



LEGAL REVIEW OF CONSUMER LAW PROTECTION ON PERSONAL DATA ON DIGITAL PLATFORM

Arfi Azhari

Faculty of Law, University of Tarumanagara,
arfiazhari11@gmail.com

Submitted: December 22, 2020; Reviewed: January 18, 2021; Accepted: March 22, 2021
DOI: 10.25041/iplr.v2i1.2189

Abstract

Legal protection for consumers must be considered because the existence of consumers is prone to fraud. Personal consumer data protect one form of legal protection for consumers in conducting transactions with business actors, both domestic and foreign transactions. With the times at this time, consumer data that exists on business actors, both in the form of state-owned enterprises or business actors in the private form, is a lot of consumer data that these business actors trade and this consumer data is widely known. The problem studied is how the consumer's legal protection of personal data on digital platforms. Research methods are using normative research methods, namely by explaining the issues and views of consumer legal protection of personal data on existing legal regulatory, digital platforms. The results illustrate that for now, consumer legal protection of personal data on digital platforms still refers to several laws and regulations in Indonesia. The government is also preparing a Draft Law on Personal Data Protection, which will become *lex specialis*. For the protection of personal consumer data in Indonesia related to personal data on digital platforms.

Keywords: Consumer Legal Protection, Personal Data, Digital Platform.

A. Introduction

The development of the world at this time has been increasing fast; the sources of information, data, and social life have greatly changed where in this era, humans have entered the postmodern era.¹ This post-modern era is a continuation of the existing modern era. In this post-modern era, it is changing the way humans digitally manage data. The digital revolution has created a new discovery to obtain, store, manipulate, and transmit data volumes in real-time, vast and complex. Therefore the digital revolution is often considered synonymous with the data revolution. These developments have encouraged the collection of a variety of data, no longer depending on considering what data might be useful in the future. However, almost all the data is collected. The government and the private sector are competing to increase their data storage capacity. They are doing data deletion less and less frequently. They find new value in data, so data is needed just like any tangible asset. This new era of data management is commonly referred to as Big Data.²

¹ Johan Setiawan, Ajat Sudrajat, "Pemikiran Postmodernisme dan Pandangannya Terhadap Ilmu Pengetahuan", *Jurnal Filsafat* 28, no. 1 (2018): 25-46, 25, DOI: 10.22146/jf.33296

² P. Malik, "Governing Big Data: Principles and Practices", *IBM Journal of Research and Development* 57, no. 1 (2013): 1-13, 1, DOI: 10.1147/JRD.2013.2241359.

The concept of personal data protection in Indonesia, which adheres to its own civil law system, is based on the 1945 Constitution of the Republic of Indonesia.³ Personal data protection is based on Human Rights (HAM), namely in Article 28F, which states that everyone has the right to communicate and obtain information. To develop the personal and social environment and the right to seek, obtain, own, store, process and convey information using all types of channels available.⁴ And also, Article 28G paragraph 1 of the 1945 Constitution of the Republic of Indonesia states that every person has the right to protection of personal, family, honour, dignity and property under their control, and is entitled to a sense of security and protection from threats of fear for the organization or not The principle of something that is a human right.⁵ Under the Constitution of the Republic of Indonesia, several laws regulate personal data, including Law Number 39 of 1999 concerning Human Rights, Law Number 36 of 1999 concerning Telecommunications, Law Number 14 of 2008 concerning Public Information Disclosure, Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 23 of 2014 concerning Population Administration, Law Number 10 of 1998 concerning Banking, Act Number 8 of 1999 concerning Consumer Protection, Regulation Of The Minister Of Communication And Informatics Republic Of Indonesia Number 20 Of 2016 About Protection Of Personal Data In Electronic Systems and Draft Law on Protection of Personal Data.⁶

Meanwhile, the protection of personal data that developed in Europe, which mostly adhered to the common law system, was originally contained in Article 8 of the European Convention.⁷ The right to data protection itself aims to protect individuals in the information society era. The country that first passed data protection laws was Germany in 1970, followed by Britain, Sweden, France, Switzerland and Austria. Similar developments also surfaced in the United States, with the Fair Credit Reporting Act of 1970, which also contained data protection elements.⁸

Based on the background description, the problem to be examined is how consumer legal protection for personal data on digital platforms, considering that in Indonesia there is no personal data protection law that specifically regulates and this causes a legal vacuum and also the absence of legal certainty to overcome legal problems related to personal data of Indonesian society. Therefore the author is interested to make a journal with the title Legal Protection Consumers of Personal Data on Digital Platforms.

Legal research is a form of scientific activity, which is based on methods, systematics, and certain thoughts, which aim to study one or several phenomena of certain laws by analyzing them. Besides that, there is also an in-depth examination of a legal factor, to then seek a solution to the problems that arise in the symptoms concerned.⁹ The type of research that the writer uses is normative legal research. Normative legal research is legal research that places law as a norm

³ Sinta Dewi Rosadi, Garry Gumelar Pratama, "Perlindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia", *Veritas et Justitia VeJ* 4, no. 1 (2018): 88-110, 95, DOI: 10.25123/vej.2916.

⁴ A. Muhammad Asrun, "Hak Asasi Manusia Dalam Kerangka Cita Negara Hukum (Catatan Perjuangan Di Mahkamah Konstitusi)", *Jurnal Cita Hukum* 4, no.1 (2016): 133-154, 136, DOI: 10.15408/jch.v4i1.3200.2016.4.1.133-154 136.

⁵ Saldi Isra, "Peran Mahkamah Konstitusi Dalam Penguatan Hak Asasi Manusia Di Indonesia", *Jurnal Konstitusi* 11, no. 3 (2014): 109-427, 415, DOI: 10.31078/jk%25x.

⁶ Siti Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia", *JURNAL BECOSS (Business Economic, Communication, and Social Sciences)* 1, no.1 (2019): 147-154, 152, DOI: 10.21512/becossjournal.v1i1.6030.

⁷ Erlina Maria Chris n Sinaga, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0", *Jurnal RechtsVinding* 9, no. 2 (2020): 237-256, 245, DOI: 10.33331/rechtsvinding.v9i2.428.

⁸ Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum", *JATISWARA* 34, no. 3 (2019): 239-249, 245, DOI: 10.29303/jatiswara.v34i3.218.

⁹ Soerjono Soekanto, *Pengantar Penelitian Hukum*, Cetakan ke-3, (Jakarta: UI Press, 1986), 43.

system building. The norm system in question is about the principles, norms, rules of legislation, court decisions, agreements and doctrines (teachings).¹⁰

B. Discussion

1. Consumer Legal Protection of Personal Data on the Digital Platform

Before discussing the legal protection of personal consumer data in Indonesia, the author will discuss the legal protection of personal data in Europe, where the concept of protection in Europe can be copied into the Bill on the Protection of Personal Data. Protection of personal consumer data in Europe using the common law system can be seen from the previous judge's decision where the common law system is based on jurisprudence. The common law is judge-made law. It's the total sum of all the cases decided by appellate courts in that state. The illinois common law is made up of all cases decided by illinois appellate courts. Two hundred years ago, almost all of the law was common law. Today, common law is still predominates in tort, contract, and agency law, and it is very important in property, employment, and some other areas.¹¹

The term personal data protection in the world varies, such as in the United States, Canada and Australia using the term personally identifiable information (PII), while in Indonesia, the term personal data (personal data) is used. between the common law system and the civil law legal system. The common law does not have a special instrument that rigidly interprets the meaning of personal data, but they provide three opportunities for an approach to describe the term, namely by using a tautological approach, a non-public (non-public approach) and a special approach (specific type approach).¹²

For example, like the United States, which adheres to a common law system of law, the United States has a long history of providing guarantees of privacy protection through initiatives in the number of policies that they implement, such as the Privacy Act 1974¹³, issued by the United States Congress. In particular, there is no national law that comprehensively regulates the management and use of personal data. Still, this concept has been mixed up with a number of federal laws and other regulations that often overlap, coincide or even conflict with one another.

In connection with the Privacy Act 1974, this instrument only contains provisions limiting the collection and use of personal information to federal agencies. In other words, this law does not apply to the collection and use of personal data by private parties.¹⁴ In principle, this law prohibits either from a private or governmental nature from opening any records relating to a person's personal data without the permission of the data holder concerned if this is not related to an examination of the law.¹⁵

In Europe, significant development of data protection law occurred when the European Union unified its data protection law through the General Data Protection Regulation of the

¹⁰ Mukti Fajar ND dan Yulianto Achmad, *Dualisme Penelitian Hukum Normatif dan Empiris*, Cetakan ke-1. (Yogyakarta: Pustaka Belajar, 2010), 34.

¹¹ Beatty, Samuelson and Abril, *Standard Edition Business Law And The Legal Environment*, (Boston: Cengage, 2017), 87.

¹² Shinta Dewi Rosadi, *CyberLaw: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional*, (Bandung: Widya Padjajaran, 2009), 71.

¹³ <https://www.justice.gov/opcl/privacy-act-1974>, accessed on October 21, 2020.

¹⁴ Thomas J. Smedinghoff (ed), *Online law: The SPA's Legal Guide to Doing Business on The Internet*, (Reading: Addison Wesley Developers Press, 1996), 273.

¹⁵ Edmon Makarim, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*, (Jakarta: RajaGrafindo Persada, 2005), 174.

European Union (EU GDPR), in 2016, and came into effect on 25 May 2018.¹⁶ The GDPR is comprehensive, covering almost all processing of personal data.¹⁷ In addition, its implementation will affect not only data controllers and processors based in the European Union but also those who offer goods or services to or monitor individual EU citizens' behaviour. As a national law, as of January 2018, at least more than 100 countries have adopted data protection laws. The structure of data protection laws generally includes:¹⁸

- a. The scope of data protection, including the scope of data controllers and processors, and territorial/jurisdictional coverage;
- b. Definition and types of personal data;
- c. Principles of data protection, including reasons for data processing;
- d. Obligations of data controllers and processors;
- e. The rights of the data owner (data subject); and
- f. Supervision and enforcement of laws are generally equipped with an independent supervisory authority (data protection authority).

In general, data protection refers to the practice, protection, and binding rules that are put in place to protect personal information and ensure that data subjects continue to control the information. In short, the data owner should be able to decide whether or not to share some information, who has access, for how long, for what reasons, and be able to modify some of this information, etc. Meanwhile, personal data when referring to the EU GDPR is: "Any information related to a person (data subject) who can recognize or can be recognized; identify directly or indirectly a person, especially by reference to an identifier such as name, identification number, location data, online identifying data or to one or more factors about the person's physical, psychological, genetic, mental, economic or social identity".¹⁹ Personal data is generally divided into two categories: General Personal Data, such as: Name, address, e-mail address, location data, IP address, web cookies; and Specific Personal Data (Sensitive), such as: race, ethnicity, religion, political views, sexual orientation, genetics, biometrics, mental and psychological conditions, criminal records.

Data protection laws should apply to automated data and automated data processing, and structured formats for storing manual data (filing systems). This means that the law must cover all data processing on computers, telephones, IoT devices, as well as paper records. He also reaches out to the public (government) and private institutions. As for individuals, it is widely accepted that processing for individual or household purposes is exempted from the law's enactment. In general, data protection laws also consider that data moves across borders, which often creates jurisdictional issues, including the possibility of conflicting applicable national laws. The law must put individuals at the center, which means ensuring that personal data is protected, regardless of whether their data is processed within or outside the territory in which they are located (extraterritorial scope). With this outreach, the transfer of personal data to entities abroad can only be done if the recipient of the data has a level of data protection that is at least equivalent to the provisions of the sender's national law.

Meanwhile, data protection principles generally emphasize the following points:

¹⁶ C. T. Ungureanu, "Legal Remedies for Personal Data Protection in European Union", *Logos Universality Mentality Education Novelty: Law* 6, no. 2 (2018): 26-47, 27, DOI: 10.18662/lumenlaw/10.

¹⁷ Anja Geller, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law From a European Perspective", *GRUR International* 69, no. 12 (2020): 1191–1203, 1193, DOI: 10.1093/grurint/ikaa136

¹⁸ <https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf>, accessed on February 25, 2021.

¹⁹ Erlina Maria Christin Sinaga, Mery Christian Putri, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0", *Jurnal Rechts Vinding Media Pembinaan Hukum Nasional* 9, no 2 (2020): 1-126, 15, DOI: 10.33331/rechtsvinding.v9i2.428.

Comparison of OECD, APEC, and GDPR

OECD (2013)	APEC (2015)	GDPR (2016)
1. <i>Collection limitation</i>	1. <i>Preventing harm</i>	1. <i>Lawfulness, fairness and transparency</i>
2. <i>Data quality</i>	2. <i>Notice</i>	2. <i>Purpose limitation</i>
3. <i>Purpose specification</i>	3. <i>Collection limitation</i>	3. <i>Data minimization</i>
4. <i>Use limitation</i>	4. <i>Uses of personal information</i>	4. <i>Accuracy</i>
5. <i>Security safeguards</i>	5. <i>Choice</i>	5. <i>Storage limitation</i>
6. <i>Openness</i>	6. <i>Integrity of personal information</i>	6. <i>Integrity and confidentiality</i>
7. <i>Individual participation</i>	7. <i>Security safeguards</i>	7. <i>Accountability</i>
8. <i>Accountability</i>	8. <i>Access and correction</i>	
	9. <i>Accountability</i>	

Data Source From:

<https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf>.

With reference to these principles, processing of personal data can only be carried out if there are a number of legal reasons as follows: there is consent from the data subject; ensure the need for processing for the validity of contracts with data subjects; compliance with legal obligations; protect the vital interests of data subjects or other people; implementation of tasks carried out in the public interest or in the exercise of the official authority granted to the controller (data); or legitimate interest, carried out by the controller or third party unless that interest is overridden by the interests, rights or freedoms of the data subject.

Meanwhile, the obligations for data controllers and processors, in general, must take technical and organizational steps to ensure and demonstrate that their data processing is legally compliant. In detail, their general obligations include: providing up-to-date data audits; comprehensive data protection policies & procedures; privacy by design and by default; data protection officer (DPO); clear procedures for data owners; data protection assessment; capacity building of its staff; strong data security measures; procedures related to violations, recording and reporting violations; assessment procedures to review and update the steps that have been taken. Meanwhile, the rights of data subject consist of: right to information, right of access; the right to correct, block and delete; the right to deny (right to object); the right to data portability; rights associated with automatic profiling and decision making; the right to effective remedy; as well as the right to compensation and accountability.²⁰

The protection of personal consumer data in the civil law legal system can be seen from Indonesia, where personal data protection can be seen from existing laws. In its development, especially after the amendments to the 1945 constitution, the right to privacy, including protection of personal data, is recognized as one of citizens' constitutional rights. This is in line with the inclusion of a special chapter on human rights (bill of rights) in the amended constitution (Chapter XA-Article 28 A-J). Provisions regarding the guarantee of personal data protection can be found in Article 28G paragraph (1) of the 1945 Constitution, which states, "Everyone has the right to protection of personal, family, honour, dignity and property under his control, and has the right to sense. safe and protected from the threat of fear to do or not do something that is a human right."²¹ "Apart from constitutional protection, Indonesia's involvement as a state party to the International Covenant on Civil and Political Rights

²⁰ Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi di Internet Beberapa Penjelasan Kunci*, (Jakarta: Elsam, 2014), 11.

²¹ Constitution of the Republic of Indonesia 1945, Article 28 G paragraph 1.

(ICCPR), which has been ratified by Law no. 12/2005, also affirms the obligation of the Indonesian government to protect the privacy and personal data of its citizens.

This is also in line with Law no. 39/1999 on Human Rights, which in several articles guarantees the protection of citizens' right to privacy, for example, Article 14 (2), Article 29 (1) and Article 31. In general, Article 29 paragraph (1) states the recognition of everyone's rights to protect personal, family, honour, dignity and property rights. This protection is not only in the context of a direct relationship but also for personal information or data. Meanwhile, Article 14 paragraph (2) states that one of the rights to self-development is the right to seek, obtain, store, process and convey information by using all available facilities. This is related to Article 31 of the Human Rights Law which also stipulates that confidentiality in communication through electronic means is guaranteed, except by order of a judge or other legitimate power in accordance with statutory provisions.

At a more specific level, there are also a number of laws and regulations that are currently in force, which relate to or contain material relating to personal data — protection, collection, processing, use, disclosure of personal data. A number of these laws and regulations can be grouped into the following sectors: (i) telecommunications and informatics; (ii) Population and archives; (iii) finance, banking and taxation; (iv) trade and industry; (v) health services; and (vi) security and law enforcement.

In the telecommunications and informatics sector, the regulation regarding the protection of the right to privacy was only related to the confidentiality of a person's personal information and communications, which was realized through the provisions on the prohibition of wiretapping Law No. 36/1999 on Telecommunications. However, in this regulation, telecommunication operators are also given the authority to carry out telecommunication recording on the grounds of proving the correctness of the use of telecommunications facilities at the request of telecommunications service users. Provisions regarding the protection of personal data in the telecommunications and informatics sector or, more broadly in the operation of electronic systems have only emerged with the existence of Law no. 11/2008 concerning Electronic Information and Transactions. Referring to the provisions of Article 26 paragraph (1) of the ITE Law, any transfer of a person's personal data must first obtain permission from the data owner (prohibition of arbitrary transfer of personal data).

If a person's personal data is transferred arbitrarily, the personal data owner can file a claim for compensation to the court (Article 26 paragraph (2)). However, the difficulty of the process of proof in civil courts in Indonesia makes it difficult for the public (data owners) to question the alleged leakage of their personal data legally. As of 2018, only one citizen lawsuit (CLS) has been filed in court. In the Cambridge Analytica case, a group of people sued Facebook for allegedly leaking personal data of Facebook users in Indonesia. In its development, after Mario Costeja's decision at the Court Justice of Europe (CJEU) in 2014²², which gave birth to the clause right to be forgotten, it has also influenced the ITE Law's changes in 2016. In the process of amending this Law, members of the DPR proposed that Indonesia also adopt the concept right to be forgotten. This proposal was then accommodated in Article 26 paragraph (3) of Law no. 19/2016 concerning Amendments to Law no. 11/2008 concerning ITE, which states: "Every Electronic System Operator is obliged to delete irrelevant Electronic Information and / or Electronic Documents which are under its control at the request of the person concerned based on a court order"²³.

Further provisions regarding the elimination of irrelevant information will further be regulated in a Government Regulation (Article 26 paragraph (4)). The formulation above is too

²² Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi di Internet Beberapa Penjelasan Kunci*, (Jakarta: Elsam, 2014), p. 12

²³ Law Number 11 of 2008 concerning Electronic Information and Transactions, Article 26 paragraph 3.

general, with the sole mention of deleting irrelevant Electronic Information and/or Electronic Documents. There is no separate detailed explanation of what is meant by irrelevant information. As a result, it has the potential to collide with several other laws and regulations in their implementation, especially with a number of regulations that guarantee the public's right to information and freedom of expression. For example, the potential tension with Law no. 40 of 1999 concerning the Press, as well as Law no. 14 of 2008 concerning Freedom of Information.²⁴ Meanwhile, in Law no. 14/2008 concerning Openness of Public Information, the protection of public data and information compiled by published public bodies in Article 6 paragraph (3) letter (c) of the KIP Law emphasizes public agencies not to provide public information relating to personal rights. It is also written in point Article 17 letters (g) and (h) which states that authentic personal deeds and one's last will or wills and information relating to personal secrets are stated as exempt information. Information that can reveal personal secrets is related to family members' history and condition, treatment of a person's physical and psychological health, financial condition, income and bank account of a person, and history of formal education and non-formal education units.

Also Based on the Population Administration (Law No. 23/2006), the state has an obligation to store and provide protection for the population's personal data. Therefore, the access rights of Administering officers and Implementing Agencies that collect personal data on residents are obliged to safeguard the information and confidentiality of such data, which is regulated in more detail in Presidential Regulation No. 67 of 2011 concerning National Identity Cards based on National Identity Number. However, this regulation still does not accommodate the protection of residents' personal data (storage and use) in relation to post-scanning and recording of data concerning people's fingerprints and eye retina. While Article 1 point 22 of Law no. 23/2014 (amendments to Law No. 23/2006), recognizes personal data as individual data that must be stored, maintained and its confidentiality is protected. Then in Article 85 of the Population Administration, it is stated that the state has an obligation to store and provide protection for the personal data of these residents. This is also stated in Article 79, which obliges the state to provide protection and appoint the minister as the person in charge of access to citizens' personal data. The problem arises when there are differences in population data classification that "must be protected/kept confidential". There are significant differences between Law No. 23/2006 and its amendments, namely Law No. 24/2013. This situation occurs as a result of the unclear categorization of personal data in Indonesia.

Comparison of the differences between Law No. 23/2006 and its amendments, namely Law No. 24/2013 on the protection of personal data

Personal Data of Residents that Must Be Protected (Sensitive Data)	
Article 84 Law No. 23/2006	Article 84 No. 24/2013
(a) Family Card Number (KK), (b) Identity Number (NIK), (c) Date, month or year of birth, (d) Information regarding physical and/or mental disabilities, (e) Population Identification Number of biological mothers, Father's National Identity Number, and (f) Some contents of important event notes.	(a) Information about physical and/or mental disabilities; (b) Fingerprints; (c) Iris; (d) Signature; and (e) Other data elements which constitute a person's disgrace.

²⁴ <http://elsam.or.id/2016/10/belum-menjawab-tantangan-aktual-revisi-uu-ite-masih-berpotensi-melanggar-kebebasan-berekspresi/>, accessed on October 21, 2020.

Data source from: <https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf>.

Meanwhile, in the context of archiving, it is closely related to the process of state administration activities, one of which is related to the administration of the archiving system by the government and does not include personal data/information, for example, population data, as well as data on teaching staff and students in tertiary institutions. In Article 3 letter (f) No. 43/2009 concerning Archives, it is stated that one of the objectives of archiving is to ensure the safety and security of archives as evidence of accountability in the life of society, nation and state. In addition, this law also regulates the retention period of data/information, which ranges from 10 to 25 years. After a retention period of 25 years, an archive (data/information), whose retention period can be extended, can also be destroyed, or it can also be opened to the public, provided that one of the records does not reveal any confidential or personal data.²⁵

The following are some cases of personal data that occur in Indonesia. The first is the case of the loss of savings from Winda Earl, an eSports athlete at Maybank Indonesia, which caused a stir in the national financial industry. With the loss of money, the Head of the Maybank Cipulir Branch has been named a suspect by the police. The police said that the suspect took Winda's money without the victim's knowledge. The money is transferred to a friend's account for profit, it can be seen here that there is less attention to personal data in this case where an individual can misuse the consumer's personal data from the Maybank bank.²⁶

In addition there is also the case of dentist Eric Priyo Prasetyo (43), The one who lost money amounting to 400 million rupiahs where his bank account was broken after he closed his cellphone number, at which time unscrupulous cell phone operators terrorized his cellphone number. These cases sued cell phone operators with losses. From several examples of these cases, it can be concluded that the personal data protection of consumers in Indonesia is still weak where individuals from the business actors misuse the personal data of consumers. Therefore it is very necessary to have laws and regulations to cover legal events that have been described.²⁷

Third is the case that happened to Ayu (35), who lives in Malang, and lost hundreds of millions of money in her Tabukan, where this case occurred on Sunday, November 22, 2020. On that day, Ayu was called by a person claiming to be from The state-owned enterprise bank, which informed Ayu that she received a cellphone credit of one hundred thousand. After checking, it turned out. The cellphone credit did indeed enter her cellphone number. Still, after that, the person claiming to be from the state-owned enterprise bank asked for a one-time password code Entering Ayu's cellphone, after a few and the phone ended, Ayu realized that what had happened was a fraud, and not long after that a message entered Ayu's cellphone that there was an expense of Rp.49,000,000 million rupiah from her account. This can be seen again by the weak protection of existing personal data.

From several cases that have been mentioned, there is a weak and lack of protection for personal data on digital platforms where data that should be stored is kept secret by business actors, both private companies and state-owned enterprises. As also mentioned in the Regulation of the Minister of Communication and Information Technology of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems Article 2 paragraph 1 which states as follows "Protection of Personal Data in Electronic Systems includes protection of the acquisition, collection, processing, analysis, storage,

²⁵ Law of the Republic of Indonesia No. 43 of 2009 on Archives, Article 66 paragraph 3 letter h.

²⁶ <https://nasional.kompas.com/read/2020/11/27/08454641/kasus-raibnya-uang-winda-earl-di-maybank-pengakuan-tersangka-hingga-dugaan?page=all>, accessed on February 25, 2021.

²⁷ <https://regional.kompas.com/read/2020/10/17/07284531/setelah-menutup-nomor-hp-dokter-gigi-ini-kehilangan-rp-400-juta-di-rekening?page=all>, accessed on February 25, 2021.

appearance, announcement, transmission, dissemination and destruction of Personal Data.²⁸ “Furthermore, the public also has the right to the confidentiality of their personal data. This is stated in Article 26 letter a for the confidentiality of their Personal Data;²⁹ “then in Article 27 letter business actors or parties using personal data must maintain the confidentiality of personal data from their clients or the public, which states as follows “maintaining the confidentiality of the Personal Data they obtain, collect, process and analyze.³⁰ Regulation of the Minister of Communication and Information Technology of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems only states the rights and obligations of owners of personal data (society) and users (Business Actors). Still, there are no penalties for users who misuse people’s personal data.

There is a legal vacuum here, emptiness or vacuum. According to the Big Indonesian Dictionary, “emptiness is a matter (state, nature and so on) empty or void,” which in the legal dictionary is defined as vacuum, which is translated or means the same as “empty or vacant” From this explanation, it is narrowly defined that “legal vacuum” can be interpreted as “a state of emptiness or absence of statutory regulations (laws that regulate (certain) order in society,” so that the legal vacuum in positive law is more accurately described as “legal emptiness. laws or regulations”.³¹

It can be said that the statutory regulations (positive law) that apply to a country at a certain time is a formal system, which of course, is rather difficult to change or revoke even though it is no longer in accordance with the development of society which these laws and regulations must regulate. Law is in a vacuum when the law is still the potential to rule life. When the potential is not empowered or used, the law is still floating in a vacuum. The law has not been bound and has not been attached to be used to regulate or create order. The law that is still in a vacuum has not been able to fulfil its qualifications to fulfill the three objectives of law, namely justice, order and certainty. The purpose of the law is at the same time a gravitational force to bind or attach laws to the social situation. The social situation becomes a vehicle for the law to show its usefulness in achieving legal objectives.³²

To fill the legal void, it is necessary to make laws and regulations that are expected to be effective, the effectiveness of the legislation to be made can be seen from the following criteria:³³

- a. A good description of the situation at hand.
- b. Analyzing these assessments into a hierarchical arrangement. In this way it will be obtained a guideline, whether the use of a means produces something positive, meaning that the use of a means of healing is not worse than the disease.
- c. Verification of the proposed hypothesis ensures the achievement of the desired goals or not.
- d. Measurement of regulatory effects required.
- e. Identification of the factors that will neutralize the bad effects of the required regulations.
- f. Institutionalization of regulations in society, so that the goal of legal reform can be achieved.

The legal objectives that are closer to realistic are legal certainty and legal usefulness. Positivism emphasizes legal certainty, while functionalists prioritize legal benefits, and if it can be argued that “*summum ius, summa injuria, summa lex, summa crux*” which means harsh law can injure, unless justice can help it, thus although justice is not the sole objective of law, the

²⁸ Regulation of the Minister of Communication and Information Technology of the Republic of Indonesia Number 20 of 2016 concerning Personal Data Protection, Article 2 paragraph 1.

²⁹ *Ibid.*, Article 26 point a.

³⁰ *Ibid.*, Article 27 point a.

³¹ Gamal Abdul Nasir, “Kekosongan Hukum & Percepatan Perkembangan Masyarakat”, *Jurnal Hukum Replik* 5, no. 2 (2017): 172-183, 172, DOI: 10.31000/jhr.v5i2.925.

³² Muhammad Syukri Albani Nasution, *Hukum Dalam Pendekatan Filsafat*, (Jakarta: Kencana, 2016), 287.

³³ Adam Podgorecky, *Pendekatan Sosiologi Terhadap Hukum*, (Jakarta: Bina Aksara, 1987), 25.

most substantive objective of law is justice.³⁴ In connection with this theory, the case has been described that there must be legal protection of personal data for the public on digital platforms to guarantee the rights of the public to protect their personal data.

The Banking Law (Law No. 10/1998), regulates, among others, problems related to bank secrecy³⁵ based on the confidential principle, which obliges banks to keep everything related to data and information about customers confidential, both financial situation as well as personal information.³⁶ In Article 1 paragraph (28) of the Banking Law, bank secrecy is interpreted as anything related to depositing customers' information and deposits. Thus, the principles of trust and confidentiality as the basis for financial institutions' performance are also applied in the relationship between the customer and the bank. Customers in storing or using other bank products must provide personal data deemed necessary to the bank.

In the context of trade, apart from talking about electronic transactions, which the ITE Law and PP PSTE regulate, personal data protection is also closely related to Law no. 8/1997 on Documents Company, Law no. 8/1999 concerning Consumer Protection, and Law no. 7/2014 on Trade. Unfortunately, the Consumer Protection Law does not specifically mention the protection of personal data (consumers), as part of consumer rights, which business actors must protect. The Consumer Protection Law emphasizes the availability of accurate information for consumers (related to goods and services), which business actors provide. Even so, the Trade Law does not specifically regulate the obligation to protect personal data (consumers). However, in the provisions of Article 65 paragraph (3) of the law it is emphasized that in trading using an electronic system (e-commerce), every trading actor must fully refer to the applicable provisions of the ITE Law. This means that provisions regarding personal data protection are also binding on every trade that utilizes electronic systems. Therefore, the formation of government regulations regarding trade through an electronic system mandated by Article 66 of the Trade Law should also regulate consumer personal data protection, with reference to existing laws and regulations, especially the ITE Law and the Consumer Protection Law.

The Indonesian government is also preparing a Bill on Personal Data Protection, whose material is to more or less adopt the materials available in the EU GDPR, consisting of 15 Chapters and 74 Articles. This bill regulates from General Provisions, Types of Personal Data, Rights of Personal Data Owners, Processing of Personal Data, Obligations of Personal Data Controllers and Processors in Personal Data Processing, Transfers of Personal Data, Prohibitions on the Use of Personal Data, Establishment of a Code of Conduct for Personal Data Controllers, Exceptions Against Personal Data Protection, Dispute Resolution, International Cooperation, Community Role, Criminal Provisions, Transitional Provisions, and Closing Provisions.³⁷

In this bill, personal data is interpreted as: "any data about a person either identified and / or individually identifiable or combined with other information either directly or indirectly through electronic and/or non-electronic systems". Personal data is divided into two categories: general personal data and specific personal data (sensitive). Unfortunately, this draft does not mention in detail the types of personal data that fall into specific/sensitive qualifications, only said to be determined in accordance with statutory regulations. The application of this law will follow the principle of extra-territorial jurisdiction. It is said in it, "This law applies to every person, public body, business actor, and organization / institution that carries out legal actions as regulated in this law, whether within the jurisdiction of Indonesia or outside the jurisdiction

³⁴ Dominikus Rato, *Filsafat Hukum Mencari, Menemukan dan Memahami Hukum* (Yogyakarta: Laksbang Pressindo, 2010), 59.

³⁵ Yunus Husein, *Rahasia Bank dan Penegakan Hukum* (Jakarta: Pustaka Juanda Tigelima, 2010), 11-13.

³⁶ Djoni S. Gazali dan Rachmadi Usman, *Hukum Perbankan* (Jakarta: Sinar Grafika, 2010), 30.

³⁷ <https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf>, accessed on February 25, 2021.

of Indonesia, which has legal consequences within the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia and is detrimental to Indonesia's interests".³⁸

Data transfer is possible both domestically and abroad, with a number of requirements. If domestically, the data controller and data processor must ensure the protection of such personal data according to the provisions of laws and regulations. Meanwhile, suppose the data transfer is carried out outside Indonesia. In that case, the data controller must first ask for and obtain written consent from the Personal Data Owner to transfer the Personal Data they process to third parties outside Indonesia's jurisdiction. In addition, the transfer of personal data abroad is only possible if:

- a. The country or international organization has a level of Personal Data protection equal to or higher than this Act;
- b. There is a contract between the Personal Data Controller and a third party outside the territory of Indonesia with due observance to the aspect of protecting Personal Data; and/or
- c. There are international agreements between countries.³⁹

The Bill also stipulates provisions regarding exceptions in the application of personal data protection. These exceptions apply:

- a. In the interests of national defence and security;
- b. It is necessary for the benefit of the judicial process in accordance with the provisions of laws and regulations;
- c. For state administration and public interest, particularly economical or financial interests;
- d. To enforce the professional code of ethics;
- e. For data aggregates, the processing of which is intended for statistical and scientific research purposes. However, there is no further explanation regarding the limitations and mechanisms in these exceptions, including the absence of a mandate to form technical regulations to regulate exceptions. It just said, "exceptions are implemented only in the context of implementing the provisions of laws and / or international treaties that have been ratified".⁴⁰

The thing that has not been completely regulated in this Bill is the establishment of an independent regulatory body or a commission for the protection of personal data. This supervisory task is instead left to the government, in accordance with their respective sectors, in coordination with the Minister of Communication and Information Technology. This means that the Ministry of Home Affairs will supervise personal data related to population, OJK will monitor personal data related to finance and banking, the Ministry of Health will monitor personal data related to patient medical records, the Ministry of Law and Human Rights will monitor personal data related to passport and other legal data, and so on.

C. Conclusion

Regulation on the protection of personal data in Indonesia in this digital platform is very much needed because considering the progress of the times, where data storage and data processing have used a digital system, there are indeed several laws and regulations that also regulate personal data, but these are just ordinary rules, not a special regulation, and also this data protection is in private regulation no. 20 of 2016 concerning personal data protection, but there are no criminal penalties for individuals who abuse and disseminate personal data of Indonesians on digital platforms. In addition, the Indonesian government has also prepared eight priorities in the development of e-commerce in Indonesia according to Presidential Regulation No. 74/2017 on the Roadmap for the National Electronic-Based Trading System for

³⁸ *Ibid.*, 11.

³⁹ *Ibid.*, 12.

⁴⁰ *Ibid.*

the Year, which includes: incorporation, taxation, consumer protection, education and human resources, communication infrastructure, logistics, cybersecurity. The discussion regarding the protection of personal data is one of the priorities regarding consumer protection. The government is also ready, the Draft Law on Personal Data Protection, which will be a special lex for personal data protection of consumers in Indonesia. There are also criminal sanctions for individuals who misuse and disseminate Indonesian people's personal data on digital platforms.

REFERENCES

A. Journal

- Asrun, A. Muhammad “Hak Asasi Manusia Dalam Kerangka Cita Negara Hukum (Catatan Perjuangan Di Mahkamah Konstitusi)”, *Jurnal Cita Hukum* 4, no.1, 2016: 133-154, DOI: 10.15408/jch.v4i1.3200.2016.4.1.133-154 136.
- Geller, Anja. “How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective”, *GRUR International* 69, no. 12, 2020: 1191–1203, DOI: 10.1093/grurint/ikaa136
- Isra, Saldi. “Peran Mahkamah Konstitusi dalam Penguatan Hak Asasi Manusia di Indonesia”, *Jurnal Konstitusi* 11, no. 3, 2014: 109-427, DOI: 10.31078/jk%25x.
- Malik, P. “Governing Big Data: Principles and Practices”, *IBM Journal of Research and Development* 57, no. 1, 2013: 1-13, DOI: 10.1147/JRD.2013.2241359.
- Nasir, Gamal Abdul. “Kekosongan Hukum & Percepatan Perkembangan Masyarakat”, *Jurnal Hukum Replik* 5, no. 2, 2017: 172-183, DOI: 10.31000/jhr.v5i2.925.
- Priscyllia, Fanny. “Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum”, *JATISWARA* 34, no. 3, 2019: 239-249, DOI: 10.29303/jatiswara.v34i3.218.
- Rosadi, Sinta Dewi., Pratama, Garry Gumelar. “Perlindungan Privasi dan Data Pribadidalam Era Ekonomi Digital di Indonesia”, *Veritas et Justitia VeJ* 4, no. 1, 2018: 88-110, DOI: 10.25123/vej.2916.
- Setiawan, Johan., Sudrajat, Ajat. “Pemikiran Postmodernisme dan Pandangannya Terhadap Ilmu Pengetahuan”, *Jurnal Filsafat* 28, no. 1, 2018: 25-46, DOI: 10.22146/jf.33296
- Sinaga, Erlina Maria Chris. “Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0”, *Jurnal RechtsVinding* 9, no. 2, 2020: 237–256, DOI: 10.33331/rechtsvinding.v9i2.428.
- Sinaga, Erlina Maria Christin., Putri, Mery Christian. “Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0”, *Jurnal Rechts Vinding Media Pembinaan Hukum Nasional* 9, no 2, 2020: 1-126, DOI: 10.33331/rechtsvinding.v9i2.428.
- Ungureanu, C. T. “Legal Remedies for Personal Data Protection in European Union”, *Logos Universality Mentality Education Novelty: Law* 6, no. 2, 2018: 26-47, DOI: 10.18662/lumenlaw/10.
- Yuniarti, Siti. “Perlindungan Hukum Data Pribadi di Indonesia”, *Jurnal BECOSS (Business Economic, Communication, and Social Sciences)* 1, no.1, 2019: 147-154, DOI: 10.21512/becossjournal.v1i1.6030.

B. Books

- Husein, Yunus. *Rahasia Bank dan Penegakan Hukum*. Jakarta: Pustaka Juanda Tigalima, 2010.
- Makarim, Edmon. *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*. Jakarta: PT. Raja Grafindo Persada, 2005.
- ND, Mukti Fajar., Achmad, Yulianto. *Dualisme Penelitian Hukum Normatif dan Empiris*. Cetakan ke-1. Yogyakarta: Pustaka Belajar, 2010.
- Podgorecky, Adam. *Pendekatan Sosiologi Terhadap Hukum*. Jakarta: Bina Aksara, 1987.

- Rato, Dominikus. *Filsafat Hukum Mencari, Menemukan dan Memahami Hukum*. Yogyakarta: Laksbang Pressindo, 2010.
- Rosadi, Shinta Dewi. *CyberLaw: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum*. Bandung: Widya Padjajaran, 2009.
- S. Gazali, Djoni., Usman, Rachmadi. *Hukum Perbankan*. Jakarta: Sinar Grafika, 2010.
- Samuelson., Abril, Beatty. *Standard Edition Business Law and The Legal Environment*, Boston: Cengage, 2017.
- Smedinghoff, J. Thomas, *online law: The SPA's Legal Guide to Doing Business on The Internet*. Reading: Addison Wesley Developers Press, 1996.
- Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Cetakan ke-3 Jakarta: UI, 1986.
- Syukri, Muhammad Albani Nasution. *Hukum Dalam Pendekatan Filsafat*. Jakarta: Kencana, 2016.
- Wahyudi, Djafar., Komarudin, Asep. *Perlindungan Hak Atas Privasi di Internet Beberapa Penjelasan Kunci*. Jakarta: Elsam, 2014.

C. Legislations

- 1945 Constitution of the Republic of Indonesia.
- Law Number 39 of 1999 concerning Human Rights.
- Law Number 36 of 1999 concerning Telecommunication.
- Law Number 14 of 2008 on Freedom of Information.
- Law Number 43 of 2009 concerning Archives.
- Law Number 11 of 2008 concerning Electronic Information and Transactions.
- Law Number 23 of 2014 concerning Population Administration
- Law Number 10 of 1998 concerning Banking.
- Law Number 8 of 1999 concerning Consumer Protection.
- Regulation of the Minister of Communication and Information Technology of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems

D. Internet

- <https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf>, accessed on February 25, 2021.
- <https://www.justice.gov/opcl/privacy-act-1974>, accessed on October 21, 2020.
- <http://elsam.or.id/2016/10/belum-menjawab-tantangan-aktual-revisi-uu-ite-masih-berpotensi-melanggar-kebebasan-berekspresi/>, accessed on October 21, 2020.

