy rights are recognized and appropriately protected. Additionally, the principle of the rule of law mandates that no entity, including governments, is exempt from the obligation to comply with data protection laws. By consistently enforcing the law and imposing sanctions on violators, the state ensures that all parties, both public and private, are subject to the same laws. This creates legal certainty and provides guarantees that individual rights, including the right to privacy and data security, are respected and protected in accordance with the principles of the Rule of Law.

In this regard, Indonesia itself has regulations that can serve as a legal umbrella for the protection of personal data through Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), which was only implemented some time ago. The enactment of the PDP Law marks a new era in terms of personal data protection in Indonesia, this is because there are no regulations at the level of law that specifically regulate the protection of personal data in Indonesia. The PDP Law is the first law that specifically regulates personal data protection in Indonesia and is expected to accommodate all the needs of the Indonesian people regarding personal data protection. Shinta Dewi Rosadi, a personal data protection expert from Padjadjaran University, believes that

Web Sites", available at https://www.pikiran-rakyat.com/nasional/pr-01572317/data-ratusan-ribu-pasien-covid-19-diduga-bocor-dijual-peretas-di-situs-dark-web.

[8] Indonesian Law Number 11 of 2008 concerning Electronic Information and Transactions, General Explanation.

[9] Welfare State on Britannica Online Encyclopedia, available at https://www.britannica.com/money/topic/welfare-state

Indonesia should have had a Personal Data Protection Law some time ago.[10] The recent enactment of this law is an irony, because Indonesia is one of the countries with the largest online trade and a mobile phone population of 360 million or more than the population. With the existence of laws and regulations that specifically regulate Personal Data Protection, the government can regulate various things such as how long personal data storage service providers can store someone's personal data. Even though there is a special law on personal data protection (UU PDP), there is concern about protection for privacy and protection of personal data because the PDP Law is not considered to be the final solution to the problem of personal data protection and data leakage. Currently, Indonesia has a law that regulates personal data protection (UU PDP). However, the PDP Law itself is considered to still not be the final solution in overcoming various problems related to personal data protection, for example regarding institutions authorized to supervise data protection, then the existence of unequal sanctions between the public and private sectors who commit violations and various other problems.

Based on the background that has been presented, this research was conducted to find out about the legal politics of personal data protection in Indonesia. Then, this research aims to convey things that can be used as input in improving the PDP Law. Finally, this research will reveal the challenges, obstacles and opportunities faced in implementing the PDP Law.

The research problems of this paper are:

1. Legal Politics of Personal Data Protection in Indonesia;
2. Things that can be regulated in order to improve the Personal Data Protection Law;
3. Challenges in Enforcing Personal Data Protection Laws in Indonesia

II. DISCUSSION

A. The Concept of Privacy and Personal Data Protection.

In the development of human rights, new types of human rights emerge. One of them is the right to privacy. In 1890, Warren and Brandheis, in their article in the Harvard Law Review entitled "The Right to Privacy"[11], introduced the concept of the right to be left alone. This concept emerged as a result of human spiritual needs, namely the need to have feelings, thoughts and the right to enjoy life respected. Warren and Brandheis said:

> ***"Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition".***

The right to privacy means that everyone has the right to live and not be disturbed in their private life, whether by other people or even the state. Therefore, the state has the responsibility and obligation to regulate and recognize these rights. There are reasons why these rights must be protected. The first reason is, in everyday interactions, a person has the right to close his personal life so that he can protect himself in certain circumstances. The second reason is, in living one's life, sometimes a person needs time to be alone (solitude), without interference or interaction from

[10] Indotelko: There are no personal data regulations, Indonesia loses IDR 500 billion, available at http://www.indotelko.com/kanal?c=id&it=data-pribadi-indonesia-rugi-500-miliar

[11] Warren, Brandheis, (1890), "The Right to Privacy", Harvard Law Review, Massachusetts, p.5.

other humans, for this privacy is needed.

The right to privacy means that everyone has the right to live and not be disturbed in their private life, whether by other people or even the state. Therefore, the state has the responsibility and obligation to regulate and recognize these rights. There are reasons why these rights must be protected. The first reason is, in everyday interactions, a person has the right to close his personal life so that he can protect himself in certain circumstances. The second reason is, in living one's life, sometimes a person needs time to be alone (solitude), without interference or interaction from other humans, for this privacy is needed. The third reason is that privacy is a right that stands alone and does not depend on anything else. So, a person will lose the right to privacy if he himself conveys things of a personal nature to the public or to the public. The fourth reason is that privacy is also a person's right to have domestic relationships, including how he builds marital relationships and builds his family. This is of course not a public assumption and other people should not know these things, this right is identified by Warren as the right against the world. The final reason is, if this right is violated, it will be difficult to assess and show the location of the losses experienced by someone. This is because if someone's personal life is disturbed, of course the victim can sue the perpetrator for compensation as a result of the losses they suffered. Of course, the losses experienced will be difficult to estimate, because the form of loss experienced is an immaterial loss.[12] Privacy is a concept that is very difficult to define, this is because each person has different boundaries depending on each person's perspective.[13] Privacy as a right inherent in humans can be divided into several types, namely privacy of information, physical privacy, privacy to determine one's identity, and privacy of property. The state, through the government, is responsible for protecting itself from all efforts or actions aimed at violating these rights. Information considered private can come in many forms and vary depending on the purposes for which they are used. Simson Garfinkel divides it into five or five categories, namely personal information, private information, personality identifiable information, anonymized information, and aggregate information.[14]

Regarding to the Protection of Personal Data, Data is raw material for information, defined as an orderly group of symbols that represent quantities, actions, objects, and so on. Data is formed from characters which can be alphabets, numbers or special symbols. Data is compiled and then processed into data structures, file structures and databases.[15] Based on the legal concept of telematics, data is a formal representation of a concept, fact, or instruction.[16] According to Gordon B. Davis, data is a raw material for producing information.[17] Meanwhile, personal data according to Article 1 paragraph (1) of the UK Data Protection Act is data relating to a living individual and can be identified from the data or from data or information that is owned or will be owned by the data controller. The term data protection was first used in Germany and

[12] Shinta Dewi, (2017) "Principles of Protection of Personal Data of Credit Card Customers According to National Regulations and Their Implementation", *Jurnal Sosiohumaniora*. Vol.19, No.3, p.208 - 209.

[13] Shinta Dewi, *"Privacy Protection of Personal Information in E-Commerce According to International Law"*, Bandung. p.53.

[14] Garfinkel, Simson. "Database Nation: The Death of Privacy in the 21st Century". Massachusets: O'Reilly, 2000. p.100.

[15] Purwanto, (2007) *Research on Legal Protection of Digital Data.* Jakarta: Badan Pembinaan Hukum Nasional, p.13.

[16] Pendit, et.al, *The Meaning of Information: Continuation of a Debate*. Jakarta: Kesaint-Blanc. 1992. p20.

[17] Davis, Gordon B. "Management information System", Jakarta: PT. Pustaka Binaman Pressindo, 1984. p12.

Sweden in the 1970s where this matter was regulated in law.[18] The implementation of this data protection law was motivated by the start of the use of computers as a tool for storing population data, especially for population census purposes, where in reality there were many violations committed by both the government and the private sector. Thus, this law has a role as a legal umbrella if there is misuse of personal data owned by an individual.

Based on this, many other countries have started to follow and enforce similar regulations in their countries. However, each country uses different terms regarding personal information and personal data. However, in substance the two terms have almost the same meaning. [19] Countries such as the United States, Canada and Australia use the term personal information, while countries in the European Union use the term personal data. Personal data consists of facts, communications or opinions relating to the individual. So it can be said that personal data is very personal and sensitive information so that the individual concerned wants to store or restrict other people from collecting, using or distributing it to other parties. Jerry Kang said that personal data describes information that is closely related to a person which will distinguish the characteristics of each individual.[20] So basically, the form of data protection is divided into two categories, namely data protection in the form of securing physical data, both visible and invisible data. Another form is the existence of regulations that regulate the use of data by other people who are not entitled to it, misuse of data for certain interests, and destruction of the data itself.

B. The Legal Politics of Personal Data Protection in Indonesia .

Indonesia is a country based on law (Article 1 Paragraph (3) of the 1945 Constitution), meaning that all aspects of life in society, state and government must always be based on law. To realize a rule of law, one of the things that is needed is legal instruments that are used to regulate balance and justice in all areas of people's lives and livelihoods through statutory regulations. This shows that legislation has an important role in the Indonesian legal state. Legislative Regulations are written regulations that contain generally binding legal norms and are formed or stipulated by state institutions or authorized officials through procedures stipulated in Legislative Regulations.[21] Mochtar Kusumaatmadja in the Theory of Development Law says that, "the role of law in development is to ensure that change occurs in an orderly manner. The law plays a role through the help of legislation and court decisions, or a combination of both".[22] The state as the "driver" of government has an obligation to accommodate and protect the needs of its citizens. This can be done through the process of establishing statutory regulations. As a country with a legal system that is heavily influenced by the Civil Law legal system, written law is used as the most important source of law. Thus, written law is very much needed as a guarantor of legal certainty.

Along the way, regulations regarding the protection of personal data have actually been briefly regulated in various existing laws. For example, these regulations are

[18] *Op Cit, Shinta Dewi, "Privacy Protection of Personal Information in E-Commerce According to International Law"*. p.37.
[19] *Ibid.*

[20] Jerry Kang, (1998) "Information Privacy in Cyberspace Transaction", *Stanford Law ReviewVol 50*, Apr. p.5.
[21] Article 1 paragraph (2) Law no. 12 of 2011 concerning the Formation of Legislative Regulations.
[22] Kusumaatmadja, Mochtar. "Legal Development in the Context of National Development", Bandung: Bina Cipta, 1975, p.4.

contained in Law no. 43 of 2009 concerning Archives. This Basic Archives Law regulates that archival institutions and archive creators can close access to archives on the grounds that if the archive is opened to the public, one of the reasons is that it could reveal secrets or personal data. From here we can see that one of the principles of personal data protection, namely use for limited, has been implemented, where archival institutions and archive creators can close access to personal data.

Another example of regulation regarding personal data is also contained in Law no. 8 of 1997 concerning Company Documents. This law regulates aspects of data protection within the company scope. This law also classifies company documents as data. Apart from that, this law also regulates the retention and destruction of documents. The retention and destruction schedule must be determined by the data custodian and approved by the management concerned. This is also a reflection of the implementation of the principle of personal data protection, namely kept no longer than is absolutely necessary. This principle regulates the time period for which data needs to be stored and destroyed. If the data has been used according to its intended purpose, the data must be immediately destroyed.

The next rule regulates the protection of personal data in the Banking Law, which relates to bank secrets. In Article 40 of this Law, it is regulated that banks are obliged to keep confidential information regarding depositors and their deposits, except in the cases referred to in Article 41, Article 41A, Article 42, Article 43, Article 44 and Article 44A. These articles provide exceptions for matters such as: tax purposes, for settlement of bank receivables, for judicial purposes in criminal cases, as well as at the request, consent or power of attorney from deposit customers, where the bank can violate the provisions regarding bank secrecy, of course by certain procedures.[23]

Regulations regarding personal data protection are further mentioned in Law no. 36 of 1999 concerning Telecommunications. In this law, personal data protection is not explicitly regulated, this law prioritizes access to data. This law regulates that every person is prohibited from carrying out unauthorized, illegal or manipulative acts: (a) access to telecommunications networks; and/or (b) access to telecommunications services; and/or (c) access to special telecommunications networks. Violators of these provisions are threatened with a maximum prison sentence of 6 (six) years and/or a maximum fine of 600 million rupiah. Furthermore, Article 40 of this law stipulates that every person is prohibited from intercepting information transmitted via telecommunications networks in any form. Violators of this provision are subject to a maximum prison sentence of 15 years. Apart from the matters mentioned above, this law also regulates the obligation of telecommunications service providers to keep confidential information sent by funds or received by telecommunications service customers via the fund's telecommunications network or the telecommunications services they provide (Article 42 Paragraph (1)). Organizers who violate these provisions are threatened with a maximum prison sentence of 2 (two) years and/or a maximum fine of 200 million rupiah.

Furthermore, personal data protection is also mentioned in Law Number 11 of 2008 concerning Information and Electronic Transactions. This law regulates that in the use of Information Technology, protection of personal data is one part of personal rights. This is regulated in Article 9 of this law where business actors who offer products through electronic systems must provide complete and correct information regarding contract terms, manufacturers and the products offered. Furthermore, Article 26 Paragraph (1) of this law states that unless otherwise determined by Legislative Regulations, the use of

[23] Makarim, Edmond. "Introduction to Telematics Law", Jakarta: Radja Grafindo Persada, 2009. P.179.

any information via electronic media relating to a person's personal data must be based on the consent of the person concerned. It can be seen that this article also adheres to one of the principles of personal data protection, namely the general principle. According to this principle, a person's personal data cannot be taken without the consent of the person concerned. The collection of data to be processed must be adequate and not excessive; for legitimate purposes, with the consent of the individual concerned (Provision of data to other parties must be based on consent). Then in Paragraph (2) it is stated that every person whose rights as intended in Paragraph (1) have been violated can file a lawsuit for the losses they have experienced based on this law.

Furthermore, in the explanation of this article (Paragraph (1)), it is explained that in the use of Information Technology, the protection of personal data is one part of personal rights. The protection of personal data in Article 26 is a fundamental protection of privacy and data. It contains data protection which contains elements regarding minimal and very broad protection of privacy. However, if a general interpretation of data protection is drawn, then specific data protection has actually been regulated in subsequent articles, as stated in Articles 30 to 33 and Article 35 which is included in CHAPTER VII concerning Prohibited Actions. If the general interpretation is used, then violations of personal data protection can be based on the provisions in this article.

In addition to the statutory regulations mentioned above, the Minister of Communication and Information has issued Regulation of the Minister of Information and Communication Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems. This Ministerial Regulation covers protection for the acquisition, collection, processing, analysis, storage, display, announcement, sending, dissemination and destruction of personal data, as regulated in Article 2 Paragraph (1) of the PDP Ministerial Regulation. This Ministerial Regulation covers protection for the acquisition, collection, processing, analysis, storage, display, announcement, sending, dissemination and destruction of personal data, as regulated in Article 2 Paragraph (1) of the PDP Ministerial Regulation. This Ministerial Regulation was issued due to the urgent need for legal regulations governing the protection of personal data. The Ministry of Communication and Information is aware of the need for statutory-level regulations that specifically regulate the protection of personal data. However, it takes quite a long time to form new laws and regulations, while the need for written rules governing the protection of personal data is urgently needed. Acting Director General of Informatics Applications, Mariam Barata, in an interview with CNN Indonesia said that, "We chose to issue this regulation in the form of a Ministerial Regulation because it is the easiest to complete, because we want it as soon as possible." This Ministerial Regulation, said Mariam, was issued because the protection of personal data was urgent. Meanwhile, to issue a law, the process time will be much longer. Head of the Yogyakarta Special Region Communication and Information Service, Rony Primanto, said that personal data protection in Indonesia is still very weak. However, he is optimistic about the government's commitment to protecting the personal data of the Indonesian people. He added that data protection is indeed uncertain, but there is already Ministerial Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, but this Regulation is only a Ministerial Regulation, not yet at the level of a Legislative Regulation, the Government needs to make this Ministerial Regulation into law.

Currently, Indonesia has Law Number 27 of 2022 concerning Personal Data Protection. Based on this Law, personal data is data about natural persons who are identified or can be identified individually or in combination with other information,

either directly or indirectly, through electronic or non-electronic systems.[24] This law categorizes personal data into two, namely specific data (includes health data and information, biometric data, genetic data, criminal records, child data, personal financial data; and/or other data in accordance with statutory provisions) and general data (includes full name, gender, nationality, religion, marital status, and/or personal data combined to identify a person).[25] Then this law defines personal data protection through Article 1 number 2, namely the overall efforts to protect personal data in the process of personal data processing in order to guarantee the constitutional rights of personal data subjects. In the PDP Law there are also personal data controllers and personal data processors. Personal data controller is any person, public body and international organization acting individually or jointly in determining the purposes and exercising control over the processing of personal data.[26] Meanwhile, a personal data processor is any person, public body and international organization acting individually or jointly in processing personal data on behalf of the personal data controller.[27] Furthermore, the PDP Law regulates the obligations of personal data controllers. Articles 20 to Article 50 of the PDP Law regulate the obligations of personal data controllers, which include the obligation to show proof of the consent that the personal data subject has given when processing personal data, the obligation to maintain the confidentiality of personal data, and the obligation to prevent personal data from being accessed unlawfully.[28]

C. Provisions that can be added to the Indonesian PDP Law.

The process of forming and drafting Law Number 27 of 2022 concerning Personal Data Protection has gone through various processes. In forming and compiling a statutory regulation, it is impossible to compile a perfect regulatory product without any loopholes or deficiencies. This also applies to the Indonesian PDP Law, although in general this law can accommodate the need for personal data protection in Indonesia, the author believes that the PDP Law can be further refined. This can be done by adding new provisions, so that the PDP Law gets better and of course can protect and accommodate the needs of the Indonesian people in terms of personal data protection. These provisions include:

Affirmation of Prioritization of Administrative Sanctions

In Law Number 27 of 2022 concerning Personal Data Protection, the author found that there has been no confirmation or prioritization of types of sanctions for incidents of personal data breaches. In the provisions of the PDP Law, there is no strict separation regarding the application of sanctions. When there is a violation or misuse of personal data, which type of sanction takes precedence, between administrative sanctions and criminal sanctions which must take priority in order to resolve disputes related to the management of personal data, compared to criminal sanctions.

In enforcing personal data protection laws, administrative sanctions should take precedence before criminal sanctions. Administrative sanctions enable data protection authorities to respond to breaches quickly and efficiently. For example, administrative fines and corrective orders can be implemented immediately to stop

[24] Article 1 number 1 Law Number 27 of 2022 concerning Personal Data Protection (UU PDP)
[25] Article 4 of the PDP Law
[26] Article 1 number 4 of the PDP Law
[27] Article 1 number 4 of the PDP Law
[28] Article 24, Article 36, and Article 39 paragraph (1) of the PDP Law

violations and prevent further damage. This provides flexibility in enforcement and allows authorities to adjust fines based on the severity of the offense and the capacity of the organization concerned.[29] Prioritizing administrative sanctions before criminal sanctions is a balanced and pragmatic approach to enforcing Iceland's PDPA. This enables a quick and efficient response to breaches, ensuring that the resources of law enforcement and data protection authorities are used effectively. In addition, this approach helps reduce the burden on the justice system, allowing it to focus on very serious cases that require criminal intervention.

Regulating Public Bodies as part of Personal Data Controllers and Processors

Article 1 paragraph (4) of the Indonesian PDP Law regulates the definition of a Personal Data Controller, which reads:

> *Personal Data Controller is every person, public body and international organization acting. individually or jointly in determining the purposes and exercising control over the processing of Personal Data.*

Furthermore, paragraph (5) defines Personal Data Processor, namely:

> *Personal Data Processor is any person, public body and international organization acting individually or jointly in processing Personal Data on behalf of the Personal Data Controller.*

If we examine it again, those categorized as either controllers or processors are people, public bodies and international organizations. In this article, Public Bodies are not included. In fact, many activities related to the collection and use of personal data involve public bodies. The easiest example that exists in our daily lives is e-KTP or Electronic Driving License.

The authors believes that Article 1 paragraph (4) and (5) of Law Number 27 of 2022 needs to be revised to also include Public Bodies as part of Data Controllers and Processors. By not including Public Bodies as Data Controllers and Processors, this will create uncertainty in terms of personal data protection, even though the Indonesian PDP Law was formed to protect the personal data of Indonesian citizens from violations and misuse of personal data. Apart from that, this can create ambiguity in the responsibilities and obligations of Public Bodies in controlling and processing personal data, even though in practice there are many activities carried out by Public Bodies that involve the collection and use of personal data.

Provisions regarding Guarantees of Stronger Protection for the Data of Children and Vulnerable Groups

The presence of the PDP Law in Indonesia has been eagerly awaited by various parties. However, the presence of the PDP Law still raises various notes, one of which is regarding the protection of personal data for vulnerable groups. In particular, the PDP Law regulates the processing of personal data of children and people with disabilities. Children's personal data is categorized as specific data, because it is a sensitive type of data and its processing carries risks to the owner. Apart from child data, biometric data, credit cards and criminal records are also included in the specific data category.

Children's personal data which is categorized as specific personal data is actually something that is as it should be. This is because children are parties who are

[29] Insights: Data Protected, available at https://www.linklaters.com/en-us/insights/data-protected/data-protected---iceland.

deemed unable to give consent because children are categorized as parties who are not yet legally competent. Apart from that, children also tend not to understand the consequences and consequences of processing personal data. The PDP Law stipulates that the processing of children's personal data must be "specially carried out" and requires the consent of parents or guardians.

The main problem here is that there are no clear regulations regarding the form of "special provision". This causes personal data processors to not have clear legal protection standards in processing children's personal data. This could result in the potential for misuse of children's personal data.

Apart from relating to children's personal data, the PDP also regulates that the personal data of people with disabilities is held specifically and requires their consent. This regulation actually indicates the government's attention to people with disabilities. However, problems can also arise because the form or practice of implementation in the field is still unclear.

Include the Principle of Non-Discrimination in the PDP Law

Article 3 of Law Number 27 of 2022 concerning Personal Data Protection regulates the principles that apply to this Law. The principles that apply to this Law are protection, legal certainty, public interest, expediency, prudence, balance, accountability and confidentiality. If we compare it with the PDP Law in other countries, the principles contained in the PDP Law are actually quite complete. However, in the author's view there is an important principle that is not included in this Law, namely Non-Discrimination. The principle of non-discrimination in personal data protection emphasizes that a person's personal data must not be used as a basis for differentiating or treating someone unfairly or unequally. This means that personal data controllers and processors must treat all individuals fairly and equally, without regard to race, religion, ethnicity, gender, political views and other irrelevant factors.

The absence of this principle in the PDP Law could lead to a looser interpretation or even misuse of personal data for discriminatory or unfair purposes. Apart from that, this has the potential to open up space for misuse of data to discriminate against certain minority groups. On the other hand, the spirit of specific personal data protection regulations is to avoid discrimination against data subjects.

The principle of non-discrimination in personal data protection laws is a vital foundation in ensuring that every individual is treated fairly and equally under the law, regardless of personal factors such as a person's race, religion or political views. The existence of this principle is not only to protect human rights, but also to ensure the creation of a more just and inclusive society. In an era where technology is increasingly involved in decision making, the principle of non-discrimination becomes increasingly important to prevent digital discrimination that can occur through the use of algorithms and data analysis that do not take these values into account. Including the principle of non-discrimination in data protection laws also strengthens public confidence in the data protection system, as individuals will feel more confident that their personal information will not be misused or used for discriminatory purposes. Additionally, by adopting this principle, a country also ensures compliance with international standards such as those set out in the European Union's General Data Protection Regulation (GDPR), which in turn can facilitate safe and secure cross-border data transfers.

D. Challenges in Enforcing Personal Data Protection Laws in Indonesia

Chalenges

With the enactment of Law Number 27 of 2022, the protection of personal data of Indonesian citizens can be more or less protected. However, in enacting this law, the government has big homework that has the potential to become a challenge in its implementation. The first challenge is related to the effort and costs that must be incurred in its implementation. The "price" that must be paid in implementing the PDP Law is certain to be very expensive. This is because the private and corporate sectors will be involved.

If you look more closely, companies and public bodies such as the financial industry, banking, hospitals and other business institutions are actually the ones who benefit most from the absence of the PDP Law. This can be seen from the widespread leakage and misuse of data by business actors for the sake of profit. The easiest example to find is the number of telemarketers who deliver product promotions, even though consumers never provide their personal data to the telemarketer. This happens because indications arise of customer or consumer data being traded.[30]

Apart from that, digital platforms, companies and public bodies which have been carrying out activities to collect and utilize big data containing personal data are actually the ones who are negligent in protecting data, because they are able to study and control the use of people's personal data.[31] So, the first effort that the government must make is to ensure that companies and public bodies can truly comply with the PDP Law. The next challenge is people's understanding of this rule. The government must also ensure that all levels of society can understand this rule. Because, if people do not understand these rules, violations or misuse of personal data could be carried out by the people themselves unintentionally. This can happen because our society's culture likes to share and belong to a collective society. In our society, the concept of privacy tends not to be the main thing, compared to societies that adhere to individualist cultures. Therefore, there is a very large potential for violations of this law to be carried out unintentionally by the people themselves. The most common example is school institutions uploading student activities via social media.[32] This violates the PDP Law even though it was done unintentionally, because in Article 4 paragraph (2) of this Law it is regulated that children's data is a type of specific personal data, while on the other hand there are still many people who do not understand about personal data and its regulation.

The next challenge is children's personal data which is prone to misuse by technology platforms. Through the PDP Law, the protection of children's personal data becomes a priority. However, the regulations regarding children's personal data in the PDP Law are considered insufficient to protect children's personal data from misuse. The contents of the PDP Law regulate children's personal data which is categorized as specific data. This means that data that is sensitive and has a high risk to the data owner can be equated with financial data, medical data, or someone's criminal record.

[30] Wildan Novriansah: Sales of Bank Customer Data via Darkweb revealed, available at https://news.detik.com/berita/d-6876746/terungkap-penjualan-data-nasabah-bank-via-darkweb.

[31] Ministry of Communication and Information: Together Protect Personal Data on Digital Platforms, available at https://www.kominfo.go.id/content/detail/28343/bersama-lindungi-data-pribadi-di-platform-digital/0/artikel

[32] The Coversation: The Personal Data Protection Law is vulnerable to victims and does not guarantee strong data protection, available at https://theconversation.com/panel-ahli-uu-perlindungan-data-pribadi-rentan-makan-korban-dan-belum-jamin-proteksi-data-yang-kuat-191018

The PDP Law regulates that platforms that control and process children's personal data must organize it specifically and must obtain consent from the child's parents or guardians. However, apart from being related to the consent of parents or guardians, the PDP Law does not yet explicitly regulate this form of "special provision".

Apart from that, the PDP Law does not regulate the age of children which can be categorized as children's personal data. This should be regulated considering that the legal system in Indonesia still has varied regulations regarding child age limits. The contents of the Child Protection Law and the Civil Code also provide different age limits for children. This difference can then lead to different interpretations regarding the age limit for children who have the potential to abuse digital platforms. This arrangement, which is considered insufficient, has the potential to cause problems in the future. Digital platforms that offer new methods for children's learning and socializing have recently been commercialized. Reports from Narasi and Human Rights Watch reported that educational platforms were proven to have sold children's data with the aim of developing their business. With the rapid development of technology, especially in the field of education, it is very possible that a child who by law should receive an education, is instead forced to accept invasive data practices from various existing educational platforms. Ironically, nowadays this is considered normal and tends to be allowed to happen.

Opportunities

Apart from creating obstacles and challenges in its implementation, the PDP Law also presents potential opportunities that can be felt by the community. The fundamental changes caused by the PDP Law will also open up new business opportunities for Indonesian advocates. Parties who must comply with the provisions of the PDP Law will of course need the assistance of advocates to ensure that their personal data management activities do not violate and avoid the threat of sanctions from the PDP Law. Therefore, the implementation of the PDP Law is expected to bring various kinds of demand for legal services for legal practitioners in Indonesia.

Advocates will receive various requests for legal consultation, because the PDP Law requires the preparation of various documents (privacy protection policy, code of conduct, personal data management, and a written consent letter from the data owner) in managing personal data. Apart from that, it is also necessary to develop steps to prevent and overcome personal data leaks, and so on. Furthermore, this will not only come from within the country, but also from users of legal services from abroad, considering that the PDP Law also has a scope, where its provisions bind personal data organizers domiciled outside the territory of Indonesia as long as what they manage is data. individual Indonesian residents.

The large number of legal services provided in the field of privacy and personal data protection is generally due to the complexity of privacy regulations and personal data protection, making personal data providers need those who have expertise in this field. This is evident from, where the majority of correspondence from actors in the personal data management industry in America and Europe stated that they use the assistance of external legal service providers to handle privacy matters and protect their personal data. Apart from bringing benefits to legal practitioners, the PDP Law is also expected to generate new business fields for domestic providers of support services for the advocate profession; for example, legal education providers. In direct proportion to the large number of requests for legal services in the field of privacy and personal data protection, of course there will be many Indonesian

advocates who need legal knowledge in this field, because this field can be said to be still relatively new among legal practitioners in Indonesia.

Then, there are also business opportunities as an organization or association that issues certification for legal practitioners who carry out specialized practices in the field of personal data protection. The practice of certification has been developing for quite some time in America and Europe (and more recently in Singapore, Hong Kong and India), and the practice has become commercial in the privacy and personal data protection industry abroad. One example, the certification (CIPP) issued by shows that the recipient is familiar with the rules for privacy and personal data protection. To get CIPP certification, the exam is priced at US$ 550 (around Rp. 7.5 million). Next, certification recipients need to dig into their pockets again and pay an additional US$ 125 (around Rp. 1.7 million) per year for the certification to remain valid.

Lastly, the PDP Law will increase public awareness of personal data protection. As Roscoe Pound said, Law as a tool of social engineering. With the enactment of the PDP Law, it is hoped that people will change, from previously ignoring and not caring about their personal data, to becoming more concerned and maintaining the security of their personal data from data leaks.

III.CONCLUSION

In conclusion, Indonesia's legal framework on personal data protection has evolved over the years, encompassing regulations from various laws, including those related to archives, company documents, banking, telecommunications, information and electronic transactions, as well as specific ministerial regulations. These laws reflect the country's commitment to safeguarding individuals' personal data in different contexts, such as archives and company operations, banking secrecy, telecommunications, electronic transactions, and electronic systems. Each of these regulations outlines specific provisions for the protection, processing, storage, and destruction of personal data, ensuring that data usage is lawful, limited, and respectful of individuals' privacy rights. The newly enacted Law Number 27 of 2022 concerning Personal Data Protection further solidifies Indonesia's stance on personal data protection by defining personal data categories, establishing the roles and responsibilities of personal data controllers and processors, and outlining obligations for data controllers to ensure consent, confidentiality, and lawful data processing. Moving forward, the implementation and enforcement of these regulations, including the PDP Law, will be crucial in upholding individuals' rights to privacy and fostering trust in data handling practices. There is a need for continued effort to enhance awareness, compliance, and capacity-building among stakeholders to effectively navigate the complexities of personal data protection in the digital age. Overall, the comprehensive legal framework in Indonesia demonstrates a commitment to modernizing data protection practices and ensuring that personal data is handled responsibly, ethically, and in line with constitutional rights. By consolidating and strengthening these legal provisions, Indonesia can further advance its data protection regime and promote a safe and secure environment for data processing activities.

Indonesia's enactment of Law Number 27 of 2022 concerning Personal Data Protection marks a significant step towards strengthening the protection of personal data for Indonesian citizens. However, the implementation of this law presents various challenges that the government must address. One major challenge is the significant effort and costs required to implement the PDP Law, especially involving

private and corporate sectors that may have benefitted from the lack of data protection regulations. Ensuring compliance from companies and public bodies, such as financial institutions and hospitals, is crucial to prevent data misuse and leakage for profit-driven purposes. Another challenge lies in fostering public understanding of the regulations. Given Indonesia's cultural inclination towards collective society and a lesser emphasis on privacy, there is a risk of unintentional violations due to lack of awareness. Ensuring educational initiatives to raise awareness among all levels of society is essential to mitigate this risk. Moreover, the protection of children's personal data presents a specific challenge as current regulations may be deemed insufficient to prevent misuse by technology platforms. Ambiguities regarding the age at which children's data is protected and the lack of specific provisions pose potential problems for the future safeguarding of children's data from exploitation.

Despite the challenges, the implementation of the PDP Law also brings opportunities, particularly for legal practitioners. The law creates a demand for legal services related to privacy protection and personal data management, offering new business avenues and potentially attracting international clients seeking compliance with Indonesian regulations. Additionally, the law may lead to the development of certification programs and specialized practices in personal data protection, similar to existing practices in other regions. This could enhance legal knowledge in the field and create new business opportunities for domestic support services providers and legal education institutions. Overall, while the implementation of the PDP Law poses challenges, it also holds the potential to raise public awareness, drive legal innovation, and create new avenues for legal practitioners and support services in the field of personal data protection in Indonesia.

BIBLIOGRAPHY

Alza Ahdira: "Hundreds of Thousands Covid-19 Patients Data Allegedly Leaked, sold by Hackers on Dark Web Sites", available at https://www.pikiran-rakyat.com/nasional/pr-01572317/data-ratusan-ribu-pasien-covid-19-diduga-bocor-dijual-peretas-di-situs-dark-web.

Bagus Sudirman, "Get to know the meaning and function of BIG DATA", available at http://teknik-informatika-s1.stekom.ac.id/informasi/baca/Mengenal-Pengertian-Dan-Fungsi-BIG-DATA/bda947d7ccc3524999a0fabe36b3783a24bd510b

Data protection, available at https://theconversation.com/panel-ahli-uu-perlindungan-data-pribadi-rentan-makan-korban-dan-belum-jamin-proteksi-data-yang-kuat-191018

Davis, Gordon B. "Management information System", Jakarta: PT. Pustaka Binaman Pressindo, 1984. p12.

Endang Sumardi, "The development of communication technology has changed every aspect of people's daily lives", available at https://portal.sukabumikota.go.id/4112/perkembangan-teknologi-komunikasi-telah-mengubah-setiap-aspek-kehidupan-masyarakat-sehari-hari

Garfinkel, Simson. "Database Nation: The Death of Privacy in the 21st Century". Massachusets: O'Reilly, 2000.

Indonesia, Undang-Undang tentang Informasi dan Transaksi Elektronik (Law regarding Information and Electronic Transaction) UU No. 19 Tahun 2016 (Law Number 19 Year 2016)

Indonesia, Undang-Undang tentang Perlindungan Data Pribadi (Law regarding Personal Data Protection), UU No. 27 Tahun 2022 (Law Number 27 Year 2022).

Indotelko: There are no personal data regulations, Indonesia loses IDR 500 billion, available at http://www.indotelko.com/kanal?c=id&it=data-pribadi-indonesia-rugi-500-miliar

Insights: Data Protected, available at https://www.linklaters.com/en-us/insights/data-protected/data-protected---iceland.

Jerry Kang, (1998) "Information Privacy in Cyberspace Transaction", *Stanford Law ReviewVol 50*, Apr

Kusumaatmadja, Mochtar. "Legal Development in the Context of National Development", Bandung: Bina Cipta, 1975.

Makarim, Edmond. "Introduction to Telematics Law", Jakarta: Radja Grafindo Persada, 2009.

Ministry of Communication and Information: Together Protect Personal Data on Digital Platforms, available at https://www.kominfo.go.id/content/detail/28343/bersama-lindungi-data-pribadi-di-platform-digital/0/artikel

Narendra,, Albertus Pramukti. (2015), "Big Data, Data Analysis, and Librarian Competency Development", *Record and Library Journal*: Vol. 1: No. 2.

Noam Rotem and Ran Locar, "Indonesian Government's Covid-19 App Accidentally Exposes Over 1 Million People in Massive Data Leak", available at https://regional.kontan.co.id/news/psbb-jakarta-berlaku-hari-ini-ingat-kembali-protokol-kesehatan-dan-sanksinya?page=all

Pendit, et.al, *The Meaning of Information: Continuation of a Debate*. Jakarta: Kesaint-Blanc. 1992.

Purwanto, (2007) *Research on Legal Protection of Digital Data.* Jakarta: Badan Pembinaan Hukum Nasional.

Sinta Dewi, "*Cyber Law: Aspects of Data Privacy According to International, Regional and National Law"*, Bandung: Refika Aditama, 2015.

Shinta Dewi, (2017) "Principles of Protection of Personal Data of Credit Card Customers According to National Regulations and Their Implementation", *Jurnal Sosiohumaniora*. Vol.19, No.3.

Shinta Dewi, *"Privacy Protection of Personal Information in E-Commerce According to International Law"*, Bandung.

The Coversation: The Personal Data Protection Law is vulnerable to victims and does not guarantee strong

United Nations Conference on Trade and Development: "Information and Communication Technology Development Indices", *ICT Development Indices*, New York and Geneva, 2003.

Warren, Brandheis, (1890), "The Right to Privacy", Harvard Law Review, Massachusetts.

Welfare State on Britannica Online Encyclopedia, available at https://www.britannica.com/money/topic/welfare-state

Wildan Novriansah: Sales of Bank Customer Data via Darkweb revealed, available at https://news.detik.com/berita/d-6876746/terungkap-penjualan-data-nasabah-bank-via-darkweb.