

Consumer's Personal Data Protection in the Digital Era

Hasnati Hasnati,¹ Puti Mayang Seruni²

¹Faculty of Law, Universitas Lancang Kuning, Pekanbaru, Indonesia

²Faculty of Law, Universitas Islam Riau, Pekanbaru, Indonesia
putimayangseruni@law.uir.ac.id

Abstract

This research aimed to analyze the legislative arrangements related to the protection of personal data, especially for consumers. This research is important because it discusses the potential misuse of personal data belonging to consumers. The research was conducted normatively and analyzed qualitatively, and the results of this research on personal data protection in Indonesia are described descriptively. This research has resulted in new findings in the form of protection in the latest regulation and also challenges to enforce the regulation. So that these findings can be used as material for further research. The protection of personal data in Indonesia is regulated in several regulations. However, in 2022 Indonesia enacted Law number 27 of 2022 on the protection of personal data. This law contains specific norms regarding the right to protection of personal data from the limitation and definition of matters related to personal data, rights and obligations of subjects related to personal data to the regulation of sanctions. Currently, the protection of personal data, especially for consumers, still faces challenges, ranging from the challenge of low public awareness, standard clauses in consumer agreements to the absence of special institutions whose duties oversee the problems and implementation of data protection.

Keyword: Consumer; Digital; Personal Data; Protection

1. INTRODUCTION

Following the Covid-19 pandemic, Indonesia's digital economy has grown at an accelerated rate. The digital economy of Indonesia was valued at US\$44 billion in 2020, compared to merely US\$18 billion for Thailand, US\$14 billion for Vietnam, US\$11.4 billion for Malaysia, US\$9 billion for Singapore, and US\$7.5 billion for the Philippines. According to this data, Indonesia had the most growth in its digital economy in Southeast Asia in 2020.¹

The development of the digital economy has also been followed by the development of network-based data storage methods or systems. This change brings its own advantages including being able to store an unlimited amount of data, easier, practical, economical and easily accessible anytime and anywhere. However, among its advantages, network-based data storage has disadvantages and even dangers. Network-based data storage opens up opportunities for data leakage because there is a possibility of being tapped by certain parties. Leaks of personal information can be exploited for malicious activities like fraud, theft, bank account

¹ Al Sentot Sudarwanto and Dona Budi Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime* 29, no. 4 (September 30, 2022): 1443–57, <https://doi.org/10.1108/JFC-09-2021-0193>.

intrusions, unsolicited product promotion, and invasions of privacy.² Furthermore, the misuse of personal data has also given birth to cyber-crime, especially in the form of phishing or crime with the mode of luring victims with a number of data owned so that the victim believes and believes in providing complete personal data to the perpetrator.³

In Indonesia, there have been a number of data leakage cases. Among them is what happened to Tokopedia in 2020 which resulted in the hacking of 15 million user data containing e-mails, passwords and usernames and was successfully sold for USD 5,000 in 2020.⁴ Then in May 2023 Bank Syariah Indonesia also faced a hack suspected by ransomware which resulted in network system paralysis for several days. The next case of leakage of bank customer data in Indonesia obtained from Bank Indonesia's website in 2021 to 2022 was carried out by Russian hackers, Conro Ransomware with the modus operandi of locking the system and retrieving the data.⁵ It is known that the data that was successfully retrieved was 52,767 document items with a capacity of 74 gigabytes hacked from 237 computer devices on Bank Indonesia's network.⁶

The data leakage cases that have occurred have encouraged Indonesia to provide protection regarding personal data rights which are then outlined in the form of concrete regulations. Especially considering that Indonesia is a state of law that guarantees legal order that provides legal protection to the community.⁷ Since 2016, the government of Indonesia through the Ministry of Information and Communication has prepared a "Draft Law (Bill) on Personal Data Protection". However, it was only in January 2022 that the draft was enacted and became Law No. 27 of 2022 concerning Personal Data Protection (PDP Law).

There is no other research that examines the protection of consumer personal data in the digital era. However, issues regarding personal data protection in Indonesia have been discussed by several previous researchers. First, the research conducted by Erlina Maria and team. This research resulted in the finding that data security in

² Jean Pierre Guy Gashami, Christian Fernando Libaque-Saenz, and Younghoon Chang, "Social-Media-Based Risk Communication for Data Co-Security on the Cloud," *Industrial Management and Data Systems* 120, no. 3 (March 22, 2020): 442–63, <https://doi.org/10.1108/IMDS-03-2019-0131>.

³ Faiz Emery Muhammad and Beniharmoni Harefa, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web," *Jurnal USM Law Review* 6, no. 1 (April 24, 2023): 226, <https://doi.org/10.26623/julr.v6i1.6649>.

⁴ Muhammad Fathur, "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen," in *National Conference on Law Studies (NCOLS)*, vol. 2 (Universitas Pembangunan Nasional Veteran Jakarta, 2020), 43–60, <https://conference.upnvj.ac.id/index.php/ncols/article/view/1345>.

⁵ Aditama Candra Kusuma and Ayu Diah Rahmani, "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)," *SUPREMASI : Jurnal Hukum* 5, no. 1 (October 4, 2022): 46–63, <https://doi.org/10.36441/supremasi.v5i1.721>.

⁶ Kusuma and Rahmani.

⁷ Widiatama, Hadi Mahmud, and Suparwi, "Ideologi Pancasila Sebagai Dasar Membangun Negara Hukum Indonesia," *Jurnal USM Law Review* 3, no. 2 (2020): 310–27, <https://doi.org/http://dx.doi.org/10.26623/julr.v3i2.2774>.

Indonesia is currently regulated in regulations that are sectoral in nature so that it does not seem to be able to protect effectively and optimally.⁸ This research is quite detailed in discussing sectoral regulations that discuss personal data protection, so it can be a material and source of data for further research. However, when this research was conducted, there was no specific legal regulation governing personal data in Indonesia, so this article concludes that Indonesia has not yet prepared for the industrial revolution 4.0. The weakness of this research has also been answered in the discussion in this article. Second, the research conducted by Aditama Chandra Kusuma and team. This research found that Bank Indonesia has been negligent towards the security of bank customers' personal data in this country, the slow response from Bank Indonesia then shows that this country is still weak in terms of personal data protection, both in terms of regulations, technological resources and human resources.⁹ The strength of this research is that at the time of publication, it discussed a 'booming' issue, so it can be an additional insight for the general public. However, this research only focuses on a case regarding personal data leakage at Bank Indonesia so that the conclusions obtained are casuistic. Third, research conducted by Hanifan Niffari. This research concluded that personal data protection is protected in the constitution whose implementation is based on the personal data protection model of the European Union's General Data Protection Regulation (GDPR).¹⁰

This research has the advantage of examining the side of personal data protection from the constitutional level which then the regulatory practice is compared with regulations regulated by other countries, especially the European Union. Other countries have known the advantages of the concept of personal data protection regulated in the European Union's GDPR.

The differences between the previous research and this research are the point of the study which focuses on the protection of consumer rights as the basis for the protection of rights to personal data. The next difference is that at the time the research was conducted, Indonesia did not yet have a PDP Law. Therefore, this research can be said to have produced new findings in the form of a comparison of the form of protection in various regulations, both the old and the latest, then also reveal the challenges to enforce the regulation. These findings can then be used as material for further research in the field of personal data protection. This article

⁸ Erlina Maria Christin Sinaga and Mery Christian Putri, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 2 (August 27, 2020): 237, <https://doi.org/10.33331/rechtsvinding.v9i2.428>.

⁹ Kusuma and Rahmani, "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)."

¹⁰ Hanifan Niffari, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)," *Selidik: Jurnal Hukum Dan Bisnis* 7, no. 1 (2020): 105–20, <https://doi.org/https://doi.org/10.35814/selidik.v6i1.1699>.

discusses how regulations that protect personal data from unintended use by the owner can serve as a shield to protect consumer privacy and security, as well as the barriers to personal data protection in Indonesia. This article aims to see to what extent the PDP Law can provide consumer protection related to personal data in Indonesia. Hopefully, this research contribute ideas about data protection in Indonesia both in terms of regulations and challenges currently faced, so that people may become more aware of the importance of personal data protection for consumers.

2. METHOD

The normative legal method that only examines secondary data was chosen as the method of this research.¹¹ This research was conducted by examining legal materials in secondary data. The legal materials examined include primary, secondary and tertiary legal materials. First, selection of primary legal materials containing data that is binding with the problem to be studied, namely laws and regulations, jurisprudence or court decisions.¹² In this article, the primary legal materials selected for study are the Law on Personal Data Protection, the Law on Consumer Protection and several other laws that contain articles on personal data protection. Second, examining secondary legal materials that can help explain primary legal materials, such as draft laws, results of previous research, including legal expert opinions.¹³ Third, selecting tertiary legal materials which are materials used as an explanation of the meaning of primary and secondary legal materials, for example tertiary legal materials, namely legal dictionaries and encyclopedias.¹⁴ The data collected was then analyzed using a qualitative method, which is a way of researching by collecting and then analyzing the data obtained from the results of the literature review with the problems to be discussed. This qualitative analysis resulted in descriptive data analysis. The results of the research were then presented descriptively. The material that has been collected is then described logically and systematically which in the end will be linked and analyzed with the results of the literature study in order to answer the problem. The conclusions in the research to be carried out were drawn together based on deductive logic, which is the drawing of conclusions that process from general to more specific.

¹¹ Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat* (Jakarta: Rajawali Pers, 2010).

¹² Soekanto and Mamudji.

¹³ Amiruddin and Zainal Asikin, *Pengantar Metode Penelitian Hukum*, 10th ed. (Jakarta: Raja Grafindo, 2018).

¹⁴ Amiruddin and Asikin.

3. RESULTS AND DISCUSSION

3.1 Protection of Consumers' Personal Data Rights Under Indonesian Law

The role of customers who utilise digitalization to obtain their everyday necessities is inextricably linked to the fast growth of Indonesia's digital economy. Selling and buying items over the internet and having them shipped by a goods forwarding company is known as electronic commerce, or e-commerce.¹⁵ Marketplace is a type of e-commerce with many users today. Marketplace is also known as an online buying and selling service that facilitates meetings between sellers and buyers.¹⁶ In addition to the marketplace, a digital economy model that is also popular today is Financial Technology (fintech). Fintech refers to the practical application of information technology to enhance banking and other financial services.¹⁷ These developments then bring new problems, namely the vulnerability of embezzlement of consumer personal data by irresponsible individuals. Because in transactions carried out via the internet, consumers are required to fill in some personal data such as name, gender, population identification number, cell phone number, address and even personal photos. This data is indeed needed in the user verification process, especially in application-based systems in e-commerce and fintech.

The personal data that consumers voluntarily fill in related to account verification is then collected in one internet-based network. This large amount of consumer personal data is useful for business development, especially for determining target markets and advertising targets for a product. So that by holding consumer personal data, it can be seen what the market pattern is in a particular product. Therefore, in practice, there is a lot of buying and selling of data or exchanging consumer data between one company and another. If a company already holds consumer data, it is likely that the company is superior to its competitors who do not have this data.

The issue of personal data has become important as the number of consumers transacting over the internet has increased. Because consumers' personal data is so important, many forms of abuse have begun to occur, such as personal data trading, embezzled customer accounts, personal data leaked intentionally or unintentionally, fraud and pornography.

¹⁵ Dinda Pratiwi and Rianda Dirkareshza, "Pengelabuan Informasi Harga Di E-Commerce Terhadap Konsumen Melalui Flash Sale," *Jurnal Ius Constituendum* 8, no. 3 (2023): 406–23, <https://doi.org/http://dx.doi.org/10.26623/jic.v8i3.7344>.

¹⁶ Gelora Martanti, "Perlindungan Konsumen Bagi Penyandang Disabilitas Pada Sektor Perdagangan Online Berbasis Aplikasi Marketplace," *Jurnal USM Law Review* 6, no. 1 (2023): 242–59, <https://doi.org/http://dx.doi.org/10.26623/julr.v6i1.6387>.

¹⁷ Husni Kurniawati and Yunanto Yunanto, "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur Dalam Aktivitas Pinjaman Online," *Jurnal Ius Constituendum* 7, no. 1 (2022): 102–14, <https://doi.org/http://dx.doi.org/10.26623/jic.v7i1.4290>.

Based on this logic, it is important to contain legal regulations that serve as a legal umbrella to protect personal data, especially for consumers. From a conceptual standpoint, personal data is conceptually equivalent to privacy. Preserving one's integrity and dignity is the fundamental premise of privacy.¹⁸ The concept of privacy itself can be understood in a variety of ways, such as the freedom to select one's own path in life, the right to privacy-preserving technologies, the right to peaceful communication, and the right to be unbothered.¹⁹ This implies that in cases where personal data is associated with the right to privacy, an individual's personal data cannot be shared or utilised without the owner's consent. The data cannot be used, sold, or distributed for reasons other than those approved by the identity owner, even after it has been kept in a network database for a considerable amount of time and is no longer relevant to the original reason for supplying the information.

The Republic of Indonesia's 1945 Constitution does not explicitly define the phrase "protection of personal data rights." However, Article 28 G, paragraph 1 of the 1945 Constitution of the Republic of Indonesia, which declares that everyone has the right to protection of self, family, honour, dignity, and property under his/her control, really accommodates the notion of personal protection implicitly. This article further clarifies that everyone has the fundamental right to feel safe and fear-free, regardless of whether they choose to do or not do something.

Part of the protected human rights includes the protection of the person, property, and feelings of security.²⁰ Therefore, as the article states, personal data protection is the most recent advancement in personal self-protection.²¹

Law No. 8 Year 1999 on Consumer Protection (Consumer Protection Law) does not specifically address the protection of consumers' personal data. However, from the standpoint of Article 1 Paragraph 1 of the Consumer Protection Law, consumer protection refers to all actions taken to guarantee consumers' legal certainty and protection. This broad definition appears to be the cornerstone for guaranteeing the privacy of customer information. It's only that this Law makes no clear reference to or explanation of privacy with regard to consumer personal data. Given that the Law has been in effect since 1999, this makes sense. At the time, the importance of protecting consumers' rights to personal data was not yet understood. Therefore, in

¹⁸ Sinaga and Putri, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0."

¹⁹ Russel Butarbutar, "Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia," in *3rd International Conference on Law and Governance (ICLAVE 2019)* (Atlantis Press, 2020), 154–63, <https://doi.org/10.2991/aebmr.k.200321.020>.

²⁰ Mriya Afifah Furqania and Ahmad Sholikhin Ruslie, "Tanggung Gugat Pemerintah Dalam Perlindungan Data Pribadi," *Bureaucracy Journal* 3, no. 1 (2022): 482–93, <https://doi.org/https://doi.org/10.53363/bureau.v3i1.195>.

²¹ Faiz Rahman and Dian Agung Wicaksono, "Researching References on Interpretation of Personal Data in the Indonesian Constitution," *Jurnal Penelitian Hukum De Jure* 21, no. 2 (June 24, 2021): 187, <https://doi.org/10.30641/dejure.2021.v21.187-200>.

accordance with Article 4 I of the Consumer Protection Act, which includes consumer rights, the protection of personal data belonging to consumers can be examined based on other laws. This is because the rights specified in the provisions of other laws and regulations are stipulated independently from those of the Consumer Protection Act.

A number of clauses of Law No. 39/1999 on Human Rights (Human Rights Law) protect citizens' privacy. The law's Article 14 Paragraph 2 highlights everyone's right to use all means at their disposal to seek out, obtain, possess, store, process, and communicate information. The right of every individual to the defence of their person, family, honour, dignity, and property is then affirmed by Article 29 Paragraph 1. If examined more deeply, it can be concluded that obtaining and using something is a right for every citizen, but this right is also limited by other people's rights related to self-protection, including personal data. This means that when someone wants to obtain data and then use the data for their own interests, it is not allowed to obtain and process data, especially personal data owned by others without the will of that person.

At this time, certain data or information is generally contained in an electronic system. Unless the law specifically states otherwise, all information in electronic media pertaining to personal data belonging to individuals must be used with the owner's consent, as per Article 26 of Law No. 19/2016 on the amending of Law No. 11/2008 on Electronic Information and Transactions (EIT Law). If it is found that rights related to personal data are violated, the owner of personal data can file a lawsuit. Electronic system operators must delete unrelated data if requested by the data owner and if requested based on a court order.

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions contains additional regulations pertaining to personal electronic data. Article 1 Point 29 of the Government Regulation on the Implementation of Electronic Systems and Transactions defines electronic data as personal information that can be uniquely identified, either by itself or in combination with other information obtained directly or indirectly from electronic and/or non-electronic systems.

The data mentioned above comprises both manual data that is not based on electronic systems and data that is based on electronic systems (electronic data). Writings, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail (e-mail), telegrams, telex, telecopy, or the like, letters, signs, numbers, access codes, symbols, or perforations are all considered forms of electronic data, as defined by Article 1 Point 30 of the Government Regulation.

The protection of personal data was governed by a number of stand-alone laws before the Personal Data Protection Law was passed. These laws included the previously mentioned Consumer Protection Law, Human Rights Law, EIT Law,

and PP on the Implementation of Electronic Systems and Transactions. Furthermore, other rules and regulations also cover the security of personal data, for example "Law No. 24 of 2013 Concerning the Amendment to Law No. 23 of 2006 Concerning Population Administration, Law No. 36 of 2009 Concerning Health, Law No. 36 of 1999 Concerning Telecommunications, Law No. 14 of 2008 Concerning Public Information Disclosure, Regulation of the Minister of Communication and Information Technology No. 20 of 2016 Concerning the Protection of Personal Data in Electronic Systems and OJK Regulation No. 77/POJK.01/2016 Concerning Information Technology-Based Money Lending and Borrowing Services." The above regulations still discuss the protection of personal data. The above regulations still discuss the protection of personal data partially, there is no affirmation of definitions, affirmation related to the boundaries of personal data as well as the rights and obligations of personal data owners and personal data controllers specifically.

Ensuring the protection of personal data as stipulated by the aforementioned laws and regulations is insufficient to address the present issues. The challenge in question comes from technological developments that make changes in economic transactions become digital-based. Especially when the Covid-19 pandemic hit. Lifestyle changes that limit direct interaction stimulate digital economics growth in Indonesia. The effect of digitalization on many sectors of human life has certain challenges. The influence of the internet is part of consumer privacy that must be protected because the evidence of information from customers is very likely to be used improperly by people who do not have a sense of responsibility to commit criminal acts against the person who owns the data.²² Thus, since 2016, a bill that specifically governs the protection of personal data has been proposed. To boost Indonesia's economic growth, this law must be able to safeguard both customers and the community as individuals. Therefore, the Draft Law on Personal Data Protection was proposed by the government through the Ministry of Communication and Information.

The long process in enacting the Personal Data Protection Bill occurred because of the conflict of interest between agencies that will bear certain responsibilities when this bill is enacted. The discussion became complicated when it would regulate the authority, institutions, financial management, regulation of rights and obligations

²² Utari Afnesia and Rahmi Ayunda, "Perlindungan Data Diri Peminjam Dalam Transaksi Pinjaman Online: Kajian Perspektif Perlindungan Konsumen Di Indonesia," *Jurnal Komunitas Yustisia* 4, no. 3 (2021), <https://doi.org/https://doi.org/10.23887/jatayu.v4i3.43743>.

and sanctions that would be regulated in the bill.²³ After several years of delays, finally in October 2022 Protection PDP Law was enacted.

The PDP Law establishes key provisions that serve as benchmarks for Indonesia's unique personal data protection regime. The PDP Law enhances the prior legislation that governed the protection of personal data. Definitions, justifications, and restrictions that must be taken into account in relation to the protection of personal data are provided by these points.

The main concern is the legal topics that this PDP Law protects. This PDP Law covers all legal subjects, including individuals, public organisations, and international organisations that are based in or outside of the Republic of Indonesia but have an impact on the rule of law for the Republic of Indonesia or for Indonesian citizens. This includes both natural persons (*natuurlijk persoon*) and legal entities (*recht persoon*). However, actions pertaining to personal data that are carried out by an individual while they are a private or household member are not covered by this PDP Law. To restrict the extent of protection covered in personal data, it is crucial to define the topic.

Second, regarding the types of personal data that are protected, this type of personal data was previously not regulated in any regulation. The types of personal data according to the PDP Law are general/common and specific/distinctive. General personal data includes full name, gender, nationality, belief, marital status and all data related to a person's personal identity. Specific personal data includes information on health conditions, biometric records, genetic information, criminal records, children's personal data, financial and all data contained in laws and regulations. These two types of personal data have similarities with those regulated in the GDPR applicable in Europe. Where GDPR divides types of personal data into General Personal Data and Specific Personal Data.

Third, regarding the rights of personal data subjects, this right was not previously discussed in detail in any regulation. The PDP Law defines protected rights related to personal data subjects, which are natural persons to whom personal data is attached, or can be said to be the owner of personal data identity. Some of the rights regulated range from the right to obtain information about the basis and purpose of a request for personal data, forms of accountability, the right to rectify their personal data, access to personal documents, to the possibility of requesting the cessation and withdrawal of consent to the processing of their personal data. The rights of the subject or owner of personal data are important to emphasize and are relevant to the current conditions where digital consumers must share some of their

²³ Padma Widyantari and Adi Sulistiyono, "Pelaksanaan Harmonisasi Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP)," *Jurnal Privat Law* 8, no. 1 (2020): 117–23, <https://doi.org/https://doi.org/10.20961/privat.v8i1.40384>.

personal data in order to enjoy digital services. Once the consumer feels that the data is no longer relevant to the digital services, he/she enjoys or feels that the data is in unsafe hands, the consumer has the right to request that his/her personal data be removed from the system.

Fourth, regarding the obligations of personal data controllers, the obligations of personal data controllers are related to the rights of personal data owners. This obligation starts from a clear foundation for the management of consumer-owned data, the consent of the data owner, guaranteeing access to information on personal data managed in relation to the personal data concerned and being obliged to manage personal data belonging to consumers in accordance with statutory regulations. This obligation encourages data controllers, who are usually on the business side, to be careful in managing the data.

Fifth, regarding the government's role in personal data protection, the PDP Law mandates that the government establish an institution that acts as a personal data protector. The establishment of this institution will also be further regulated and discussed in a special implementing regulation. This institution is expected to help resolve personal data issues that arise due to economic digitization.

Sixth, regarding sanctions, PDP Law contains two types of sanctions for violations of this law. These sanctions are in the form of administrative sanctions and criminal sanctions. Included in administrative sanctions can be in the form of written warnings, stopping temporary activities, actions to delete personal data to a fine of up to two percent of the annual income of the personal data controller. Criminal sanctions may include imprisonment of up to six years and a fine of up to six billion rupiah. The punishment for the controller of personal data who is a company is to impose punishment on the management, command holder, command giver, beneficial owner, and the company. With a note that the punishment for the corporation is only a fine of 10 times the maximum fine regulated. The PDP Law also regulates additional punishment in the form of forcible retrieval of corporate profits and corporate assets obtained from the criminal act and is obliged to pay compensation.

3.2. Challenges Faced in Protecting Personal Data Rights in Indonesia

The PDP Law's passage does not mean that Indonesia's issues with personal data security are resolved. It is anticipated that the PDP Law will open a new chapter in the defence of citizens' rights to privacy pertaining to their innate identities. According to Lawrence M. Friedman, a nation's ability to properly implement its legal system depends on the success of its legal framework, legal content, and legal culture. Legal content refers to rules dictating how an institution should operate,

legal structure leads to law enforcement personnel or institutions authorised to implement the law, and lastly, there is a legal culture, which is defined as the social attitudes and values that exist in society.²⁴ In addition, there is also Soerjono Soekanto who provides opinions related to important factors in the success of law enforcement. The factors in question are the law itself, law enforcers and means of law enforcement, society and the culture that is carried out.²⁵

Law enforcement related to the protection of citizens' rights cannot run well if the legal substance component or the legal factor itself does not contain a solution to overcome a particular problem. So how the content or sound of the PDP Law will determine whether this Law can provide solutions to the problems of personal data protection that are being faced. Furthermore, how law enforcement can correctly execute the PDP Law is a significant factor in law enforcement's approach to consumer personal data protection. Naturally, in this situation a forum in the shape of a unique organisation that manages matters pertaining to Indonesian personal data protection is required. Finally, if the legal substance is ideal and law enforcers have served properly, then the next component that must be considered is the legal culture or how the culture prevails in society. Quite often, regulations in Indonesia cannot be implemented by citizens because they do not understand the urgency of enforcing these regulations. There are several challenges that are being faced by consumers in Indonesia, especially regarding personal data protection. Which at this time these challenges still cannot be overcome with the PDP Law which is not even two years after it was enacted.

The public's awareness is the first obstacle. Public awareness of the need to secure the personal information associated with them is now the largest obstacle to the protection of consumers' personal data. This awareness will arise if the public already understands the dangers associated with the misuse of personal data. There are many cases of fraud or scamming via the internet where people are asked to provide personal data with the promise of a reward or prize. Fraud under the guise of a door-prize until now has claimed many victims. Victims who are tempted by the lure of a prize are then led to provide personal data such as full name, ID card number to various passwords such as ATM, M- Banking, e-mail, and even social media passwords. This is very dangerous because with the password information, the perpetrator can access the victim's personal account and can even connect to other accounts. Unfortunately, the latest PDP Law does not regulate the role of the government to conduct campaigns or education related to awareness related to personal data as an active preventive effort from the consumer or data owner side.

²⁴ Lawrence M. Friedman, *Sistem Hukum Perspektif Ilmu Sosial* (bandung: Penerbit Nusa Media, 2009).

²⁵ Soerjono Soekanto, *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum* (Jakarta: PT. Raja Grafindo Persada, 2008).

The emphasis on protection in the PDP Law is still related to repressive efforts, namely the existence of sanctions when violations have occurred. Meanwhile, preventive efforts are also focused on the obligation of data managers to do and not do something related to personal data under their control. According to the author, the role of public education should be entrusted to the personal data protection institution as mentioned in Article 58 of the PDP Law.

Second, regarding standard clauses, standard clauses are a challenge that consumers must face. The Consumer Protection Law's Article 1 Point 10 discusses standard clause wording. Any norms, provisions, and conditions that corporate actors have unilaterally developed in advance and that are then outlined in a legally enforceable document or agreement that consumers must comply with are referred to as standard clauses in the article.

The use of standard provisions governed by Article 18 of the Law on Consumer Protection is prohibited under a number of circumstances. However, the prohibition is still about the prohibition to include clauses that eliminate the responsibility of entrepreneurs related to goods and or services taken by customers or other things that are unilaterally beneficial for business actors but detrimental to consumers related to goods and/or services that are the object of transactions.

The ban on the inclusion of standard provisions requesting the authorization of the customer to submit specific personal data that is unrelated to the ongoing buying and selling activities is still not supported by the customer Protection Law. It also does not contain a prohibition for business actors to include the consent of consumers so that business actors can use the personal data for unilateral interests. This is reasonable because this consumer protection law was enacted around 23 years ago and is valid until now. At that time, the internet was not yet freely accessible to the public, so the term personal data protection was not recognized.

Standard clauses are currently born from business practices that aim to facilitate buying and selling transactions. Business actors like to use standard clauses in standard agreements that are the same for each consumer for reasons of effectiveness. Because it is very difficult and time consuming if the agreement with all consumers is compiled one by one and different between consumers. The existence of standard clauses will simplify, shorten time and save operational costs, especially if applied to business relationships that require complex agreements.²⁶

The participation of one of the parties in the standard clause, especially when drafting the points of the agreement, is missing. Therefore, it is only natural to say

²⁶ Muhamad Hasan Muaziz and Achmad Busro, "Pengaturan Klausula Baku Dalam Hukum Perjanjian Untuk Mencapai Keadilan Berkontrak," *Jurnal Law Reform* 11, no. 1 (2015): 74–84, <https://doi.org/https://dx.doi.org/10.14710/lr.v11i1.15757>.

that standard clauses limit the existence of the principle of freedom of contract.²⁷ There are several things that are desired by the principle of freedom of contract, namely that everyone is free to want to make or not make an agreement, free to promise with anyone, free to determine the type and form of the agreement, free also to decide what kind of content and conditions to be included including other forms of freedom related to the agreement as long as it does not violate the laws and regulations. So, by using standard clauses in an agreement with consumers, the real freedom left for consumers is "take it or leave it". If they object to the clause in the agreement, the consumer is allowed to not enter into the agreement.

Nowadays, consumers are usually asked to fill in their personal data, especially in application-based systems such as e-Commerce and Fintech. This personal data is indeed important to obtain so that the identity of the user who uses the application can be known. Especially in e-commerce, of course, identity is needed such as name, address, and telephone number for the purpose of shipping goods. But it is not uncommon for business actors to ask for personal data that is not too relevant to the activities related to the application. This huge amount of personal data belonging to consumers then becomes a target for certain parties. This then opens up opportunities for forms of abuse of consumer personal data such as illegal personal data transactions, embezzling customer accounts, personal data that is accidentally or intentionally leaked, fraud, advertising spam to pornography.

The obligation to provide data requested by businesses is a dilemma, as it often puts consumers in a position where they have no choice but to fill in or provide their personal data. Because if they do not provide or fill in personal data, the transaction they need cannot take place. Meanwhile, there is no option to negotiate this. Pressured by necessity, consumers then inevitably fill in the data. The only solution to this challenge is that business actors must be able to guarantee that consumers' personal data is in safe hands and free from misuse or leakage. This means that enforcement of the PDP Law plays an important role. In the author's opinion, it would be better if the PDP Law also prohibits the use of standard clauses that 'force' potential consumers to include things that are not relevant to the activities carried out.

The second challenge is regarding the special authorized institution. The challenge is institutional. Currently, Indonesia does not have a special institution whose duties and functions cover the issues and implementation of personal data protection. In fact, the existence of a special institution that will focus on enforcing the rules regarding personal data is important. This is because what is included in

²⁷ Lidia Febrianti, Thamrin S, and Puti Mayang Seruni, "Standard Clauses in Employment Agreement Based on the Freedom of Contract Principle," *JCH (Jurnal Cendekia Hukum)* 8, no. September (2022): 18–29.

personal data are facts, confidential information related to personal opinions and communications that the owner wants to keep and protect it from other parties.²⁸ This institutional matter has been mandated with instructions for its establishment in the PDP Law. The implementation of personal data protection as mandated by this law is carried out by an institution established by the president and will be directly responsible to the president. This means that the PDP Law requires a special institution that is responsible as a regulator, supervisor, law enforcer and dispute resolution related to personal data protection in Indonesia. However, issues related to the position and structure of the institution and the authority granted to this institution have not been further regulated.

4. CONCLUSION

As per Article 28 G, paragraph 1 of the 1945 Constitution, the right to personal data is the most recent advancement in personal protection. Prior to the PDP Law, Indonesia's protection of personal data rights was governed by a number of independent regulations, such as "Human Rights Law, EIT Law, Government Regulation on the Implementation of Electronic Systems and Transactions, Population Administration Law, Health Law, Telecommunications Law, Public Information Disclosure Law, Minister of Communication and Information Technology Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems and OJK Regulation Number 77/POJK.01/2016 concerning Information Technology-Based Money Lending-Borrowing Services". Until finally in 2022 Indonesia finally has a special law that covers the protection of personal data, namely the PDP Law. The PDP Law regulates many important points and clearly defines personal data, from subjects, rights and obligations of the parties concerned, institutions to regulating threats in the form of administrative and criminal sanctions. The enactment of PDP Law is a new point of efforts in facing challenges regarding personal data protection, especially for consumers. These challenges include low public awareness of the importance of personal data protection, the existence of standard clauses that are commonly used, and the unclear establishment of specialized institutions in the field of personal data protection.

REFERENCES

- Afnesia, Utari, and Rahmi Ayunda. "Perlindungan Data Diri Peminjam Dalam Transaksi Pinjaman Online: Kajian Perspektif Perlindungan Konsumen Di Indonesia." *Jurnal Komunitas Yustisia* 4, no. 3 (2021). <https://doi.org/https://doi.org/10.23887/jatayu.v4i3.43743>.
- Amiruddin, and Zainal Asikin. *Pengantar Metode Penelitian Hukum*. 10th ed.

²⁸ Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia," *Kanun Jurnal Ilmu Hukum* 20, no. 2 (August 18, 2018): 369–84, <https://doi.org/10.24815/kanun.v20i2.11159>.

- Jakarta: Raja Grafindo, 2018.
- Butarbutar, Russel. "Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia." In *3rd International Conference on Law and Governance (ICLAVE 2019)*, 154–63. Atlantis Press, 2020. <https://doi.org/10.2991/aebmr.k.200321.020>.
- Fathur, Muhammad. "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen." In *National Conference on Law Studies (NCOLS)*, 2:43–60. Universitas Pembangunan Nasional Veteran Jakarta, 2020. <https://conference.upnvj.ac.id/index.php/ncols/article/view/1345>.
- Febrianti, Lidia, Thamrin S, and Puti Mayang Seruni. "Standard Clauses in Employment Agreement Based on the Freedom of Contract Principle." *JCH (Jurnal Cendekia Hukum)* 8, no. September (2022): 18–29.
- Friedman, Lawrence M. *Sistem Hukum Perspektif Ilmu Sosial*. Bandung: Penerbit Nusa Media, 2009.
- Furqania, Mriya Afifah, and Ahmad Sholikhin Ruslie. "Tanggung Gugat Pemerintah Dalam Perlindungan Data Pribadi." *Bureaucracy Journal* 3, no. 1 (2022): 482–93. <https://doi.org/https://doi.org/10.53363/bureau.v3i1.195>.
- Gashami, Jean Pierre Guy, Christian Fernando Libaque-Saenz, and Younghoon Chang. "Social-Media-Based Risk Communication for Data Co-Security on the Cloud." *Industrial Management and Data Systems* 120, no. 3 (March 22, 2020): 442–63. <https://doi.org/10.1108/IMDS-03-2019-0131>.
- Kurniawati, Husni, and Yunanto Yunanto. "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur Dalam Aktivitas Pinjaman Online." *Jurnal Ius Constituendum* 7, no. 1 (2022): 102–14. <https://doi.org/http://dx.doi.org/10.26623/jic.v7i1.4290>.
- Kusuma, Aditama Candra, and Ayu Diah Rahmani. "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)." *Supremasi: Jurnal Hukum* 5, no. 1 (October 4, 2022): 46–63. <https://doi.org/10.36441/supremasi.v5i1.721>.
- Martanti, Gelora. "Perlindungan Konsumen Bagi Penyandang Disabilitas Pada Sektor Perdagangan Online Berbasis Aplikasi Marketplace." *Jurnal USM Law Review* 6, no. 1 (2023): 242–59. <https://doi.org/http://dx.doi.org/10.26623/julr.v6i1.6387>.
- Muaziz, Muhamad Hasan, and Achmad Busro. "Pengaturan Klausula Baku Dalam Hukum Perjanjian Untuk Mencapai Keadilan Berkontrak." *Jurnal Law Reform* 11, no. 1 (2015): 74–84. <https://doi.org/https://dx.doi.org/10.14710/lr.v11i1.15757>.
- Muhammad, Faiz Emery, and Beniharmoni Harefa. "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phising Berbasis Web." *Jurnal USM Law Review* 6, no. 1 (April 24, 2023): 226. <https://doi.org/10.26623/julr.v6i1.6649>.
- Niffari, Hanifan. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)." *Selisik: Jurnal Hukum Dan Bisnis* 7, no. 1 (2020): 105–20. <https://doi.org/https://doi.org/10.35814/selisik.v6i1.1699>.
- Pratiwi, Dinda, and Rianda Dirkareshza. "Pengelabuan Informasi Harga Di E-Commerce Terhadap Konsumen Melalui Flash Sale." *Jurnal Ius Constituendum* 8, no. 3 (2023): 406–23.

- <https://doi.org/http://dx.doi.org/10.26623/jic.v8i3.7344>.
- Rahman, Faiz, and Dian Agung Wicaksono. "Researching References on Interpretation of Personal Data in the Indonesian Constitution." *Jurnal Penelitian Hukum De Jure* 21, no. 2 (June 24, 2021): 187. <https://doi.org/10.30641/dejure.2021.v21.187-200>.
- Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia." *Kanun Jurnal Ilmu Hukum* 20, no. 2 (August 18, 2018): 369–84. <https://doi.org/10.24815/kanun.v20i2.11159>.
- Sinaga, Erlina Maria Christin, and Mery Christian Putri. "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 2 (August 27, 2020): 237. <https://doi.org/10.33331/rechtsvinding.v9i2.428>.
- Soekanto, Soerjono. *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*. Jakarta: PT. Raja Grafindo Persada, 2008.
- Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers, 2010.
- Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma. "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia." *Journal of Financial Crime* 29, no. 4 (September 30, 2022): 1443–57. <https://doi.org/10.1108/JFC-09-2021-0193>.
- Widiatama, Hadi Mahmud, and Suparwi. "Ideologi Pancasila Sebagai Dasar Membangun Negara Hukum Indonesia." *Jurnal USM Law Review* 3, no. 2 (2020): 310–27. <https://doi.org/http://dx.doi.org/10.26623/julr.v3i2.2774>.
- Widyantari, Padma, and Adi Sulistiyono. "Pelaksanaan Harmonisasi Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP)." *Jurnal Privat Law* 8, no. 1 (2020): 117–23. <https://doi.org/https://doi.org/10.20961/privat.v8i1.40384>.