REVIEW OF PERSONAL DATA PROTECTION LEGAL REGULATIONS IN INDONESIA

Safira Widya Attidhira, Yana Sukma Permana
IBLAM College of Law, Jakarta, Indonesia
Jl. Kramat Raya No.25, Senen, Jakarta Pusat
safirattidhira@gmail.com, yanasukma@iblam.ac.id

Received 18 September 2022 • Revised 20 October 2022 • Accepted 28 November 2022

Abstract

The advancement of information and communication technology had caused an increase in data breaches and data misuse. The state is encouraged to have strong law regulations concerning the protection of personal data of its society. This research then aims to explain the lack of legal regulation in Indonesia regarding the protection of personal data. In analyzing the problem, this research used the juridical-normative method (legal research) by oriented on the law principles, law norms, and positive law in Indonesia which is relevant to the research's topic. The conceptual approach was also used in this research because the researcher is more focused on the law regulation that had been issuance. Legal sources were then much used as research data, starting from the Indonesian Constitution to the draft regulation. This research shows that different from Malaysia and Singapore that are already have the Personal Data Protection Act, Indonesia does not yet have a comprehensive personal data protection law. This is because the protection and misuse of personal data in Indonesia are still regulated as sectoral or scattered in several regulations and acts. As a consequence, Indonesia does not have a clear reference for handling the data misuse cases that are happening. This research then gives some advice and recommendations to the government to pass the Draft Regulation on Personal Data Protection which has been discussed since 2016.

Keywords: Data misuse, legal vacuum, personal data protection

INTRODUCTION

The development of technology and information in various aspects of life today has had the impact of social change in a very fast time so that it affects the culture of human behavior in social life,[1] so that more and more community activities use internet media in communicating, shopping, ordering food, ordering motorcycle taxis online, and so on. In carrying out online activities, everyone is usually required to fill in personal data, especially as a condition for registering an application. Therefore, the protection of personal data is increasingly needed to prevent data leakage or misuse. This is because personal data has a close relationship with the concept of privacy, which is an idea to maintain one's dignity and integrity.[2]

The urgency of legal protection of personal data is indeed increasing along with the advancement of the internet. People often complain that their data is misused, or that their identity and privacy are not strictly guarded. In some cases, personal data that is leaked eventually leads to fraud and pornography.[3] The threat of misuse of personal data in Indonesia has also increased after the government implemented an electronic ID card or e-KTP program. This is a program for recording public personal data by the government and launched in 2011. Personal data contained in e-KTP is certainly prone to be misused by several parties, especially if the level of security is weak.[4]

For example, there was once an issue of theft of personal data that was used to apply for an online loan illegally. The victims stated that they never applied for the funds, but suddenly they got a bill. The victim's personal data is also suspected to have been stolen and misused by irresponsible parties. In early 2022, Indonesia even experienced another case of personal data leakage. A number of Covid-19 patient data belonging to the Ministry of Health was found to have been sold on the RaidForum website, including patient medical records from various hospitals. The number of patients who experienced data leaks even reached 6 million people with a data size of 720 GB. Not only that, as many as 160 thousand data on job applicants at Pertamina companies were also leaked and distributed on RaidForum.[5]

Therefore, regulations regarding the protection of personal data are urgently needed to anticipate the threat of misuse and data leakage in various fields, such as the banking industry, electronic-based identity card programs, and online friendship sites including Facebook, Whatsapp, Twitter, and Instagram.[6] The problem is, Indonesia does not yet have a law that specifically regulates the protection and misuse of personal data. This country does recognize that the protection of personal data is part of human rights. However, as the primary source of law in Indonesia, the 1945 Constitution does not explicitly mention the protection of personal data, but only provides recommendations to protect human rights.[7]

This research then argues that the protection of personal data in Indonesia is still weak. Regarding the protection of personal data, it has been regulated in a number of laws and other regulations. However, these laws or regulations are not unified or holistic, but are scattered and separated into various laws. Indonesia also actually has a Personal Data Protection Bill (RUU PDP). However, since it was formulated in 2014, the bill has not been ratified. This delay hinders the process of protecting personal data in Indonesia. As a consequence, there is still a lot of misuse and leakage of personal data because there are no special regulations governing this matter.

This study also compares the legal protection of personal data in Indonesia with neighboring countries. The discussion has indeed been contained in research conducted by Rosadi.[8] However, it was different with Rosadi[9] Focusing on ASEAN countries, this research will compare with the legal regulations on personal data protection in Malaysia, Singapore, and non-ASEAN countries, namely

---

1 Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, Bandung: Refika Aditama, 2005, hlm. 1.

2 Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi di Internet: Beberapa Penjelasan Kunci*, Jakarta: Elsam, 2014, hlm. 2.

3 Muhamad H. Rumlus dan Hanif Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik", *Jurnal HAM*, Vol. 11, No. 2, 2020, hlm. 290.

4 Rosalinda E. Latumahina, "Aspek Hukum Perlindungan Data Pribadi di Dunia Maya", *Jurnal Gema Aktualita*, Vol. 3, No. 2, 2014, hlm. 15.

5 CNN Indonesia, "Kebocoran Data Pribadi yang Tak Berujung di RI", https://www.cnnindonesia.com/teknologi/20220112191045-185-745842/kebocoran-data-pribadi-yang-tak-berujung-di-ri, accessed on 28th May 2022.

6 Dewa G. S. Mangku, et al., "The Personal Data Protection of Internet Users in Indonesia", *Journal of Southwest Jiaotong University*, Vol. 56, No. 1, 2021, hlm. 203.

7 Sinta D. Rosadi, "Protecting Privacy On Personal Data In Digital Economic Era: Legal Framework In Indonesia", *Brwaijaya Law Journal*, Vol. 5, No. 1, 2018, hlm. 145.

8 Ibid.

9 I bid.

Australia. This research also provides recommendations on better legal frameworks and mechanisms to achieve effectiveness in protecting personal data in Indonesia.

METHODS

The research method used is juridical-normative or legal research. Therefore, this research is guided by legal principles, legal norms, and positive law in Indonesia that are relevant to the protection and misuse of personal data. The researcher then tries to find the truth in a coherent manner regarding whether or not legal regulations are in accordance with legal norms, norms (in the form of prohibition orders) with legal principles, and a person's behavior with legal norms or principles. This study also uses a conceptual approach because researchers tend to focus on legal regulations that have been issued. This is because there is no new regulation specifically dealing with issues related to personal data.

The research data used then focuses more on secondary data, such as government documents, books, journal articles, internet articles, and other sources related to the research topic. A number of legal sources are also used, namely (1) primary legal sources such as the 1945 Constitution, laws, government regulations, presidential regulations, and ministerial regulations; (2) secondary sources of law such as draft laws; and (3) tertiary legal materials such as encyclopedias and legal dictionaries. All data that has been collected will then be compiled systematically and analyzed qualitatively.

RESULTS AND DISCUSSION

A. Definition of Personal Data According to Theory and Law

Personal data has various definitions. According to Black's Law Dictionary, personal data is closely related to privacy rights, namely the rights of human freedom and independence that must be protected, including from government intervention or interference regarding personal matters.[10] Personal data protection then refers to the special protection provided by law in the process of collecting, registering, storing, using and disseminating personal data.[11] Meanwhile, in Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, it is stated that, "Personal Data is certain individual data that is stored, maintained, and kept the truth and its confidentiality protected".[12]

In addition, the definition of personal data is also explained in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. This law states that "Personal Data is certain personal data that is stored, maintained, and kept true and its confidentiality protected". Furthermore, what is meant by certain individual data is "every true and real information that is attached and can be identified, either directly or indirectly, on each individual whose utilization is in accordance with the provisions of the legislation".[13]

In the PDP Bill, it is then explained that "Personal Data is any data about a person either identified and/or can be identified separately or combined with other information either directly or indirectly through electronic and/or non-electronic systems". The bill also classifies personal data into general and specific categories. General personal data includes full name, gender, nationality, religion, and/or personal data combined to identify a person. Meanwhile, specific personal data includes health data and information, biometric data, genetic data, sexual life/orientation, political views, crime records, child data, personal financial data, and/or other data in accordance with statutory regulations.[14]

B. Protection of Personal Data in Other Countries

Laws regarding the protection of personal data have been implemented in Indonesia's neighboring countries, including Malaysia, Singapore, and Australia. In Malaysia, there is the Personal

---

[10] Ni G. A. P. Nitayanti dan Ni M. A. Y. Griadhi, "Perlindungan Hukum terhadap Informasi Pribadi terkait *Privacy Right* Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik", https://ojs.unud.ac.id/index.php/Kerthanegara/article/download/10713/7619, downloaded on 14th of December 2021.

[11] Lydia K. Saragih, "Perlindungan Hukum Data Pribadi terhadap Penyalahgunaan Data Pribadi pada Platform Media Sosial", *Jurnal Hukum De'rechtstaat*, Vol. 6, No. 2, hlm. 126-127.

[12] Pasal 1 Ayat (22) Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

[13] Pasal 1 Ayat (2), *Op.Cit.*

[14] Pasal 2 Ayat (3) *Op.Cit.*

Data Protection Act of 2010 which aims to regulate the processing of personal data in commercial transactions. This law gives rights to each individual (Data Subjects) in relation to the collection, use, and/or storage (processing) of their personal data, and places similar obligations on individuals or entities in doing so (Data Users).[15] The cross-border transfer of data is then regulated by stipulating that the transfer of personal data outside Malaysia is not allowed, unless it takes place in a place determined by the Minister of Information, Culture and Communication.[16] In addition, the country of destination must also have an adequate level of protection, or equivalent to the protection of the Personal Data Protection Act. Malaysia then established the Personal Data Protection Department and the Personal Data Protection

Advisory Committee to maintain the effective implementation of the law.

In addition, Singapore also has the Personal Data Protection Act of 2012 which is used to regulate the collection, use and disclosure of data by organizations in ways that recognize the right of individuals to protect their personal data, as well as the need for organizations to collect, use or disclose data. the person for a specific purpose that can be accounted for.[17] This law then establishes a Personal Data Protection Commission which has a variety of comprehensive tasks in providing protection for people's personal data.[18] Not only that, a number of advisory committees were also appointed to provide advice to the Commission in carrying out its duties. This law was then amended on 2 November 2020 to keep the data protection landscape up to date and in line with international standards.[19]

Meanwhile, personal data in Australia is protected by a combination of commonwealth, country and territory legislation. Each of these regulations incorporates a set of privacy principles based on the OECD Principles or the Organization for Economic Co-operation and Development's Guideliness on the Protection of Privacy and Transborder flows of Personal Information.[20] The earliest legislation governing the collection, use, storage and disclosure of personal data was the Privacy Act of 1988. In addition, there are also a number of regulations concerning the protection of personal data, such as the Spam Act 2003, Do Not Call Register Act 2006, and the Data-matching (Assistance and Tax) Act 1990.[21] In Australia's Privacy Act, there are special regulations regarding personal data which are classified into several types, such as employment data; health; finance; telecommunication; decryption assistance; scientific, statistical, and historical research objectives; children; email, internet, and video monitoring; direct marketing and cookies; data analytics; and mobile applications.[22]

C. Personal Data Protection in Indonesia: Comparison with Other Countries

The initiative to provide personal data protection in Indonesia was driven by regulations on human rights under the 1945 Constitution. After that, the protection of personal data was then regulated in a number of laws, namely:

1. Article 40 Paragraph (1) of Law Number 10 of 1998 concerning Banking provides an obligation to banks to keep data and information about their customers confidential;[23]
2. Article 42 Paragraph (1) of Law Number 36 Year 1999 concerning Telecommunications which requires service providers to ensure the security of all information sent or received through telecommunications services or networks;[24]
3. Article 2 of Law Number 8 of 1999 concerning Consumer Protection which explains that consumer protection must be based on the principles of benefit, justice, balance, security and consumer safety, as well as legal certainty;[25]

---

15 Pasal 1 Ayat (2) *The Personal Data Protection Code of Practice*.

16 Herdi Setiawan, Mohammad G. A. Z., dan Dewi A. Mochtar, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi e-Commerce", *Merdeka Law Journal*, Vol. 1, No. 2, 2020, hlm. 106.

17 Pasal 3 *Personal Data Protection Act* 2012.

18 Warren B. Chik, "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy", *Computer Law and Security Review*, Vol. 29, No. 5, 2013, hlm. 564.

19 Singapore – Personal Data Protection (Amendment) Act 2020.

20 David Watts dan Pompeu Cassanovas, "Privacy and Data Protection in Australia: a Critical overview", https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf, downloaded on 17th December 2021.

21 Peter Leonard, "Australian Data Protection and Privacy Laws: A Primer", https://iabaustralia.com.au/wp-content/uploads/2019/08/Australian-Privacy-and-Data-Protection-Law_A-Primer_2019_Peter-Leonard_Data-Synergies.pdf, downloaded 17th December 2021.

22 Ibid.

23 Pasal 40 Ayat (1) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

24 Pasal 42 Ayat (1) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

25 Pasal 2 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

4. Article 21 of Law Number 39 of 1999 concerning Human Rights has recognized that everyone has the right to personal integrity, so that they cannot become objects of research without their consent;[26]
5. Article 6 Paragraph (3) of Law Number 14 of 2008 concerning Openness of Public Information which mentions some information that cannot be submitted to public agencies, one of which is information on personal rights;[27]
6. Article 57 Paragraph (1) of Law Number 36 Year 2009 concerning Health which guarantees the protection of personal data of every patient;[28]
7. Article 84 Paragraphs (1) and (2) of Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration which guarantees the protection of personal data of residents, such as information on physical or mental disabilities, fingerprints , iris, signature, and disgrace;[29]
8. Article 26 Paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) which states that the use of any electronic information related to personal data must be approved of that person;[30]
9. Article 1 Number 1 and 2 of the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems which mentions personal data as a person's identity that is clear and clear, so that it becomes a determination of personal evidence that is maintained, guarded, and placed in a safe manner. safe;[31]
10. Article 1 Number 27 of Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions which states that personal data must be stored, kept true, and kept confidential.[32]

When it comes to personal data protection, the legal regulations in Indonesia are almost the same as in Australia, namely they are sectoral or spread to various regulations. In Australia, the regulations spread across the commonwealth, country and territory levels. Meanwhile, legal protection in Malaysia and Singapore tends to be better than Indonesia. This is because the personal data protection laws in both countries have been regulated in a comprehensive law, namely the Personal Data Protection Act 2010 in Malaysia and the Personal Data Protection Act 2012 in Singapore. Meanwhile, Article 26 Paragraph (1) of the ITE Law has similarities with the contents of the Data Protection Act 2010 in Malaysia. Both regulations seek to ensure that before personal data is collected and processed, there must be prior consent from the subject.[33]

Indonesia has actually prepared a draft law that specifically regulates the protection of personal data (RUU PDP). On January 24, 2020, President Joko Widodo has signed the bill and has entered the Prolegnas Priority 2021. Through the PDP Bill, Indonesia will incorporate all regulations regarding privacy or personal data into the law. The final draft of this law will have 15 Chapters and 72 Articles covering the following topics.

1. Definition and types of personal data;
2. The rights of the owner of personal data;
3. Processing of personal data;
4. Obligations of personal data controllers and personal data processors in processing personal data;
5. Transfer of personal data;
6. Administrative sanctions;
7. Prohibition on the use of personal data;
8. Establishment of a code of conduct for controlling personal data;
9. Dispute settlement and procedural law;

---

[26] Pasal 21 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.
[27] Pasal 6 Ayat (3) Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.
[28] Pasal 57 Ayat (1) Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan.
[29] Pasal 84 Ayat (1) dan (2) Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.
[30] Pasal 26 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
[31] Pasal 1 Nomor 1 dan 2 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.
[32] Pasal 1 Nomor 27 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
[33] Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia", *Kanun Jurnal Ilmu Hukum*, Vol. 20, No. 2, hlm. 378.

10. International cooperation;
11. The role of government and society.[34]

If the PDP Bill is successfully passed, then Indonesia will have regulations that are almost similar to those of Malaysia and Singapore. For example, the PDP Bill has provisions regarding the transfer of personal data abroad, similar to the provisions in the Data Protection Act 2010 in Malaysia. Furthermore, if Malaysia has a Personal Data Protection Department and Singapore has a Commission i Protection of Personal Data, then Indonesia will have the controller and processor of personal data. In this context, the personal data controller is tasked with determining objectives and controls in data processing. They are also required to ensure the accuracy, completeness, consistency, and security of the personal data that has been collected. Meanwhile, the personal data processor is in charge of processing data on behalf of the controller. The data processor then has legal responsibility for any data processing activities performed.[35]

D. Legal loopholes in the implementation of the Personal Data Protection Policy

Existing legal regulations are often unable to work effectively in keeping up with increasingly sophisticated technological developments. There are many legal regulations that run relatively slowly compared to the development of society.[36] This is what happened in Indonesia. The government has indeed included the subject of personal data protection in various regulations. However, the number of regulations does not guarantee that the protection of personal data in Indonesia has been running optimally. On the contrary, the Indonesian government is still weak in providing such protection to its people. This is because the legal regulations regarding the protection of personal data are still sectoral and not yet comprehensive. Indonesia also does not yet have a responsive legal instrument in providing strong protection for people's personal data.[37]

In other words, Indonesia does not have regulations that specifically regulate the protection of personal data. If a case occurs, the regulations used as references tend to be different, but generally the government often refers to the Law on Information and Electronic Transactions (UU ITE). This unclear legal certainty can certainly result in the vulnerability of personal data security. This is also due to the absence of standardization on the principles of personal data protection, thus causing a lack of recognition of the rights of data owners.[38] As a consequence, people's anxiety and concern are increasing because their personal data can be threatened with security.

Moreover, the ITE Law, which is often used as a reference, is actually still insignificant in regulating the protection of personal data. This is because the articles in the law are still in the form of general provisions, and do not explain further about issues that are widely discussed in the international arena.[39] In fact, the ITE Law and Law Number 24 of 2013 concerning Population Administration have contradictory classifications regarding general and sensitive data.[40] This difference can certainly lead to multiple interpretations, even though clear regulations are needed to create legal certainty in society.[41] Due to the unclear regulations governing the protection of personal data, a gap or legal vacuum regarding this matter has occurred in Indonesia.

In addition, the low implementation of personal data protection in Indonesia is also caused by four main factors. First, electronic evidence is sometimes difficult to provide and identify. This is because a number of programs and data that are on a computer can be easily moved, deleted, duplicated, and manipulated.[42] Second, the lack of cyber facilities and infrastructure. In law enforcement offices, the computer facilities used for cyber operations are still limited. Facilities that are more complete are usually only owned by police stations and other law enforcement agencies located in urban areas.[43]

---

[34] Rancangan Undang-Undang Perlindungan Data Pribadi.

[35] Muhammad Firdaus, "A Review of Personal Data Protection Law in Indonesia", https://osf.io/tmnwg/download, downloaded on 17th December 2021.

[36] Sinta Dewi, "Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia", *Yustisia*, Vol. 5, No. 1, 2016, hlm. 27.

[37] Herdi Setiawan, Mohammad G. A. Z., dan Dewi A. Mochtar, *Op.Cit.*, hlm. 106.

[38] Dewa G. S. Mangku, et al., *Op.Cit.,* hlm. 204.

[39] Lia Sautunnida, *Op.Cit.*, hlm. 382.

[40] Gliddheo A. Riyadi, "Data Privacy in the Indonesian Personal Data Protection Legislation", *Policy Brief No. 7,* Maret 2021, Center for Indonesian Policy Studies, hlm. 3.

[41] Pamadi Sarkadi, *Sistem Hukum Indonesia*, Jakarta: Universitas Terbuka, 2007, hlm. 11.

[42] Ranty M. Jhon, "Existence of Criminal Law on Dealing Cyber Crime in Indonesia", *Indonesian Journal of Criminal Law Studies*, Vol. 3, No. 1, hlm. 31.

[43] Mifrakhur R. Habibie dan Isnatul Liviani, "Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Sistem Hukum Indonesia", *Al Qanun: Jurnal Pemikiran dan Pembaharusan Hukum Islam,* Vol. 23, No. 2, 2020, hlm. 421.

Third, law enforcers still have low awareness of cybercrime cases, including in terms of personal data protection. This in turn leads to delays in responding to case reports from the public. They often say that there is no such case, without conducting further investigation. Fourth, public awareness is also still low about the importance of protecting personal data. So if they experience a case involving their personal data, then they just let it go and are reluctant to report it to the authorities.

E. Definition of Misuse of Personal Data and Case Examples

If the legal protection of personal data is still weak, it can cause leakage or misuse of the data. To quote Situmeang,[44] misuse of personal data is an act that has elements of a criminal act, especially theft and fraud. These actions include violations of the law in information technology, and even violations of human rights because personal data has become part of a person's human rights that must be protected. Misuse of personal data can be in the form of online loans, the use of online transportation, and the copying of information and data from the customer's ATM card (skimming).[45]

Misuse of personal data in Indonesia is still common. In the banking sector, irresponsible banks can leak customer information and sell it to other parties. In the health sector, patient data can also be traded for insurance purposes or obtaining assistance from the government. In online transportation, consumers' telephone numbers can also be used to provide threats for giving bad ratings to drivers. While in the online marketplace, the cookie technology used can access consumer personal data, such as communication data, addresses, shopping locations, and shopping preferences.[46]

Here are a number of examples of cases of leakage or misuse of personal data in Indonesia that are widely discussed:

1. Hacking of 91 million user accounts and 7 million merchant accounts on Tokopedia in May 2020 for sale on the darkweb at a price of around Rp. 74 million;[47]
2. Hacking of 13 million user accounts on Bukalapak and sold on a hacker forum called Raid Forum in May 2020;[48]
3. Leakage of 1.2 million user data in Bhinneka in May 2020;[49]
4. Leakage of population data as many as 2.3 million permanent voter list data (DPT) in Yogyakarta in the 2014 election;[50]
5. The alleged leak of 279 population data sold at the Raid Forum in May 2021;[51]

F. Laws Regarding Misuse of Personal Data in Other Countries

In the Personal Data Protection Act 2010 in Malaysia, it is not clearly stated about the law against misuse of personal data. However, the law contains laws against violators or people who do not comply with its provisions. This can be interpreted as misuse of data which is contrary to the provisions in the Personal Data Protection Act 2010. In this law, it is explained that the authorities can search and arrest violators. In fact, a person who damages or loses evidence can be subject to a fine of less than RM 50,000 (approximately IDR 170 million) and/or imprisonment for less than six months.[52] In addition, the authorities or the police may arrest any person believed to have committed or attempted to violate the law. These arrests should be made without delay by bringing the violators

---

44 Sahat M. T. Situmeang, *Op.Cit*., hlm. 39.
45 Ibid.
46 Siti Yuniarti, *Op.Cit.*, hlm. 148.
47 CNN Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual", https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual, accessed on 17th December 2021.
48 CNN Indonesia, "13 Juta Data Bocor Bukalapak Dijual di Forum Hacker", https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker, accessed on 17th December 2021.
49 Roy Franedya, "1,2 Juta Data Pengguna Dikabarkan Bocor, Bhinneka Minta Maaf", https://www.cnbcindonesia.com/tech/20200512164725-37-157971/12-juta-data-pengguna-dikabarkan-bocor-bhinneka-minta-maaf, accessed on 17th December 2021.
50 Riyan Setiawan, "KPU Membenarkan 2,3 Juta Data yang Bocor Merupakan DPT Tahun 2014", https://tirto.id/kpu-membenarkan-23-juta-data-yang-bocor-merupakan-dpt-tahun-2014-fA5B, accessed on 17th December 2021.
51 Roy, "Heboh! Data KTP Hingga Nomor HP 279 Juta Warga RI Bocor?", https://www.cnbcindonesia.com/tech/20210520160626-37-247096/heboh-data-ktp-hingga-nomor-hp-279-juta-warga-ri-bocor, accessed on 17th December 2021.
52 Pasal 113 Ayat (7) Personal Data Protection Act 2010.

to the nearest police station.[53] However, the Personal Data Protection Act 2010 provides exceptions to state and federal governments, as well as data processed entirely outside Malaysia.[54]

Meanwhile, the law regarding data misuse in Singapore is clearly regulated. In Article 26A of the Personal Data Protection Act 2012, it is stated that data misuse is unauthorized access, collection, use, disclosure, copying, modification, or deletion of personal data.[55] After being amended in 2020, the Personal Data Protection Act provides more detailed and strict provisions regarding cases of data misuse. The penalties for perpetrators are becoming more severe, namely fines ranging from S$ 1 million (approximately Rp. 10.5 billion) to S$ 10 million (approximately Rp. 100.5 billion) for perpetrators of incidents of data misuse that cause losses to Singapore.[56] Meanwhile, any person who discloses and misuses another person's data to cause harm to that person, will be subject to a fine of around S$ 5,000 (approximately IDR 52 million) and/or imprisonment for less than two years.[57]

Furthermore, Australia has incorporated the Notifiable Data Breach (NDB) scheme into the Privacy Act on 22 February 2018. This scheme requires a number of organizations governed by the Privacy Act to notify any person who is at risk of becoming a victim of data misuse. This notice must contain recommendations on the steps that should be taken in response to acts of misuse of personal data. The whole process is under the supervision of the Privacy Commissioner who is responsible for resolving complaints for misuse of personal data.[58] In most cases, the Commissioner will endeavor to reconcile the two parties. Apologies to the complainant are punishments that are often obtained through a conciliation process, and are then followed up by the provision of compensation in the amount of less than AU$100,000[59] (approximately IDR 1 billion). However, since March 2014, the Commissioner has had significant new powers, including punishing any perpetrators of serious or repeated data misuse, with a fine of around AU$1.8 million (approximately Rp. 18.4 billion).[60]

G. Laws Regarding the Misuse of Personal Data in Indonesia, and the Problems

Regarding the misuse of data in Indonesia, it has been regulated in various regulations and laws. One of the earliest laws governing this matter was Law Number 36 of 1999 concerning Telecommunications. In this law, it is stated that telecommunications service providers who leak or misuse their consumer data will be subject to a fine of Rp. 200,000,000 and/or imprisonment for a maximum of two years.[61] Sanctions against perpetrators of misuse of personal data are further regulated in the ITE Law, namely:

1. Distributing, sending, and/or accessing information containing insults or defamation will result in a maximum fine of Rp. 750,000,000 and/or imprisonment for a maximum of four years;[62]
2. Distribution, delivery, and/or access of information containing threats or extortion will result in a maximum fine of Rp. 1,000,000,000 and/or imprisonment for a maximum of six years;[63]
3. The distribution, delivery, and/or access of information containing threats of violence or intimidation will result in a maximum fine of Rp. 750,000,000 and/or imprisonment for a maximum of four years.[64]

The act of misuse of personal data is then regulated more fully in the PDP Bill which has been formulated since 2016. In this bill, disputes over the misuse of personal data will be resolved through arbitration, courts, or other alternative institutions. If it is done through a court, then the trial process is carried out in a closed manner in order to protect the privacy of personal data that has been misused.[65] The types of sanctions given are also divided into two categories, namely administrative and criminal sanctions. In giving administrative sanctions, the perpetrators will be given a written warning, personal data processing activities will be suspended temporarily, personal data will be

---

53 Pasal 127 Ayat (1) dan (2) Personal Data Protection Act 2010.
54 Ali Alibeigi dan Abu B. Munir, "Malaysian Personal Data Protection Act, a Mysterious Application", *University of Bologna Law Review*, Vol. 5, Issue 2, 2021, hlm. 366.
55 Pasal 26 A Personal Data Protection Act 2012.
56 Singapore – Personal Data Protection (Amendment) Act 2020.
57 Ibid.
58 David Watts dan Pompeu Casanovas, *Op.Cit.*
59 Peter Leonard, *Op.Cit.*
60 Ibid.
61 Pasal 57 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.
62 Pasal 45 Ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
63 Pasal 45 Ayat (4) *Op.Cit.*
64 Pasal 45B *Op.Cit*.
65 Pasal 56 Rancangan Undang-Undang tentang Perlindungan Data Pribadi.

deleted or destroyed, compensate for the losses that have been caused, and pay administrative fines.[66]

Meanwhile, the criminal sanctions are as follows..

1. The collection or collection of other people's personal data will be subject to a maximum fine of Rp. 50,000,000,000 or imprisonment for a maximum of five years;[67]
2. Disclosure of other people's personal data will be subject to a maximum fine of Rp. 20,000,000,000 or imprisonment for a maximum of two years;[68]
3. The use of other people's personal data will be subject to a maximum fine of Rp. 70,000,000,000,000 or imprisonment for a maximum of seven years;[69]
4. Installation and/or operation of visual data processing equipment in public places so as to threaten the security of personal data will be subject to a maximum fine of Rp. 10,000,000,000 or imprisonment for a maximum of one year;[70]
5. The use of processing tools or visual data processing in public places to identify other people will be subject to a maximum fine of Rp. 10,000,000,000 or imprisonment for a maximum of one year;[71]
6. Falsifying personal data with the aim of providing benefits to oneself or others will be subject to a maximum fine of Rp. 60,000,000,000 or imprisonment for a maximum of six years;[72]
7. Making a sale or purchase of personal data will be subject to a maximum fine of Rp. 50,000,000,000 or imprisonment for a maximum of five years.[73]

Provisions regarding the misuse of personal data are indeed more regulated in the PDP Bill. However, it should be emphasized again that the bill has not yet been ratified, so the regulations cannot be enforced. Meanwhile, other laws and regulations concerning the misuse of personal data still have a number of shortcomings. For example, Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration does provide a complete explanation of the definition and types of personal data. However, the law does not regulate in detail about the acquisition, processing and storage of people's personal data.

In Article 15 of the ITE Law, it has been stated that electronic system operators are required to operate their electronic systems safely, and are ready to take responsibility if problems occur in their operation. Article 15 Paragraph (1) also further explains that reports on data leakage or misuse are deemed invalid after the electronic system operator is able to prove the existence of compelling conditions, or the negligence and error of the user of the electronic system. However, the ITE Law has not yet regulated the provisions for accountability from online marketplaces that are more specific when user data leaks occur.[74] In addition, sanctions and penalties have not been comprehensively regulated, especially sanctions and penalties given to online marketplaces as providers of electronic systems.

Not only that, a number of articles in the ITE Law are still problematic and give rise to multiple interpretations or different interpretations. This can be seen in Article 27 Paragraph (1) regarding violations of decency, and Article 27 Paragraph (3) regarding defamation. The two articles do not provide clear information regarding the types of actions that are classified as violations of decency and defamation.[75] Anyone who is annoyed by another person's words can feel angry and then report it to the authorities, even if the person did not mean to hurt him.

In addition, there is also ambiguity in Article 29 regarding threats of violence and acts of terror. In this article, there is no further explanation regarding actions that are classified as scaring other people. As a consequence, attempts to warn and advise others may be considered an act of fright if the person is frightened. The ambiguity in a number of these articles can certainly have a negative

---

66 Pasal 50 Ayat (2) *Op.Cit*.
67 Pasal 61 Ayat (1) *Op.Cit*.
68 Pasal 61 Ayat (2) *Op.Cit*.
69 Pasal 61 Ayat (3) *Op.Cit*.
70 Pasal 62 *Op.Cit*.
71 Pasal 63 *Op.Cit*.
72 Pasal 64 Ayat (1) *Op.Cit*.
73 Pasal 64 Ayat (2) *Op.Cit*.
74 Maichel Delpiero, et al., "Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban *Online Marketplace* dalam Pelindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data", *Padjajaran Law Review*, Vol. 9, No. 1, 2021, hlm. 14.
75 Yosephus Mainake dan Luthvi F. Nola, "Dampak Pasal-Pasal Multitafsir dalam Undang-Undang tentang Informasi dan Transaksi Elektronik", *Info Singkat: Kajian Singkat terhadap Isu Aktual dan Strategis*, Vol. 12, No. 16, 2020, hlm. 3.

impact, such as limiting people's freedom to express and express their opinions. In fact, many people have been arrested after criticizing the government.

Furthermore, ambiguity can also be seen from Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. In this regulation, it is stated that online marketplaces involved in data leakage cases will be given administrative sanctions, such as fines, termination of access, temporary suspension, written warnings, or being removed from the list. However, the implementation of a number of these sanctions still tends to be weak.[76] This is because the regulation does not yet have specific provisions regarding the classification of data leakage problems. The absence of these provisions can create ambiguity for law enforcers in providing administrative sanctions to online marketplaces.

Weaknesses in legal substance can also be seen from Article 14 Paragraph (5) of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. The article states that if a user's personal data fails to obtain protection or is leaked, the electronic system operator must notify the data owner in written form. However, the problem is, the article does not provide provisions regarding the time of notification. Therefore, if a data leak occurs, the online marketplace can at any time notify its users that their data has been leaked. This causes the notification time to be delayed and data leak cases become difficult to handle.

H. Legal Gap in Law Enforcement in Cases of Misuse of Personal Data in Indonesia

Cases of leakage or misuse of personal data in Indonesia are still common, especially for political and business purposes. The rise of these cases is caused by weak legal protection and supervision. Most government agencies and companies also do not know how to manage and secure the personal data of the public or their consumers. In Indonesia, the most common data leak cases are user data leaks from several online marketplaces. Some of them are the leak of 91 million user data on Tokopedia, the leak of 13 million user data on Bukalapak, and the leak of 1.2 million user data on Bhinneka.

However, the three cases did not undergo further investigation. This is caused by the unclear legal regulations governing data leakage. Most consumers also decided not to take the case to court. This reluctance is caused by the trial process which takes a long time, the process of proving errors or omissions in the online marketplace accompanied by various kinds of electronic evidence, as well as proving consumer losses after their personal data is leaked and misused.[77] Tokopedia only stated that the issue of data leakage did indeed occur, but that financial accounts and password data from consumers were ensured to remain safe. This indicates that regulations containing provisions regarding data misuse are still not running optimally, especially Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. In fact, according to this regulation, Tokopedia is required to submit in writing about cases of data leakage that occurred to its consumers. Written notification must include at least five things, namely:

1. The type or category of personal data that has been leaked;
2. Number of data subjects or consumers who have been affected;
3. The contact of the personal data protection officer who can be contacted;
4. Possible consequences arising from the leakage of personal data;
5. Actions that have been taken by Tokopedia in dealing with the leak case..[78]

In addition, the handling of cases of leakage of 279 million BPJS Health data also tends to be unclear. The Ministry of Communication and Information Technology (Kominfo) has indeed closed the data seller's account. The Ministry has also taken anticipatory steps by cutting off access to three links on the internet, namely anonfiles.com, mega.nz, and bayfiles.com. On October 25, the spokesperson for the Ministry of Communication and Informatics, Dedy Primadi, even stated that the investigation process into the BPJS case had been completed and an official decision would soon be issued.[79]

However, until now, Kominfo has not released the results of the decision, even though the BPJS data leak case occurred in May 2021. This case has shown that the public's personal data, which is vital, cannot be protected and maintained properly by the government. In fact, the Directorate General

---

[76] Maichel Delpiero, et al., *Op.Cit.*, hlm. 15.

[77] Muhammad Fathur, "Tanggung Jawab Tokopedia terhadap Kebocoran Data Pribadi Konsumen", *Paper presented on 2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*, 2020, hlm. 47.

[78] Muhammad Fathur, *Op.Cit.*, hlm. 52.

[79] Novina P. Bestari, "Investigasi Dugaan Data BPJS Kesehatan Bocor Usai, Hasilnya?", https://www.cnbcindonesia.com/tech/20211025134818-37-286329/investigasi-dugaan-data-bpjs-kesehatan-bocor-usai-hasilnya, accessed on 18th December 2021.

of Population and Civil Registration has given private companies access to personal data of residents, such as ID cards and NIK.[80] The government argues that the provision of the data is intended to improve the company's services in the community.

A number of these phenomena indicate that there have been loopholes or legal vacuums in Indonesia, especially in terms of cases of data leakage and misuse. As a consequence, electronic system operators who act as data controllers tend to avoid the obligations assigned to them. In fact, data controllers are required to maintain the personal data security infrastructure of their users, which includes the implementation of encryption and assurance of confidentiality, integrity, and resilience in data processing and services. [81] Legal loopholes or gaps in cases of data misuse in Indonesia can certainly weaken the level of legal certainty. In fact, legal certainty is very necessary because it acts as a judicial protection against the arbitrary actions of other parties.[82]

I. Recommendations and Suggestions

After discussing a number of issues regarding the protection and misuse of personal data in Indonesia, this paper then provides two recommendations and suggestions so that the personal data protection process can run effectively.

1. Legal Needs (Laws) Regarding Personal Data Protection in Indonesia

Legal instruments in Indonesia are still not responsive to the needs of the community in strengthening the protection of their personal data. To be responsive, legal instruments related to personal data protection must meet at least two criteria. First, having an international character or following the development of international trends. This can be done through more detailed arrangements for data transfers abroad. The process requires special government approval, and can only be transferred to countries with a strong level of privacy protection. Second, it becomes the glue element between the individual and the economic community. This means that the protection of personal data also includes the protection of personal rights, in which the fulfillment of these rights must involve the active role of the state.[83]

The government must recognize that the existence of a law on the protection of personal data is a necessity that cannot be postponed any longer. This is because the law is very urgent to fulfill national interests, as well as to facilitate international relations between Indonesia and other countries, especially in facilitating trade, industry, and transnational investment.[84] The existence of a law on the protection of personal data can also realize good governance. In this context, the government needs to support the development of information technology through laws and regulations so that the use of information technology becomes safer. Through the enactment of the law, the government can reduce the potential loss to Indonesia as a result of disturbing the privacy of people's personal data.

The urgency of personal data protection has actually been mandated in the 2005-2025 Long Term Development Plan. This is intended to anticipate the impact of convergence between telecommunications, information technology, and broadcasting. Therefore, Indonesia must establish a good and coordinated information technology legal system to create legal certainty. To quote Rosadi,[85] Legal regulations regarding the protection of personal data must at least include the following.

1. The principle that forms the basis for the formation of laws and regulations must take national and international development into account. This principle should be based on the 1945 Constitution, especially Article 28G which recognizes that the right to privacy of personal data must be protected.
2. The concept of regulation should also take into account the principle of fair use of information (the principle of fairness of information) which requires the existence of a standard of practice, to ensure that entities that collect and use personal data have adequate protection. Such standards have been adopted by many countries, such as the principles of the OECD Guideliness 1980, the EU General Directive 1995, and the APEC Framework 2004.
3. The use of clear definitions of substantial terms, such as the use of the term data or information. In addition, the scope of the regulation must also be clear, the subjects regulated by law must be determined, as well as the need to regulate exceptions in obtaining or

[80] Ririn Aswandi, et al., "Perlindungan Data dan Informasi Pribadi Melalui *Indonesian Data Protection System* (IDPS)", *LEGISLATIF*, Vol. 3, No. 2, hlm. 176-177.
[81] Dewa G. S. Mangku, et al., *Op.Cit.*, hlm. 205.
[82] Sudikno Mertokusumo, *Mengenal Hukum: Suatu Pengantar*, Bandung: Citra Aditya Bakti, 2013, hlm. 160.
[83] Herdi Setiawan, et al., *Op.Cit*., hlm. 106.
[84] Sinta D. Rosadi, *Op.Cit.*, hlm. 149.
[85] Sinta D. Rosadi, *Op.Cit.*, hlm. 150-153.

disclosing personal data of a person in certain cases, such as for national security, national defense, public interest, and legal processes. the judge.

4. Involving certain institutions to implement the law, so that it can run effectively and be able to resolve existing legal issues. This institution is at least divided into two, namely the courts and the information commission. In addition, private institutions are also required to participate in enforcing legal protection of personal data.

2. Legal Needs or Law Enforcement Mechanisms in Cases of Misuse (Leakage) of Personal Data in Indonesia

The effectiveness of law enforcement depends on a number of factors that influence its implementation, namely regulatory factors or the law itself, law enforcement factors, infrastructure or facilities that are able to expedite legal processes, community factors that are included in the scope of regulations, and cultural factors. First, regulations or laws governing the misuse of personal data need to be established. In this regulation, personal data must be clearly defined in order to determine the orientation of the regulation and its application. Classification of personal data is also needed to make processing easier and more efficient. For example, the Personal Data Protection Act 2010 in Malaysia and the Personal Data Protection Act 2012 in Singapore, which includes health data as personal data that has a special nature.[86]

Second, the law enforcement factor. Law enforcement officers need to learn more about the world of cyber or information and communication technology. Therefore, they can identify potential hazards during data processing. The data controller then needs to evaluate the level of danger and assess the vulnerability of the system and its operations, so that cases of data leakage or misuse can be prevented. Third, the factor of facilities or facilities. This factor still needs to be improved because cyber facilities in law enforcement offices are still relatively low. Relatively complete cyber facilities are only owned by police or law enforcement offices in big cities. In order to improve the protection of personal data, the government needs to provide cyber facilities in every law enforcement office that is responsible for the matter.

Fourth, the community factor. The problem that often occurs is that public awareness is still low on the importance of protecting personal data. As a consequence, people are reluctant to report if their personal data is leaked or misused. In order to overcome these problems, the government needs to disseminate information to the public that personal data is important and must be protected. This socialization process is intended to increase public awareness, so that they become more careful in providing or disclosing their personal data. Fifth, cultural factors. The government needs to create a legal culture or legal culture in society, so that people's behavior will be in accordance with applicable legal regulations. This can be done through the provision of socialization and legal training to the community, especially to local or remote communities.

CONCLUSION

There are many laws and regulations regarding the protection and misuse of personal data in Indonesia, such as Law Number 10 of 1998 concerning Banking, Law Number 14 of 2008 concerning Openness of Public Information, Law Number 19 of 2016 concerning Amendments to Laws - Law Number 11 of 2008 concerning Information and Electronic Transactions, Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, Law Number 36 of 1999 concerning Telecommunications, Law Number 36 of 2009 concerning Health, Law Number 39 of 1999 concerning Human Rights, Law Number 8 of 1999 concerning Consumer Protection, Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, and Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions.

However, these regulations are still sectoral in nature or spread into various kinds of regulations. As a consequence, Indonesia does not have a clear legal reference in handling cases involving people's personal data. This is very different from Malaysia and Singapore, which already have comprehensive legal regulations in providing protection for their people's personal data, namely in the form of the Personal Data Protection Act. Indonesia does have a Personal Data Protection Bill. However, although it has been formulated since 2016, the bill has not been ratified until now.

Legal loopholes or vacancies regarding the protection of personal data then lead to more cases of data leakage or misuse in Indonesia. As many as millions of people's personal data in online marketplaces have even been leaked and traded on the dark web. However, the government did not

[86] Faiz Rahman, *Op.Cit.*, hlm. 97.

give proper punishment to the online marketplace, even though they had been negligent in protecting the personal data of millions of consumers. Not only that, hundreds of millions of Indonesian population data also leaked, ranging from ID cards to NIK. This leak caused the government's performance to be increasingly questioned because it was unable to maintain vital population data.
Therefore, this study provides suggestions and recommendations to the government to immediately ratify the PDP Bill. This bill is very urgent to follow up cases of leakage and misuse of personal data that are increasingly rampant, so that the legalization process cannot be delayed any longer. In addition, the government also needs to improve the quality of law enforcers, as well as the cyber facilities in their offices. The process of socialization and legal training also needs to be carried out to the community to increase their awareness, so that a legal culture can be realized. These steps need to be taken by the Indonesian government so that legal protection of personal data can run optimally. The state will no longer feel disadvantaged because cases of data leakage and misuse can be prevented or suppressed to a minimum.

REFERENCES

Book

Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesi*, Bandung: Refika Aditama, 2005.

Pamadi Sarkadi, *Sistem Hukum Indonesia*, Jakarta: Universitas Terbuka, 2007.

Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakkan Hukum*, Jakarta: Rajawali, 1983.

Sudikno Mertokusumo, *Mengenal Hukum: Suatu Pengantar*, Bandung: Citra Aditya Bakti, 2013.

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

Journal Articles

Ali Alibeigi dan Abu B. Munir, "Malaysian Personal Data Protection Act, a Mysterious Application", *University of Bologna Law Review*, Vol. 5, Issue 2, 2021, hlm. 362-374.

Budi K. B. Putra, "Kebijakan Aplikasi Tindak Pidana Siber (*Cyber Crime*) di Indonesia", *Journal of Law*, Vol. 1, No. 1, 2018, hlm. 1-14.

David Watts dan Pompeu Casanovas, "Privacy and Data Protection in Australia: a Critical overview", https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf, downloaded on 17th December 2021.

Dewa G. S. Mangku, et al., "The Personal Data Protection of Internet Users in Indonesia", *Journal of Southwest Jiaotong University*, Vol. 56, No. 1, 2021, hlm. 202-209.

Faiz Rahman, "Kerangka Hukum Perlindungan Data Pribadi dalam Penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia", *Jurnal Legislasi Indonesia*, Vol. 18, No. 1, 2021, hlm. 81-102.

Herdi Setiawan, et al., "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi e-Commerce", *Merdeka Law Journal*, Vol. 1, No. 2, 2020, hlm. 102-111.

Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia", *Kanun Jurnal Ilmu Hukum*, Vol. 20, No. 2, hlm. 369-384.

Lydia K. Saragih, "Perlindungan Hukum Data Pribadi terhadap Penyalahgunaan Data Pribadi pada Platform Media Sosial", *Jurnal Hukum De'rechtstaat*, Vol. 6, No. 2, hlm. 125-142.

Maichel Delpiero, et al., "Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban *Online Marketplace* dalam Pelindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data", *Padjajaran Law Review*, Vol. 9, No. 1, 2021, hlm. 1-22.

Mifrakhur R. Habibie dan Isnatul Liviani, "Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Sistem Hukum Indonesia", *Al Qanun: Jurnal Pemikiran dan Pembaharusan Hukum Islam,* Vol. 23, No. 2, 2020, hlm. 400-426.

Millencia Ang, "Consumer's Data Protection and Standard Clause in Privacy Policy in E-Commerce: A Comparative Analysis on Indonesian and Singaporean Law", *The Lawpreneurship Journal*, Vol. 1, Issue 1, 2021, hlm. 100-113.

Muhamad H. Rumlus dan Hanif Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik", *Jurnal HAM*, Vol. 11, No. 2, 2020, hlm. 285-299.

Ranty M. Jhon, "Existence of Criminal Law on Dealing Cyber Crime in Indonesia", *Indonesian Journal of Criminal Law Studies*, Vol. 3, No. 1, hlm. 25-34.

Ririn Aswandi, et al., "Perlindungan Data dan Informasi Pribadi Melalui *Indonesian Data Protection System* (IDPS)", *LEGISLATIF*, Vol. 3, No. 2, hlm. 167-190.

Rosalinda E. Latumahina, "Aspek Hukum Perlindungan Data Pribadi di Dunia Maya", *Jurnal Gema Aktualita*, Vol. 3, No. 2, 2014, hlm. 14-25.

Sahat M. T. Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber", *SASI*, Vol. 27, No. 1, hlm. 38-52.

Sekaring A. Kusnadi dan Andy U. Wijaya, "Perlindungan Hukum Data Pribadi sebagai Hak Privasi", *Al Wasath Jurnal Ilmu Hukum*, Vo. 2, No. 1, 2021, hlm. 1-15.

Sinta D. Rosadi, "Protecting Privacy On Personal Data In Digital Economic Era: Legal Framework In Indonesia", *Brwaijaya Law Journal*, Vol. 5, No. 1, 2018, hlm. 143-157.

Sinta Dewi, "Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia", *Yustisia*, Vol. 5, No. 1, 2016, hlm. 22-30.

Siti Yuniarti, "Perlindungan Hukum Data Pribadi di Indonesia", *JURNAL BECOSS (Business Economic, Communication, and Social Scoences)*, Vol. 1, No. 1, 2019, 147-154.

Syarpani et al., "Tinjauan Yuridis terhadap Perlindungan Data Pribadi di Media Elektronik (Berdasarkan Pasal 25 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Elektronik", *Jurnal Beraja Niti*, Vol. 3, No. 6, 2014, hlm. 1-29.

Warren B. Chik, "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy", *Computer Law and Security Review*, Vol. 29, No. 5, 2013, hlm. 554-575.

Legal Documents

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Personal Data Protection Act 2010 of Malaysia.

Personal Data Protection Act 2012 of Singapore.

Rancangan Undang-Undang tentang Perlindungan Data Pribadi.

Singapore – Personal Data Protection (Amendment) Act 2020.

The Personal Data Protection Code of Practice.

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan.

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Electronic Documents

Bisnis.com, "Data Pribadi Bocor Lagi, RUU Perlindungan Data Pribadi Makin Mendesak", https://kabar24.bisnis.com/read/20220109/15/1486824/data-pribadi-bocor-lagi-ruu-perlindungan-data-pribadi-makin-mendesak, accessed on 28th May 2022.

CNN Indonesia, "13 Juta Data Bocor Bukalapak Dijual di Forum Hacker", https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker, accessed on 17th December 2021.

CNN Indonesia, "Kebocoran Data Pribadi yang Tak Berujung di RI", https://www.cnnindonesia.com/teknologi/20220112191045-185-745842/kebocoran-data-pribadi-yang-tak-berujung-di-ri, accessed on 28th May 2022.

CNN Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual", https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual, accessed on 17th December 2021.

David Watts dan Pompeu Cassanovas, "Privacy and Data Protection in Australia: a Critical overview", https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf, downloaded on 17th December 2021.

Kompas, "Awas Pencurian Data Pribadi untuk Pinjaman Online, Begini Cara Melindunginya", https://www.kompas.com/tren/read/2021/04/27/203000165/awas-pencurian-data-pribadi-untuk-pinjaman-online-begini-cara-melindunginya?page=all, accessed on 28th May 2022.

Muhammad Firdaus, "A Review of Personal Data Protection Law in Indonesia", https://osf.io/tmnwg/download, downloaded on 17th December 2021.

Ni G. A. P. Nitayanti dan Ni M. A. Y. Griadhi, "Perlindungan Hukum terhadap Informasi Pribadi terkait *Privacy Right* Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik", https://ojs.unud.ac.id/index.php/Kerthanegara/article/download/10713/7619 , downloaded on 14th of December 2021.

Novina P. Bestari, "Investigasi Dugaan Data BPJS Kesehatan Bocor Usai, Hasilnya?", https://www.cnbcindonesia.com/tech/20211025134818-37-286329/investigasi-dugaan-data-bpjs-kesehatan-bocor-usai-hasilnya, accessed on 18th December 2021.

Peter Leonard, "Australian Data Protection and Privacy Laws: A Primer", https://iabaustralia.com.au/wp-content/uploads/2019/08/Australian-Privacy-and-Data-Protection-Law_A-Primer_2019_Peter-Leonard_Data-Synergies.pdf, downloaded 17th December 2021.

Riyan Setiawan, "KPU Membenarkan 2,3 Juta Data yang Bocor Merupakan DPT Tahun 2014", https://tirto.id/kpu-membenarkan-23-juta-data-yang-bocor-merupakan-dpt-tahun-2014-fA5B, accessed on 17th December 2021.

Roy, "Heboh! Data KTP Hingga Nomor HP 279 Juta Warga RI Bocor?", https://www.cnbcindonesia.com/tech/20210520160626-37-247096/heboh-data-ktp-hingga-nomor-hp-279-juta-warga-ri-bocor, accessed on 17th December 2021.

Roy Franedya, "1,2 Juta Data Pengguna Dikabarkan Bocor, Bhinneka Minta Maaf", https://www.cnbcindonesia.com/tech/20200512164725-37-157971/12-juta-data-pengguna-dikabarkan-bocor-bhinneka-minta-maaf, accessed on 17th December 2021.

Dokumen Lainnya

Gliddheo A. Riyadi, "Data Privacy in the Indonesian Personal Data Protection Legislation", *Policy Brief No. 7,* Maret 2021, Center for Indonesian Policy Studies, hlm. 1-9.

Muhammad Fathur, "Tanggung Jawab Tokopedia terhadap Kebocoran Data Pribadi Konsumen", *Paper presented on 2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*, 2020, hlm. 43-60.

Yosephus Mainake dan Luthvi F. Nola, "Dampak Pasal-Pasal Multitafsir dalam Undang-Undang tentang Informasi dan Transaksi Elektronik", *Info Singkat: Kajian Singkat terhadap Isu Aktual dan Strategis*, Vol. 12, No. 16, 2020, hlm. 1-6.