P-ISSN : 2745-7753
E-ISSN : 2772-6670

INDONESIAN JOURNAL OF LAW AND POLICY STUDIES

Indonesian Journal of Law and Policy Studies Volume 3 Nomor 2 Halaman 107-174 Tahun 2022 e-ISSN 2772-6670

DAFTAR ISI

■Submitted: 19 Dec 2022 ■Revised: 26 Dec 2022 ■Accepted: 31 Dec 2022

DIFFERENCES IN DATA PROTECTION SYSTEMS IN INDONESIA AND SINGAPORE

Rizki[1], Elfrida Ratnawati Gultom[2]
1,2 Trisakti University, Jakarta
West Jakarta, Indonesia: Jalan Kyai Tapa No. 1 Grogol
* Correspondence Email: rizkipakot@gmail.com

ABSTRACT The Indonesian Personal Data Protection Law, which was recently promulgated by the government, was created with the aim of protecting the privacy of public data and aims to provide a sense of legitimacy to data owners. However, there are several obstacles, one of which is the absence of any confirmation procedures for data owners before the information is used by certain government agencies or institutions, which is different from what Singapore does. In this study, we use the Normative method to collect data from the literature by extracting data every few seconds from books, analyzing data related to privacy data leaks in Indonesia and Singapore, and drawing conclusions. We anticipate that the findings will be similar to the data leak study in Singapore as the data was obtained before any organization or individual used it to carry it out.
KEYWORDS: System, Data, Data Protection

INTRODUCTION

In the current era of digitalization, digitization includes things that are necessary and have evolved into necessities for society. With the aid of digital technology, certain tasks can be completed more quickly and easily, such as satisfying daily needs by simply ordering supplies (Kurhayadi et al., 2020; Mubin, 2020). Additionally, we may order things from both domestic and international sources without leaving the house by utilizing a shopping application, saving us the trouble of going to the market or supermarket, in addition to performing other tasks using simply a digital application (Hasibuan et al., 2020; Romindo et al., 2019)

This results in changes to the way people live and work around the world, creating a world without borders, altering social behavior, culture, and law enforcement in and of itself because as societal views change, so do the laws governing the use of both basic and sophisticated technology. the most recent in society's legal developments that must be adhered to (Priliasari, 2019).

Because the data used to make transactions, such as personal identity data, can be recorded by the digital application, such as tracking shopping activities carried out, locations where shopping, phone numbers, addresses, email communication data, bank account numbers to the addresses used, transactions made via digital can hurt its users (Jamaludin et al., 2020; Rumondang et al., 2019).

This situation is of course vulnerable to the protection of consumer personal data against consumer privacy rights, in various countries this has developed into an integral part of social development, even privacy law has appeared in positional law and jurisprudence regarding privacy, long before privacy law became integral part of international human rights law (Indriani, 2017).

Since the Covid-19 pandemic occurred, many Indonesian people have registered their data in various applications, the data shows an increase of 38.3 percent from the previous year, be it online loan applications, online motorcycle taxi applications, or matchmaking applications, and other applications, every application used by consumers must fill in their data in the form listed on the web page in general and every electronic system application so that personal data input into the system can be known by the application provider company, therefore security matters for consumer data become vulnerable and easily infiltrated by people irresponsible.(Putri & Fahrozi, 2021)

The increasing need in terms of technology has led to new modes of crime, crimes that use digital data to commit fraud and other crimes, this is due to the increasing activity of some internet users for various activities so the possibility of data leakage is very large so that it is considered a serious matter, in 2011 Telkomsel experienced a data leak of 25 million of its customers, then in 2019, it was also experienced by the airline Lion Air where the data leak was in the form of identities, passports of passengers which the airline kept in an electronic storage container a server provided by the airline. With this data leak, there are fears that it will be misused by irresponsible people, such as the crime of buying and selling personal data or other types of fraud, given the current modern era where various digital-based businesses are growing that require personal data to be processed into business commodities. A data security agency ISIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center) stated that in 2020 there was a data leak with a total of 73 million data from various online applications used in Indonesia (Putri & Fahrozi, 2021; Tsamara, 2021)

The most recent news is that there was a data breach case carried out by Bjorka, a hacker who claims to have as much as 44 million data belonging to MyPertamina. Bjorka's hacker said he had 30 GB of data that had been compressed to 6 GB and which he got in November 2022, but this is not the only thing he has done; in the past, Bjorka has committed data breaches such as Indihome user data, SIM card registration data (personal data) (I. R. Dewi, 2022).

The government passed a law that addressed the protection of personal data in response to the urgency of the issue. This law was ratified by the DPR at the Plenary Session on

September 20, 2022, and it was then known as Law no. 27 the year 2022 concerning the Personal Data Protection Act (Bukit & Ayunda, 2022; Hisbulloh, 2021).

With the existence of the Personal Data Protection Act, it is hoped that it can provide a legal basis that can provide a sense of security for data owners who have been vulnerable to misuse of personal data for unwanted things, because the advancement of technology is currently growing from time to time (Nurmalasari, 2021; Situmeang, 2021). in the economic, cultural, social, religious, health and other sectors within a government related to auxiliary institutions in implementing services for the needs of the general public and this is a concern experienced by the community as the data owner (Sihombing, 2021).

This is due to the weak technology security system owned by the state in terms of data protection, this is also often experienced by the government itself which is still experiencing data leaks in government institutions, so with the existence of a legal umbrella in the form of laws passed by the government hope this can overcome all problems because with the existence of a legal umbrella, there is authority in charge of controlling and taking legal action against parties who misuse data.(Aswandi et al., 2020; S. Dewi, 2016)

By giving personal data protection priority, it is hoped that the new regulations will enable them to respond to societal needs, promote ethical innovation, and uphold human rights. In addition, the Personal Data Protection Law is expected to be a catalyst for changing people's behavior regarding data protection, as a catalyst for ecosystem development, as a means to attract new talent in personal data protection, and as a means to enhance Indonesia's position as a global country. (Ngamal & Perajaka, 2022)

In a previous article, it was stated that there is a need for a comprehensive amendment to a sectoral law that requires a specific and comprehensive amendment, which was published in a journal titled " Legal Protection of Personal Data in Indonesia," where the article stated that data encryption is a type of privacy that a person has, and it is a type of human right, which is protected by law.(Tsamara, 2021)

If we compare Singapore to other Southeast Asian countries, we see that Singapura has laws in place since 2014 that protect personal data. These laws were adopted in line with the European Data Protective Directive (EUDP), just as Malaysia did. As a result, Singapore has a special database for registering telephone numbers known as the Do Not Call (DNC) Registry (Tsamara, 2021).

The principle of consent from the data owner and notification to the data owner when utilized for a purpose are two of the many principles in Singapore's personal data protection law. data, there is a duty to inform the owner of the data, a duty to provide access and a duty to correct to institutions or agencies utilizing the data, a duty to ensure the data's accuracy and

a duty to keep it safe, a duty to set retention and transfer limits, and a duty to ensure accuracy.(Raila et al., 2021)

Apart from the fact that Singapore has sophisticated technology for data protection, which is well known, the country also takes several steps to support data protection, including installing CCTV, maintaining the internet, using drones, securing data access internet, mandating SIM registration, and offering assistance needed when registering on certain websites, such as Singapore conducting research.

METHODOLOGY

In this study, which employs the normative legal research methodology, the sources are taken from literary sources using secondary data from books, the findings from prior research from numerous articles and from several experts who consistently observe matters relating to the protection of personal data in Indonesia and Singapore, followed by tracing the development of these regulations, both in Indonesia and in Singapore, using primary data materials covering regulations in both countries and secondary data materials from earlier studies, including materials that were generated from seminars, both national seminars and international seminars and conferences. After the data is obtained, a qualitative analysis is then conducted by producing descriptive analysis data.(Darmalaksana, 2020)

RESULTS AND DISCUSSION

In the discussion related to the protection of personal data, the connection with this concept is a matter that is private in nature, another thing that can be illustrated in the realm of privacy becomes criminal law is when we enter someone else's yard without permission, because the law itself provides opportunities and space for matters relating to a person's emotional and intellectual, explanation of privacy itself until now there is no clear meaning, according to Holvast the meaning of privacy is the freedom to determine one's own path, while according to other experts Salove explained there are several criteria included in the realm of privacy including are those related to one's rights, rights in the form of closing oneself from other people, the right to close something from other people, the right to control various information from other people, the right to be alone, and the right to relate to other people.

Privacy in the context of protecting personal data has several limitations, among them a lack of absolute confidentiality. This is because these limitations relate to the territory of a particular nation at the time of the incident; generally, these limitations relate to the country's legal framework. Warren and Brandies came up with this idea because they recognize that privacy is not absolute and that there are safeguards in place to prevent the unauthorized disclosure of someone else's personal information. Additionally, they noted that prior to

information being published, data subjects must be provided with legal protections in the event that they experience legal trouble.

In the Personal Data Protection Act it is explained that the principle of application of this law is contained in Article (3) which aims to maintain confidentiality, guarantees for citizens regarding data owned, the principle of benefit, public interest, balance, prudence, which aims to encourage the economy, growth in the digital and information sector as well as increase the ability of the state for competition in the era of globalization and the state accommodates the interests of the community in order to create a balance between individuals in society so that a sense of security for data owners can be felt, the birth of this Personal Data Protection Act is to provide Considering this, including human rights that need to be protected, a legal regulation is needed to regulate this matter which aims to provide a sense of security for someone. personal data and can foster a sense of public awareness about the protection of their personal data, another background is the protection of personal data and in its implementation is more effective in a law, basically this law regulates standard matters in protection according to their respective fields each in part or in whole electronically or non-electronically on personal data in general.

1. Data Protection in Indonesia

This data protection is as mandated in article 28G paragraph (1) of the 1945 Constitution which states that "Every person has the right to protection of personal data, family, honor, dignity and property under his authority, and has the right to feel safe and protected from threats of fear to do or not do something that is a human right".

However, believe that this Personal Data Protection Act has its drawbacks. For example, article 1 point 4 states that "A Personal Data Controller is any individual, public body or international organization that acts alone or jointly in determining goals and exercising control over the processing of Personal Data." This means that private legal entities are not given the right to manage personal data.

In article 2 paragraph (2) it states "This law does not apply to the processing of personal data by individuals in personal or household activities" this phrase is considered weak and can lead to negative terms in its interpretation because this article does not accommodate the need for an individual to commit data breaches which are carried out by hackers even though basically it is only for personal purposes, whereas in article 18 in paragraph (1) it states that the processing of personal data can be carried out by 2 (two) or more data controllers "then it can be interpreted if someone uses other people's data personally or in households, this rule cannot be used because it has nothing to do with professional or commercial activities.

Due to the fact that the offending party observed the aforementioned campaign as correspondence involving the exchange of contact information, social networking, and online activities carried out in the name of activity, the offending party is aware that the aforementioned law allows for the control, monitoring, or seizure of private data, private activities, or a person's home. It is connected to either professional or commercial projects.

Many people question how much influence the Personal Data Protection Act has in overcoming existing problems, especially how much this Personal Data Protection Act can protect human rights in the field of personal data protection in the midst of the current digital wave, including matters relating to the jurisdiction of this law because This law discusses the permissibility of international agencies to process personal data in accordance with statutory rules, because this is transnational, the subject will also be transational, so it is not impossible that there will be intersections between civil jurisdiction, administrative jurisdiction and criminal jurisdiction.

Contrary to the Criminal Code, which gives criminal penalties precedence over civil law, the Personal Data Protection Act does not provide a clear distinction between administrative and criminal sanctions or which should be applied first. There are other situations, such as lex specialis, which take precedence over Article 63(2) of the Criminal Code.

Following the implementation of the Personal Data Protection Act, the government must closely monitor data protection in the context of international agreements, particularly under the supervision of a personal data protection agency with concerns about the use of data by foreign parties. In particular, if there is a dispute with data control in another country, the question of whether or not the agency that is located outside the country is opposed to the protection of the personal data that we have?

Article 56 paragraph (1) Chapter VII states that controllers of personal data can transfer personal data to controllers of personal data and/or processors of personal data outside the jurisdiction of the Republic of Indonesia in accordance with the provisions stipulated in this Law, but in paragraph (1) this does not explain the absence of the phrase "with the consent of the owner of personal data" then this is an absolute weakness so that it is contrary to the main purpose of establishing the Personal Data Protection Act, so in article 56 it does not provide added value to the protection of personal data inside and outside country.

If this is brought in a case to the International Arbitration Agency, we all know that the International Arbitration Agency's arguments are stronger than domestic law, then this can result in defeat on our part, as well as limitations on personal data control when it intersects with state jurisdiction. another because this has touched the criminal realm of other countries,

especially if there is a difficult criminal dispute without *mutual assistance in criminal matter* or extradition.

The existence of international agreements, both bilateral and multilateral, is anticipated to promote a high level of trust in personal data control agencies and data owners because this can offer a sense of security for data that has been provided to other parties in line with the achievement of the Law's goals and use. this rule because, due to differences in the legal systems of several nations, a situation that has come into the jurisdiction of another country will be handled differently. 2022 (Romli Atmasasmita)

Therefore, whether they are controllers of personal data or owners of personal data themselves, it is vital in this situation to have harsh administrative sanctions or criminal consequences against stakeholders. Indonesia itself likes to use punitive punishments. In contrast to other nations that use a system of non-penal punishments, this one places more emphasis on non-penal parts of law enforcement by educating all parties, particularly the police who are handling cases of Personal Data Protection Act infractions.

2. Data Protection in Singapore

In contrast to Indonesia, Singapore has a number of data privacy principles, including the following:

a. *Principle Consent,* the principle that every organization, including governmental bodies, is capable of accessing, using or creating private data if its owner does so.
b. *Principle Purpose* , which states that under all circumstances, any institutions or private parties that wish to collect, use, and store data must notify the data's owner of their intended use.
c. *The reasonableness principle* states that any organization or government agency that informs a data user will have clear objectives for doing so.

The application of criminal sanctions is thought to be more effective to create a deterrent effect against the misuse of personal data, and this is explained in the Singapore Data Protection Act (PDPA). Article 48 states that the punishment given is 2 years imprisonment ot the institution, so if there is a leak, outside of the above principles, then the Singaporean government can give strict sanctions against the institution, whether it is a prison sentence or a fine. In accordance with the Public Sector Governance Act of 2018 (PSGA), which requires private parties to securely protect personal data and thwart illegal access, acquisition, and use, the same rules apply here. In the event that data leaks, then the private party must be held responsible and sanctioned.

As Singapore's Personal Data Protection Act (PDPA) evolves in 2020, it aims to become a basic standard of data protection in the private sector with the aim of increasing confidence

in data processing. When private parties collect, use or disclose a person's data, they must inform them of their purpose as specified in PDPA article 20 (1) in order to obtain the consent of the person. For example during Covid-19, Singapore is using contact tracing tools to identify anyone who has been exposed to the virus. The application is called *Trace Together*, and involves the private sector. It has a feature called *Safe Entry*, which is used when visitors to public spaces input their data by scanning a barcode on the *Safe Entry application* used by private parties through the *Trace Together application* . This was followed by Indonesia doing the same thing in dealing with Covid-19 by collaborating with the private sector in terms of detecting Covid exposure itself with a different platform.

In addition to the rules made, Singapore also completes other rules to monitor whether the rules are good or not. Singapore presents the Personal Data Protection Commission (PDPC), whose main responsibility is to ensure that these regulations are properly implemented. This commission can also receive complaints from the general public, apart from being a facilitator in alternative dispute resolution. Everyone who suffers a loss as a result of this regulation can ask for help from this commission, then this commission will conduct an investigation into the report. If this is true, with clear evidence, this commission can impose fines of up to $1 million Singapore dollars, in addition to fines, you can also given a criminal sanction in the form of imprisonment for 3 years as stipulated in article 56 PDPA

CONCLUSION

There are fundamental differences between the two data protection laws, as well as the current legal protection arrangements in Indonesia and Singapore. For example, Indonesia's personal data protection law was just passed in 2022, and there have been delays in creating a legal framework for this protection, because previous personal data protection regulations were still sectoral in nature, where these regulations were widely found in various regulations such as Government Regulations, Electronic Transaction Information Laws to Ministerial Regulations, in contrast, Singapore has adopted a personal data protection regulation since 2012 and was just amended in 2020. In the Singaporean law governing the privacy of personal information, we can find that these arrangements are carried out very strictly, with the existence of several layering laws according to their respective parts and the existence of a monitoring body for the rules that have been made, this commission has the right to impose sanctions, whether sanctions Administratively in the form of fines or criminal sanctions in the form of imprisonment, this is different from in Indonesia where the Institution as a monitoring of rules can only give administrative sanctions. Another distinction is that Singapore's data protection law is based on the principle that institutions and private companies must obtain the data owner's consent before storing, using, or disclosing the data. In addition, Singapore

has advanced technological facilities that support the security of residents' personal data, including CCTV installation, the use of drones, and internet data security. The authors determine that this is the case in Singapore due to a number of variables, including the recent passage of the Personal Data Protection Act has just been passed, and the scope of the law cannot be seen or the constraints that have occurred on the response of the community besides that there are no supporting facilities like those owned by Singapore because if we can see that these two countries have similarities in personal data protection laws to improve security and boost the economy.

BIBLIOGRAPHY

Aswandi, R., Muchin, P. R. N., & Sultan, M. (2020). Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (Idps). *Jurnal Legislatif*, 167–190.

Bukit, A. N., & Ayunda, R. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1–20.

Darmalaksana, W. (2020). Metode penelitian kualitatif studi pustaka dan studi lapangan. *Pre-Print Digital Library UIN Sunan Gunung Djati Bandung*.

Dewi, I. R. (2022, November 11). Hacker Bjorka is Back, Data Apa Saja yang Pernah Dibocorkan? *CNBC Indonesia*.

Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia Jurnal Hukum*, *5*(1), 35–53.

Hasibuan, A., Jamaludin, J., Yuliana, Y., Sudirman, A., Wirapraja, A., Kusuma, A. H. P., Hwee, T. S., Napitupulu, D., Afriany, J., & Simarmata, J. (2020). *E-Business: Implementasi, Strategi dan Inovasinya*. Yayasan Kita Menulis.

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, *37*(2), 119–133.

Indriani, M. (2017). Perlindungan Privasi Dan Data Pribadi Konsumen Daring Pada Online Marketplace System. *Justitia Jurnal Hukum*, *1*(2).

Jamaludin, J., Purba, R. A., Effendy, F., Muttaqin, M., Raynonto, M. Y., Chamidah, D., Rahman, M. A., Simarmata, J., Abdillah, L. A., & Masrul, M. (2020). *Tren Teknologi Masa Depan*. Yayasan Kita Menulis.

Kurhayadi, H., Rohayati, Y., & Bambang Sucipto, M. M. (2020). *Kebijakan Publik di Era Digitalisasi*. Insan Cendekia Mandiri.

Mubin, F. (2020). *Tantangan Profesi Guru Pada Era Revolusi Industri 4.0*.

Ngamal, Y., & Perajaka, M. A. (2022). Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, *2*(2), 59–74.

Nurmalasari, N. (2021). Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum. *Syntax Idea*, *3*(8), 1947–1966.

Priliasari, E. (2019). Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online. *Majalah Hukum Nasional*, *49*(2), 1–27.

Putri, D. D. F., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. Com). *Borneo Law Review*, *5*(1), 46–68.

Raila, T. A., Rosadi, S. D., & Permata, R. R. (2021). Perlindungan data privasi di Indonesia dan Singapura terkait penerapan digital contact tracing sebagai upaya pencegahan covid-19 serta tanggungjawabnya. *Jurnal Kepastian Hukum Dan Keadilan*, *2*(1), 1–18.

Romindo, R., Muttaqin, M., Saputra, D. H., Purba, D. W., Iswahyudi, M., Banjarnahor, A. R., Kusuma, A. H. P., Effendy, F., Sulaiman, O. K., & Simarmata, J. (2019). *E-Commerce: Implementasi, Strategi dan Inovasinya*. Yayasan Kita Menulis.

Rumondang, A., Sudirman, A., Effendy, F., Simarmata, J., & Agustin, T. (2019). *Fintech: Inovasi Sistem Keuangan di Era Digital*. Yayasan Kita Menulis.

Sihombing, G. L. (2021). Perlindungan Konsumen Dalam Pengawasan Perusahaan Berbasis Financial Technology. *Jurnal Kebijakan Publik*, *12*(2), 73–80.

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*, *27*(1), 38–52.

Tsamara, N. (2021). Perbandingan Aturan Perlindungan Privasi atas Data Pribadi antara Indonesia dengan Beberapa Negara. *Jurnal Suara Hukum*, *3*(1), 53–84.