VARIA JUSTICIA

Varia Justicia
Vol. 17 No. 3 (2021) pp. 287-303
pISSN: 1907-3216 | eISSN: 2579-5198

The Importance of Enacting Indonesian Data Protection Law as a Legal Responsibility for Data Leakage

Edelweiss Premaulidiani Putri[1], Aroma Elmina Martha[2*]
[1,2] Faculty of Law, Universitas Islam Indonesia, Yogyakarta, Indonesia
*email: aroma@uii.ac.id

DOI: https://doi.org/10.31603/variajusticia.v17i3.6231

Submitted: October 2021 *Revised: November 2021* *Accepted: December 2021*

Keywords:
Digital Development; Data Leakage; Data Protection and Personal Information

ABSTRACT

The disclosure of digital development and the openness of many online transactions often lead to data leakage. Furthermore, digital development on the one hand, provides benefits to the digital economy and at the same time also led to the new impact or threat to the conventional economy from the aspect of cyber-security vulnerabilities to harm customer information and challenge the concept of privacy. The lack of government consents the data protection against the 1945 Constitution. This study aims to propose accelerating the Indonesian Personal Data Protection Bill by The House of Representative Council (DPR). This study uses a normative juridical method with a statute approach, the data used is secondary data consisting of primary and secondary legal material. The result shows the urgency of designing new regulation prior to tackling the issue on data leakage and maintaining the confidentiality of the personal data of Indonesian citizens. Through the enacting PDP Law will benefit the stakeholders, the data owner and further recognition by other countries.

1. INTRODUCTION

The Indonesian Internet Service Providers Association (APJII) released data on the penetration of internet users in Indonesia on period in 2019-2021 shown in the Figure 1, the data shows that there have the increasing number of internet users has resulted in an increase in cases of data leakage in Indonesia. It was stated that internet user penetration reached 196.71 million people out of Indonesia's total population of around 266.91 million people. This means that technological advances have touched about 73.7% of internet users in Indonesia.

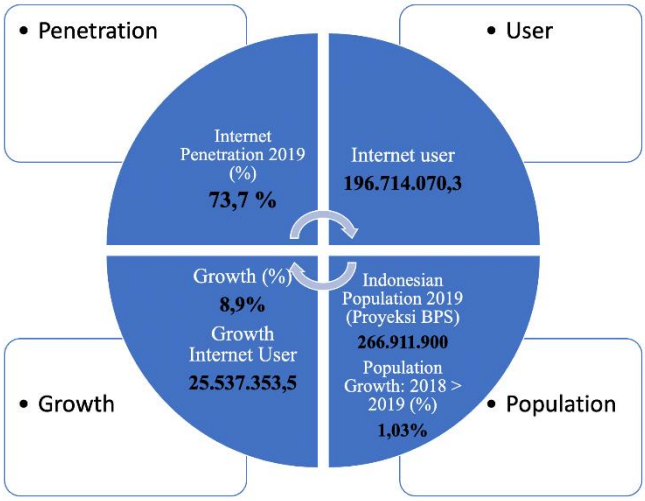

Figure 1. Penetration of Internet User 2019-2020

Source: Survey Results Report issued by the Indonesian Internet Service Providers Association (APJII) in 2019-2020 (Q2)

This technological advancement also brings new cyber-security, data protection threats and problems, which may impact public safety. While this eventually led to the adoption of the first international treaty addressing computer and Internet crime, the Council of Europe's Convention on Cyber-crime, which was adopted in 2001, has three goals: (i) harmonize substantive cybercrime law across borders; (ii) align procedural rules relevant to criminal investigations with a digital component; and (iii) put in place a practical international law enforcement cooperation framework in cybercrime cases.[1]

Then, based on research on the social media management platform Hootsuite and social agencies, found that more than half of the population, which is 64% of Indonesia's population, is connected to the internet. The data, be often utilized by illegal party for the great potentials for data leakage. Furthermore, the data from the Indonesian Consumer Institutions Foundation in 2019, the banking sector lead for the most in data leakage cases, with 106 complaints of data theft cases, followed by 96 cases of online loans, while the insurance sector 21 cases.[2]

These complaints have also increased dramatically at this time, because the use of e-commerce as a shopping platform increases when activity restrictions are carried out, the data shows there are 54 cases of e-commerce data theft from 277 cases during January to June 2020.

Privacy, in general, can be defined by various meanings. According to the Cambridge Dictionary, privacy is defined as the right to keep their personal life or

[1] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime Di Indonesia* (Jakarta: PT. Raja Gafindo persada, 2007).

[2] Ayyi Achmad Hidayah and Shila Ezerli, "Kasus Kebocoran Data Semakin Banyak, Belanja Daring Rentan" (Lokadata.id, 2020), https://lokadata.id/artikel/kasus-kebocoran-data-semakin-banyak-belanja-daring-paling-rentan.

personal information secret. According to Edwin Lawrence Godkin, as quoted by Shinta Dewi, wrote in The Nations Daily about Privacy which he called a suitable individual to have a private life and is someone's honour (personal dignity) that must be maintained as a characteristic of society civil. According to Warren Brandies privacy is the rule to enjoy life and the right to be left alone. This development of the Law was inevitable and demanded legal recognition.[3]

Recently, on May 31, 2021, the government was shocked by the news of the leak of personal data of 279 million Indonesians and sold on raid forums sites for 0.15 Bitcoin (BTC) (or 70-80 million) then the Ministry of Communication and Information Informatics has closed access to download data and blocked the site. The raid forums are detrimental to the digital economy in the midst of the Covid-19 condition in Indonesia. Then it's the same with other cases that happened to Tokopedia which basically harmed consumers, namely the number is estimated at 91 million accounts and 7 million merchant accounts suffered from data leaks hacking so that the accounts were sold at a price of US$5,000 or around Rp. 74 million this is very detrimental to the economy in Indonesia, especially the digital econom.[4]

In practice, in protecting personal data, especially consumers who are active on the internet or user of digital platformly, their privacy rights are protected under the 1945 Constitution (UUD 1945) which was lowered mandates into several regulations, namely Law No. 23 of 2006 as amended by Law No. 24 of 2013 on Population Administration of the Republic of Indonesia (AKRI), Law No. 11 of 2008 as amended by Law No. 19 Tahun 2016 concerning on Information and Electronic Transactions (ITE), Government Regulation Number 71 of 2019 concerning on the Implementation of Electronic Systems and Transactions (PP IEST), Ministerial Ministery of Communication and Informatics Regulation Number 20 of 2016 concerning on Protection of Personal Data in Electronic Systems (PERMEN PDPoES). Meanwhile, in the global scope of personal data protection is regulated through several provisions including the declaration of Human Rights (UDHR), the General Data Protection Regulation (GDPR) of the European Union, International Convention on Civil and Political Rights (ICCPR).

However, the current law is considered to be still not comprehensive and firmly in solving problems related to personal data protection in Indonesia, for this reasons in 2018 through the Ministry of Information, coined to draft the new bill on Personal Data Protection Law. The Personal Data Protection Bill which is certainly expected with the

[3] Wahyudi Djafar, "Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan," *Jurnal Becoss* 1, no. 1 (2019): 147–54.

[4] Andrea Lidwina, "Kebocoran Data Pribadi Yang Terus Berulang" (katadata.co.id, 2021), https://katadata.co.id/ariayudhistira/infografik/60b3bbeda4185/kebocoran-data-pribadi-yang-terus-berulang.

existence of the bill can provide sanctions and can protect the use of Personal Data, there is certainty in dispute resolution and the applicable procedural law.

In some regulations that currently exist the definition of data protection can be interpreted as Indonesian 1945 Constitutional (UUD 1945) article 28G states that each person shall have the right to the protection of their personal selves, families, respect, dignity, and possessions under their control. Afterwards, the legal basis of data protection constituted into the law number 19 of 2016 on Information and Transactions Electronic defined personal data is one part of personal rights. Personal rights have the following meanings:

a. The right to privacy is the right to enjoy a private life and be free from all kinds of interference.
b. Privacy rights are the rights to be able to communicate with other people without spying.
c. Privacy rights are the rights to monitor access to information about a person's personal life and data.

Law Number 23 of 2006 as amended by law 24 of 2013 on Population Administration of Republic Indonesia (AKRI) of 2013, article 1 number 22 personal data is certain data that is stored, maintained, and kept true and kept confidential. “Personal Data” under article 84 of the include:

a. Information regarding any physical or mental condition;
b. Fingerprints;
c. Eye scan;
d. Signature; and
e. Other information considered as shameful (e.g. embarrassing) for any individual.

Personal Data is divided into 2 (two) in PDP :

a. General personal data as referred to in paragraph (1) letter a includes:
   1) Name
   2) Gender
   3) Citizenship
   4) Religion, and/or:
   5) Personal data combined to identify a person
b. The term “personal data of a specific nature” as used in paragraph (1) letter b refers to the following:
   1) Health data and information
   2) Biometric data;
   3) Genetic data;
   4) Sexual life/orientation;
   5) Political views;
      a) Criminal records;

b) Child data;
c) Personal financial data; and/or
d) Other data as defined by applicable legislation

Government regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions emphasized personal data is any data about a person, either directly and/or identifiable directly or in combination with other information, either directly or indirectly through electronic and/or non-electronic. While, the international rsponse to the important of personal data protection according to Universal Declaration of Human Right (UDHR) article 12 states that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protectin of the law against such interference or attacks.

Minister of communication informatic regulation Number 20 of 2016 (PERMEN PDPoES) Article 2 Paragraph (1) Electronic system includes protection against the acquisition, collection, processing, analysis, storage, appearance, announcement, transmission, dissemination, and destruction of personal data. It by means, personal data is certain personal data stored, maintained which truthfulness and confidentiality there of secured and protected, certain individual data means any true and distrinctive information attached and identifiable either directly or indirectly to the reprective individuals which utilization there of shall be in accordance with the laws and regulations.

The EU GDPR personal data means any information related to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, such as a name, an identification number, location data, physical, economic, physiological, genetic, mental, cultural or social identity of that natural person. Furthermore, the International Covenant on Civil and Political Rights (ICCPR) article 17 stated that:

a. No one shall be subjected to arbitrary or unlawfull interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honur and reputation
b. Everyone has the right to the protection of the law against such interference Q attacks.

The birth of the bill on the protection of Personal Data is caused by the increase in digital transactions and the rise of cybercrime, demanding an immediate legal umbrella that protects the use of personal data.

Looking at the provisions of the law above regarding data protection, it is very clear that Indonesia needs a more comprehensive regulation in regulating the protection of personal data, so that the public has the right to know the purpose of using data and deleting data stored by data managers and to prevent data leakage they must be subject to sanctions and fines. This means that the protection of personal data must be protected optimally, and continuously. That the existence of legal certainty can prevent the occurrence of cybercrimes in general, for example Online Gender Based Violence

(KBGO) or misuse of personal data is intended to avoid the threat of cybercrime including KBGO and prevent the misuse of personal data by irresponsible parties as mandated by article 28G paragraph 1 1945 Constitution. In the background above, the author will focus on the protection of personal data. Discussing legal responsibility for data leakage, Negative impact on data leakage, especially in the digital sector which has an impact on economic development in Indonesia.

2. RESEARCH METHOD

This study uses a normative juridical method with a statute approach. The data used is secondary data consisting of primary and secondary legal sources. Primary legal sources consist of the 1945 Constitution, Law No. 23 of 2006 as amended by Law No. 24 of 2013 on Population Administration of the Republic of Indonesia (AKRI), Law No. 11 of 2008 as amended by Law No. 19 Tahun 2016 concerning on Information and Electronic Transactions (ITE), Government Regulation Number 71 of 2019 concerning on the Implementation of Electronic Systems and Transactions (PP IEST), Ministerial Ministery of Communication and Informatics Regulation Number 20 of 2016 concerning on Protection of Personal Data in Electronic Systems (PERMEN PDPoES). Meanwhile, in the global scope of personal data protection is regulated through several provisions including The declaration of Human Rights (UDHR), the General Data Protection Regulation (GDPR) of the European Union, International Convention on Civil and Political Rights (ICCPR). The secondary legal materials are using scientific journals, books, and other related legal documents. The data of research used the library research, which means the author reading, understanding, and finally writing conclusions from legislation, book, journal, news, and articles related to the topic. The method of data analysis using juridical qualitative which comparing the data obtained by the rule of law, convention, and other related regulations for interpreting the issues.

3. RESULT AND DISCUSSION

3.1. The Impact of Data Leakage through Digital Platform in Indonesia

The development of computer-based information communication technology has developed in society, which is everything related to internet access. On the onehand, the existence of the internet in the community certainly makes things easier, more practical, and more efficient. However, on the other hand, it also raises a number of problems including in the legal field. [5] One of them relates to the protection of personal data. Public

[5] B. W Arief, *Mayantara Crime The Development of Cybercrime Studies in Indonesia* (Jakarta: : PT Rajagrafindo Persada, 2007).

interaction through digital, especially in the use of internet access, depends on the availability, integrity and confidentiality of information in cyber space.[6]

The use of social media as a means of cross-country communication. Thus, information technology can be used as an effective medium to influence the public by informing positive opinions. Although, on the other hand, information technology can also be a threat to the nation and state if the use of knowledge and information spread negative content or even for destructive purposes.[7]

Moreover, information technology is currently a "double-edged sword", once the information and technology positively impact the improvement of welfare, progress, and human civilization. Otherwise, it may also be caused Indonesia today, various efforts to protect users' data are separated through several legal instruments mentioned in different laws, as stated in the Ministerial Regulation. In addition, the importance of the government in protecting personal data is to be able to provide security for the public against private data leakage. Also, legal protection of privacy data has been regulated in Law No. 11 of 2008 concerning Information and Electronic Transactions. However, the regulations that have been given to the government are not enough to protect the public's data because the provision on the article does not provide criminal sanctions for the leakage of personal data but only administrative sanctions.[8]

Cases of burglary or data leakage of personal data and information are problematic in Indonesia, here are some examples of cases as shown in the table 1 below:

Table 1. Personal Data Leakage Case in Indonesia

No	Cases	Number of Misuse of data	Year
1.	Personal Data leakage Case	Data leakage reached 1,162 Cases[9]	2017
2.	Personal Data leakage Case	945 Data leakage Cases	2018
3.	Lion Air Group	Estimated 7.8 million passenger data[10]	2018
4.	Tokopedia	Estimated 91 Million user data and 7 million merchant data[11]	2020
5.	Data Pemilu 2014 (KPU)	Estimated 2.3 Million 2014 election data[12]	2020
6.	Pasien Covid	Data leakage about 230K data[13]	2020

[6] Hidayat Chusnul Chotimah, "Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara," *Politica* 10, no. 2 (2019): 113–28.

[7] Rsalinda Elsina Latumahina, "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya," *Jurnal GEMA AKTUALITA* 3, no. 2 (2014): 14–25.

[8] Hidayah and Ezerli, "Kasus Kebocoran Data Semakin Banyak, Belanja Daring Rentan."

[9] Tim detiknet, "Kenapa Kasus Kebocoran Data Selalu Terulang?" (inet.detik.com, 2021), https://inet.detik.com/science/d-5577855/kenapa-kasus-kebocoran-data-selalu-terulang.

[10] Mawa Kresna, "Bagaimana Data Nasabah Kartu Kredit Diperjualbelikan" (Tirto.id, 2019), https://tirto.id/bagaimana-data-nasabah-kartu-kredit-diperjualbelikan-djSv.

[11] Lidwina, "Kebocoran Data Pribadi Yang Terus Berulang."

[12] Tech, "Ini Kronologi Tersebarnya Jutaan Data KPU Yang Bocor" (Cnbcindonesia.com, 2020), https://www.cnbcindonesia.com/tech/20200522141735-37-160286/ini-kronologi-tersebarnya-jutaan-data-kpu-yang-bocor.

[13] Leo Dwi Jatmiko, "Dugaan Kebocoran Data Pasien Covid-19, Aspek Keamanan Data Jadi Sorotan" (Bisnis.com, 2020), https://teknologi.bisnis.com/read/20220107/84/1486379/dugaan-kebocoran-data-pasien-covid-19-aspek-keamanan-data-jadi-sorotan.

7.	BPJS Kesehatan	Data leakage of 279 million user data is traded[14]	2021
8.	BRI Life	Data leakage of 2 million customer data and 463 thousand documents[15]	2021

Digital Forensic Indonesia (DFI) estimated the that third parties have hacked around 7.5 billion personal data of worldwide internet users in the last 15 years.[16] Hundreds of millions of them belong to internet users from Indonesia. Sources of data leaks in all sectors are from malicious outsiders and malicious insiders, accidental data leaks due to unsafe systems (accidental loss), hacktivists, missing gadgets or cellphones, extortion devices (ransomware), and various unknown sources.[17] Hacking of user data can occur if the data protection system on the site is not strict. As a result, personal data can be traded.[18]

The personal data leakage from Indonesian citizens is a serious challenge in term of economic aspect. The state loses reached about IDR. 600 trillion experiences by BPJS. From the case that happened, the illegal party subjected to the criminal impose is the hackers due to its responsibility from the loses. Personal information on Indonesian residents can be sold to a number of entities, including companies, law enforcement agencies, and foreign governments, by hackers. A leaked ID card's information can be used to conduct crimes.

Damage to a person's performance can result in a loss of consumers and, as a result, a drop in sales. When current consumers lose faith in a company, they begin to explore for alternatives. This might direct them to a competitor who hasn't suffered a cyber-attack. Potential new clients will be turned off by contaminated Google searches and constant bad press headlines.

Moreover, employee turnover will occur due to a data breach, particularly at the executive level because of the ramifications of the breach, some people will be dismissed. Others will depart due to the anxiety that comes with dealing with a crisis. Blame and tension are often passed down the ranks, resulting in personnel turnover.

[14] Fahmi Ahmad Burhan, "Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600 Triliun" (katadata.co.id, 2021), https://katadata.co.id/desysetyowati/digital/60d58c9c4538a/kebocoran-data-bpjs-kesehatan-disebut-bikin-rugi-negara-rp-600-triliun#:~:text=Teknologi-,Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600,merugikan negara Rp 600 triliun.&text=Warga mengakses aplikasi Badan Penyelenggara,25%2F5%2F2021).

[15] Kompas, "Ini Dugaan Sumber Kebocoran Data 2 Juta Nasabah BRI Life" (kompas.com, 2021), https://tekno.kompas.com/read/2021/07/29/10010027/ini-dugaan-sumber-kebocoran-data-2-juta-nasabah-bri-life?page=all.

[16] Lidwina, "Kebocoran Data Pribadi Yang Terus Berulang."

[17] Mansur and Dikdik M. Arief, "Cyberlaw Aspek Hukum Informasi" (Bandung: PT. Refika Aditama, 2005).

[18] Wahyudi Djafar, *Big Data Dan Pengumpulan Data Skala Besar Di Indonesia: Pengantar Untuk Memahami Tantangan Aktual Perlindungan Hak Atas Privasi (Internet Dan Hak Asasi Manusia)* (Jakarta: Pusdok Elsam, 2017).

In the digital age, personal data ownership is critical. When accessing online services, purchasing things online, creating an email account, scheduling a doctor's appointment, paying taxes, or signing a contract, each individual is asked to provide personal information. These personal data are frequently obtained without the individual's awareness and by firms or agencies that do not engage with that person directly. Their data can then be used without their permission, and for operations that they have not specifically consented to. Consent is an essential component of data privacy in any data sharing activity.[19]

The exponential rise of Indonesia's digital economy emphasizes the importance of enacting legislation to protect data privacy. The digital economy is predicted to contribute USD 100 billion to the national GDP by 2025, making it ASEAN's greatest digital economy power.

This expansion should be complemented with the preservation of personal data privacy. While this may boost trust in the digital economy, it does not appear to have an impact on digital consumer behavior. According to a 2017 Mastel and APJII study, 79 percent of Indonesians object to their personal data being transmitted without their consent, and 98 percent favor the passage of a Personal Data Protection Law (UU PDP). However, in practice, Indonesian customers appear unconcerned about the usage of their personal information. Users fail to read or comprehend the privacy policies of the organizations whose services they use, particularly the terms and conditions relating to the use of their personal data, according to a survey.

3.2. Comparison of Legislation in Data protection in Indonesia and Other Countries

In fact, data protection regulation have been regulated in several laws including: Ministery the 1945 Constitution, law No. 23 of 2006 as amended by law No. 24 of 2013 concerning population Administration of the Republic of Indonesia, Law No. 19 of 2016 concerning electronic Information and Transactions, Government Regulation Number 82 of 2012 as amended by Government Regulation Number 71 of 2019 concerning the implementation of Electronic Systems and Transactions, Minister of communication Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, Declaration of Human Rights, European Union General Data Protection Regulation (GDPR), International Convention on Civil and Political Rights (ICCPR), but this Law has not been effective because there are still overlapping laws and regulations, there is still no clear legal certainty regarding legal responsibility efforts in overcoming cases of data leakage, while the government is currently making efforts which is quite

[19] Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law," *Law, Innovation and Technology* 10, no. 1 (2018): 40–81, https://doi.org/10.1080/17579961.2018.1452176.

good by revising the Law on Information and Electronic Transactions, Government Regulations, Ministerial Regulations and so on.

Personal data protection is also known as grouping based on data sensitivity or called sensitive data. Classification of sensitive data may vary by country. In particular, the GDPR provides special protection against certain types of personal data that are considered sensitive, including information regarding ethnicity, political preferences, religion or beliefs or membership in a trade organization, biometric data for the purpose of identifying a person, health or sex life data or sexual orientation. Such sensitive data is prohibited from processing unless it fulfills a series of requirements that are explicitly stated in the GDPR, including written consent from the data owner and data collection is limited to purposes that have been definitively listed in the GDPR.

Although the personal data protection arrangements in each country may differ, in general the settings refer to the same data protection principles. In general, the data protection regime is inspired by the 1980 OECD Guidelines on Governing the Protection of Privacy and Transborder Flows of Personal Data which applies the first internationally recognized privacy principles. The following Table 2 are the principles in the protection of personal data:

Table 2. Data protection Principle

Principle	Explanation
Storage Limitation Principle	There must be limits to the storage of personal data and such data must be obtained by lawful and fair means and with the knowledge or consent of the data subject.
Data Quality Principle	Personal data must be relevant to the purpose for which it is used, and to the extent necessary for that purpose, must be accurate, complete and kept up to date.
Purpose Specification Principle	The purpose of collecting personal data must be determined no later than the time of data collection and its subsequent use is limited to the fulfillment of that purpose or other purposes that are not suitable and determined for each change of purpose.
Use Limitation Principle	Personal data may not be disclosed, made available or used for purposes other than those specified except: (a) with the consent of the data subject; or (b) by a legal authority.
Security Safeguards Principle	Personal data must be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure of data.
Openness Principle	The existence of an openness policy regarding developments, practices, and policies regarding personal data. Such means must be in place to establish the existence and nature of personal data, and the primary purpose for which it is used, as well as the identity and location of the data controller.
Individual Participation Principle	Individuals are entitled to: a. To obtain from the data controller, or confirm, whether the data controller has related data or not; b. To communicate with them, data relating to them: (i) within a reasonable time;(ii) at a cost, if any;(iii)

	justifiable reasons; and (iv) given in an understandable form; c. Given a reason if the request made under the letters (a) and (b) is rejected, and the refusal can be argued; d. To fight against their related data, and if the resistance is true, to delete the data, correct, complete or change.
Accountability Principle	The data controller shall be responsible for complying with measures that have an impact on the principles mentioned above.

In terms of personal data protection, there are two methods to protect personal data, namely the physical security of personal data itself and through regulations that aim to provide privacy guarantees for the use of personal data.[20] At the regulatory level, currently at least 107 countries have laws protecting personal data. J.B.J.M ten Berge said that one of the principles of the rule of law is the protection of human rights. Arief Shidarta formulated that one of the elements of a rule of law is the recognition, respect, and protection of Human Rights which is rooted in respect for human dignity. As a state of law, Indonesia places the protection of human rights in the constitution, through the addition of Chapter XA of Human Rights. in the Second Amendment of the 1945 Constitution. The provisions in Article 28 letter G of the 1945 Constitution which reads as follows: "Everyone has the right to protect himself, his family, honor, dignity and property under his control, and has the right to a sense of security and protection from threats. fear of doing or not doing something which is a human right", is considered as the constitutional basis for the need for personal data protection. According to Sinta Dewi Rosadi, Article 28 letter G does not explicitly mention privacy and data protection privacy.

Regarding the protection of personal data, Indonesia does not yet have specific rules regarding the protection of personal data at the statutory level. However, based on research conducted by the Institute for Community Studies and Advocacy (ELSAM) there are at least 30 (thirty) statutory provisions governing the obligation to provide personal data protection in Indonesia. The Population Administration Law is one of the provisions that have more specifically regulated the classification of personal data. Originally the scope of personal data according to Law No. 23 of 2006 on Population Administration as amended in Law No. 24 of 2013 (Population Administration Law 2013) are:[21]

a. Family Card Number;
b. ID number;
c. Date/month/year/birth;
d. Information about physical and/or mental disability;

[20] Djafar, *Big Data Dan Pengumpulan Data Skala Besar Di Indonesia: Pengantar Untuk Memahami Tantangan Aktual Perlindungan Hak Atas Privasi (Internet Dan Hak Asasi Manusia)*.

[21] H. Ridwan, *Hukum Administrasi Negara* (Jakarta: Raja Grafindo Perkasa, 2011).

e. Mother's Resident Identity Number;
f. Father's National Identity Number; and
g. Some of the contents of noteworthy events.

Furthermore, the Population Administration Law changes the scope of personal data to:

a. Information on physical and/or mental disabilities;
b. Fingerprint;
c. Iris of the eye;
d. Signature; and
e. Another data element that is someone's disgrace.

However, the Population Administration Law is only limited to regulating. In other words, the Population Administration Law does not regulate in detail the acquisition, processing and storage of personal data.

More specific law regarding the rights of data owners governed by Law no. 11 of 2008 concerning Information and Electronic Transactions which has been amended by Law no. 19 of 2016 (UU ITE). The ITE Law is the basis for the protection of personal data obtained electronically as regulated in Article 26 of the ITE Law. The consent of the data owner is key in the use of a person's personal data, as stated in Article 26 paragraph (1) of the ITE Law, where a violation will result in the export of a person's personal data. the party whose data is used to file a lawsuit in accordance with Article 26 paragraph (2) of the IT Law. The ITE Law also includes the concept of the right to be forgotten through the provisions of Article 26 paragraph (3) which gives the data owner the right to request the deletion of irrelevant personal data from the electronic system operator.

Hoever, the ITE law does not provide a definition of personal data. The term personal data was introduced in legal provisions, including digital government regulations. 18 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP 18/2012), Regulation of the Minister of Information and Digital Communication. 20 of 2016 concerning Protection of Personal Data in Electronic Systems (Permenkoinfo 20/2016). This includes sectoral implementing regulations such as OJK Circular No. 014/SEOJK.07/2014 regarding privacy and security of personal or consumer data (SEOJK 014/2014).

However, because particular legislative tools to safeguard privacy and personal data do not yet exist in Indonesia and are still sectorial, encouraging digital economic development in Indonesia is insufficient. The urgency of responding to concerns of privacy and data protection in the enactment of emerging technology is exacerbated by the lack of sectorial law that addresses the challenges. The following Figure 2 are the current regulations for protecting personal data in Indonesia, which are arranged according to the legal hierarchy of the Act. No. 12 of 2011 concerning the establishment of laws and regulations:

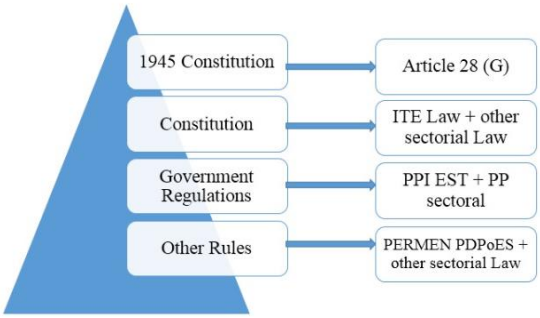

Figure 2. Personal Data protection Regulation in Indonesia

As one of the mandatory implementation provisions of the ITE Law, Government Regulation No 82/2012 stipulates that electronic system operators are responsible for maintaining the integrity of personal data and require the owner's approval. use and disclosure of personal data. However, PP No. 82/2012 does not reflect in more detail the basic principles of personal data protection. A more comprehensive principle of regulation and protection of personal data appears at a lower level of regulation, namely Permenkoinfo No. 20/2016. The scope of personal data protection in electronic systems in Permenkoninfo No. 20/2016 includes protection against the collection, collection, processing, analysis, storage, display, notification, transmission, dissemination, and dissemination, alteration and destruction of personal data. Personal data protection is also regulated in industry-specific implementing regulations such as the protection of consumer personal data regulated by Bank Indonesia and regulations by the Financial Services Authority. As a result, regulations regarding the protection of personal data in Indonesia are still sectoral.

3.3. Accelerating the Enactment of the Personal Data Bill

In the rapid advancement of technological innovations, it is possible to confirm a personal data protection emergency, in which it is easier for people to access personal data without the authorization of the account owner. Such a case may occur due to the lack of law for the protection of personal data. Although the iniciation of creating a new law has been proposed by the government, the bill has been discussed by the House of Representatives (DPR).

According to Utrecht, the law guarantees legal certainty in social interactions. Utrecht's assumption is based on Vanikan's assumption that the law is to protect the interests of each community so that these interests cannot be interfered with (containing considerations that the interests of the community take precedence). it is clear in Utrecht's theory that a good law must look at the social interactions that arise. With the case of data

leakage, the government expects the government to immediately ratify the Personal Data Protection Bill to provide legal benefits for the community.[22]

It can be said that currently there is a personal data protection emergency in the midst of rapid technological developments, therefore the Personal Data Protection Bill must be immediately ratified and promulgated in order to maintain the confidentiality of the personal data of Indonesian citizens. Protection of Indonesian Citizens' Personal Data is a fundamental thing that must be considered because the acceleration of the ratification of the Personal Data Protection Bill can be a solution to be able to manage Indonesian citizens' personal data properly and correctly. So this bill is very important to complete digital transformation in order to get clear legal guarantees against cases of data leakage that arise.

As a result, if the matter is not treated properly, Indonesia's digital economy will also be harmed. For this reason, the government must take steps to avoid the recurrence of data leaking instances and offer legal certainty to those whom incidents of personal data leakage have harm edge. Following the implementation of data protection legislation in European Union countries to reduce data leakage incidents, the digital economy has accelerated. Despite the fact that Indonesia lags behind other nations in enacting data protection rules and regulations, Indonesia must promptly follow suit and ratify the Personal Data Protection Bill as the proper course of action, given the numerous examples of data leakage that have happened in Indonesia.

Several sections of the PDP Bill remained controversial, preventing the bill from becoming law:[23]

a. The proposed PDP Bill gives the government access to personal data.
b. The draft PDP Bill specifies when data owners' authorization is not required to access their data:

a. Defense and security of the country
b. Process for law enforcement
c. Financial Services Sector Supervision
d. monetary order, payment, and financial system stability
e. Interest of the public in the country's administration

When the government requests access to personal data, it must give specific grounds. When it comes to national defence and security, the government must act quickly to gain access to the information. The government also has the right to access personal data in law enforcement processes if the courts grant permission. Allowing the

[22] Gliddheo Algifariyano Riyadi, "Data Privacy in the Indonesian Personal Data Protection Legislation," *Pancanaka* 1, no. 101 (2019): 1–9.

[23] Diana Setiawati, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (2020): 2–9, https://doi.org/10.18196/iclr.2219.

government access to citizens' personal data runs the possibility of the data being utilized for political or even economic purposes. This is unlikely to happen during the present administration, but it does open the door for future regimes to take personal information without their approval.

The PDP Bill regulates a personal data owner's ("PD Owner") rights, to include:

a. Request clarification on identification data, the legal basis for personal data, the aim of requesting and utilizing personal data, and the party requesting personal data's accountability;
b. Before a personal data controller processes it, they must fill in the gaps in their personal data;
c. Access to their personal information in compliance with the rules and regulations in place;
d. In complying with applicable rules and regulations, update data or correct errors/inaccuracies in their personal data;
e. Request that personal data processing be halted, and that personal data be deleted or destroyed;
f. Revoke permission to the processing of personal data provided to a personal data controller previously;
g. Data used to make automated decisions about persons (profiling);
h. Lawsuit and receive compensation for personal data violations in accordance with the law; and
i. Postpone or limit processing of personal data proportionately in line with the purpose of personal data processing.

The relevant stakeholders are expected to benefit directly or indirectly from the PDP Bill's enactment, particularly from the restrictions on the use of personal data and fines for violations of personal data privacy. There is currently no evidence of a PD Controller or Processor being sanctioned for a personal data breach. Once passed, the PDP Bill's provisions should help to clarify personal data protection principles and duties in the event of a data breach. Despite high expectations for what the PDP Bill will accomplish, discussions between the Bill's stakeholders are still ongoing, with a focus on the collection and processing of personal data from outside Indonesian territory, as well as the need to establish an independent body with the authority and ability to oversee personal data protection by private and public entities.

4. CONCLUSION

Based on the descriptions and discussions on the results of the research conducted, several conclusions can be drawn, the regulations regarding the protection of personal data in Indonesia are scattered in several regulations that are still general in nature so that there is no legal certainty. Furthermore, the implementation of the data protection law in

Indonesia which is currently still being discussed in parliament will provide a positive side for Indonesia in terms of digital economic growth, recognition from countries, prevention of cyber violations. Accountability for personal data protection should be subject to administrative sanctions or criminal penalties, then settlement of cases of personal data leakage can be carried out through court/litigation or (non-litigation) channels.

REFERENCES

Ahmad Burhan, Fahmi. "Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600 Triliun." katadata.co.id, 2021. https://katadata.co.id/desysetyowati/digital/60d58c9c4538a/kebocoran-data-bpjs-kesehatan-disebut-bikin-rugi-negara-rp-600-triliun#:~:text=Teknologi-,Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600,merugikan negara Rp 600 triliun.&text=Warga mengakses aplikasi Badan Penyelenggara,25%2F5%2F2021).

Arief, B. W. *Mayantara Crime The Development of Cybercrime Studies in Indonesia*. Jakarta: : PT Rajagrafindo Persada, 2007.

Chotimah, Hidayat Chusnul. "Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara." *Politica* 10, no. 2 (2019): 113–28.

Djafar, Wahyudi. *Big Data Dan Pengumpulan Data Skala Besar Di Indonesia: Pengantar Untuk Memahami Tantangan Aktual Perlindungan Hak Atas Privasi (Internet Dan Hak Asasi Manusia)*. Jakarta: Pusdok Elsam, 2017.

Djafar, Wahyudi. "Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan." *Jurnal Becoss* 1, no. 1 (2019): 147–54.

Dwi Jatmiko, Leo. "Dugaan Kebocoran Data Pasien Covid-19, Aspek Keamanan Data Jadi Sorotan." Bisnis.com, 2020. https://teknologi.bisnis.com/read/20220107/84/1486379/dugaan-kebocoran-data-pasien-covid-19-aspek-keamanan-data-jadi-sorotan.

Hidayah, Ayyi Achmad, and Shila Ezerli. "Kasus Kebocoran Data Semakin Banyak, Belanja Daring Rentan." Lokadata.id, 2020. https://lokadata.id/artikel/kasus-kebocoran-data-semakin-banyak-belanja-daring-paling-rentan.

Kompas. "Ini Dugaan Sumber Kebocoran Data 2 Juta Nasabah BRI Life." kompas.com, 2021. https://tekno.kompas.com/read/2021/07/29/10010027/ini-dugaan-sumber-kebocoran-data-2-juta-nasabah-bri-life?page=all.

Kresna, Mawa. "Bagaimana Data Nasabah Kartu Kredit Diperjualbelikan." Tirto.id, 2019. https://tirto.id/bagaimana-data-nasabah-kartu-kredit-diperjualbelikan-djSv.

Lidwina, Andrea. "Kebocoran Data Pribadi Yang Terus Berulang." katadata.co.id, 2021. https://katadata.co.id/ariayudhistira/infografik/60b3bbeda4185/kebocoran-data-pribadi-yang-terus-berulang.

Mansur, and Dikdik M. Arief. "Cyberlaw Aspek Hukum Informasi." Bandung: PT. Refika Aditama, 2005.

Nawawi Arief, Barda. *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime Di Indonesia*. Jakarta: PT. Raja Gafindo persada, 2007.

Purtova, Nadezhda. "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law." *Law, Innovation and Technology* 10, no. 1 (2018): 40–81. https://doi.org/10.1080/17579961.2018.1452176.

Ridwan, H. *Hukum Administrasi Negara*. Jakarta: Raja Grafindo Perkasa, 2011.

Riyadi, Gliddheo Algifariyano. "Data Privacy in the Indonesian Personal Data Protection Legislation." *Pancanaka* 1, no. 101 (2019): 1–9.

Rsalinda Elsina Latumahina. "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya." *Jurnal GEMA AKTUALITA* 3, no. 2 (2014): 14–25.

Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga. "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (2020): 2–9. https://doi.org/10.18196/iclr.2219.

Tech. "Ini Kronologi Tersebarnya Jutaan Data KPU Yang Bocor." Cnbcindonesia.com, 2020. https://www.cnbcindonesia.com/tech/20200522141735-37-160286/ini-kronologi-tersebarnya-jutaan-data-kpu-yang-bocor.

Tim detiknet. "Kenapa Kasus Kebocoran Data Selalu Terulang?" inet.detik.com, 2021. https://inet.detik.com/science/d-5577855/kenapa-kasus-kebocoran-data-selalu-terulang.