

CHAPTER I

INTRODUCTION

A. Background

The Post-Covid-19 pandemic has triggered many people to switch to using digital technology, which has led to increased use of the internet as a medium for daily needs. This situation is supported by various online services in multiple sectors, such as e-commerce, e-education, e-health e-payment, e-government, and others.¹ Personal data information is precious in developing and using online services.²

This data is called a digital dossier or digital file, a collection of personal data information owned by people who utilize internet technology developed by private parties who are significantly at risk of violating privacy rights over personal data.³ The increasing need for information and communication technology causes the emergence of various criminal acts that can cause harm to someone and pose a risk of leaking personal data.

In the last few decades, data protection laws in Indonesia have made significant progress and developments. Even though there have been many rules governing personal data protection, personal data violation cases have

¹ Muhammad Raihan Faiqy, Muhammad Izzar Damargara, Muhammad Alhidayah, and Jatnika Maulana, "Urgensi Realisasi Peran Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi", *Padjadjaran Law Review*, Vol. 10, No. 1 (2022), p. 1.

² Andriyanto Adhi Nugroho, Atik Winanti, and Surahmad, "Personal Data Protection in Indonesia: Legal Perspective", *International Journal of Multicultural and Multireligious Understanding*, Vol. 7, No. 7 (2020), p. 148.

³ Dian Purnama Anugerah and Masitoh Indriani, "Data Protection in Financial Technology Services: Indonesian Legal Perspective", *In IOP Conference Series: Earth and Environmental Science*, Vol. 175, No. 1 (2018), p. 1.

become a serious legal issue. This is because Indonesia is the country that ranks third with the most cases of data leakage in the world.⁴

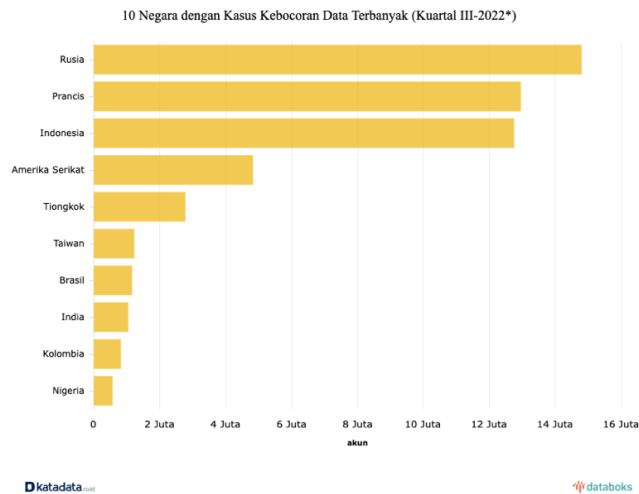


Figure 1 10 countries with the highest number of data leaks

According to data from Cyber Security Company Surfshark recorded on September 13, 2022, there were 12.74 million accounts that experienced data leaks in Indonesia during the third quarter of 2022.⁵ This data cannot be separated from the relatively high number of data leakage incidents. In the past three years, inevitably, data leaks in Indonesia have always occurred at least once a year.

In September 2019, there was a 21 million passenger data leak on the Lion Air airline.⁶ Furthermore, in April 2020, Tokopedia, a marketplace

⁴ Cindy Mutia Annur, 2022, *Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Dunia*, <https://databoks.katadata.co.id/datapublish/2022/09/13/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia>, (October 6, 2022 at 12.13 P.M).

⁵ Muhammad Aulia Zikra, 2022, *Menyikapi Kasus Kebocoran Data Pribadi di Era Digital*, <https://www.its.ac.id/news/2022/11/02/menyikapi-kasus-kebocoran-data-pribadi-di-era-digital/>, (December 6, 2022 at 12.18 P.M).

⁶ Afif Hadiani Pratiwi, Edi Wahjuni, and Nuzulia Kumala Sari, “Perbuatan Melawan Hukum dalam Kebocoran Data Penumpang Lion Air Group”, *Journal of Private and Economic Law*, Vol. 1, No. 2 (2021), p.1.

in Indonesia, experienced a data leak, and 15 million user data were hacked. Upon further investigation, the number increased to 91 million accounts and 7 million Merchant accounts.⁷ Even though a year earlier, Tokopedia had informed that there were around 91 million on its platform.⁸ That way, it can be said that almost all accounts in the Tokopedia marketplace were successfully hacked, and their data was retrieved.

This case has not yet been completed, but a new case has emerged related to the leakage of personal data at the beginning of the 2021 pandemic, which occurred in a government agency, namely the Social Security Administration Agency. In the case of the leak, it was recorded that 279 million of the Social Security Administration Agency user data were sold on the *Raidforums.com* online forum site for around IDR 87.6 million consisting of full names, identity card numbers, telephone numbers, e-mail addresses, salaries, and addresses.⁹ They give away 1 million free samples and 20 million data featuring personal photos.¹⁰ In fact, health data is included in specific data or sensitive data, so the personal data of patients as consumers really need to be protected because it contains confidential information under Law Number 36 of 2009 concerning Health Law.

⁷ Desy Komalawati, Maria Dewi M.R, and Raiseta Dwi Kartika, “Kejutan Puluhan Miliar Tokopedia Ditengah Kasus Kebocoran Data”, *Jurnal Syntax Admiration*, Vol. 2, No. 1 (2021), p.1.

⁸ Mas Rara Tri Retno Herryani and Harsono Njoto, “Perlindungan Hukum Terhadap Kebocoran Data Pribadi Konsumen Online Marketace”, *Jurnal Transparansi Hukum* Vol. 5, No. 1 (2022), p. 114.

⁹ Shella Oktaviani, Yeremia Juan Dewata, and Aryo Fadlian, “Pertanggung Jawaban Pidana Kebocoran Data BPJS Dalam Perspektif UU ITE”, *De Juncto Delicti: Journal of Law*, Vol. 1, No. 2 (2021), p. 147.

¹⁰ Farah Nabilla, 2022, *11 Daftar Kasus Kebocoran Data di Indonesia, Sebulan Tiga Kali Kejadian!*, <https://www.suara.com/news/2022/09/02/115017/11-daftar-kasus-kebocoran-data-di-indonesia-sebulan-tiga-kali-kejadian>, (December 6, 2022 at 14. 28 P.M).

In July and August, there were 2 cases of data leakage that occurred in the same year. First, data leaks at the insurance company BRI Life amounted to 2 million customers containing photos of residential identity cards, bank accounts, reports on the results of customer laboratory tests, and even information on customer taxes.¹¹ Second, as many as 1.3 million e-HAC application user data were leaked, including full names, birth dates, occupations, personal photos, identification numbers, passport numbers, Covid-19 test results, hospital identity, addresses, telephone numbers, and some other information. Until 2022, cases related to data leaks are increasing. From January to November, the Ministry of Communication and Informatics (MoCi) received 33 reports regarding data leakage and personal data protection incidents.¹²

To combat many cases that have occurred, on October 17, 2022, Indonesia enacted a Personal Data Protection Law. This law provides various forms of protection that can encourage the quality improvement of personal data protection, such as definition, type, and ownership rights of personal data, processing, exceptions, controllers, processors, transmission, authorized institutions that regulate personal data, and settlement dispute.

The high frequency of data leak instances in Indonesia indicates a lack of cyber security. In measuring the cyber security rating index, several

¹¹ Pratiwi Agustini, 2021, *Kominfo Gandeng BSSN dan Polri Selidiki Dugaan Kebocoran Data BRI Life*, <https://aptika.kominfo.go.id/2021/07/kominfo-gandeng-bssn-dan-polri-selidiki-dugaan-kebocoran-data-bri-life/>, (December 6, 2022 at 14.50 P.M).

¹² Titah Arum M. R Toewoeh, 2022, *Kominfo Gerak Cepat Tangani Lima Kasus Baru Kebocoran Data*, <https://aptika.kominfo.go.id/2022/11/kominfo-gerak-cepat-tangani-lima-kasus-baru-kebocoran-data/>, (December 6, 2022, at 15.15 P.M).

indicators are used, such as the relevant country's legal regulations regarding cyber security, whether or not the government or other authorities cooperate to supervise data controllers and processors regarding cyber security requirements to a series of cyber security programs, and the presence or absence of crisis management to deal with cybersecurity incidents.¹³

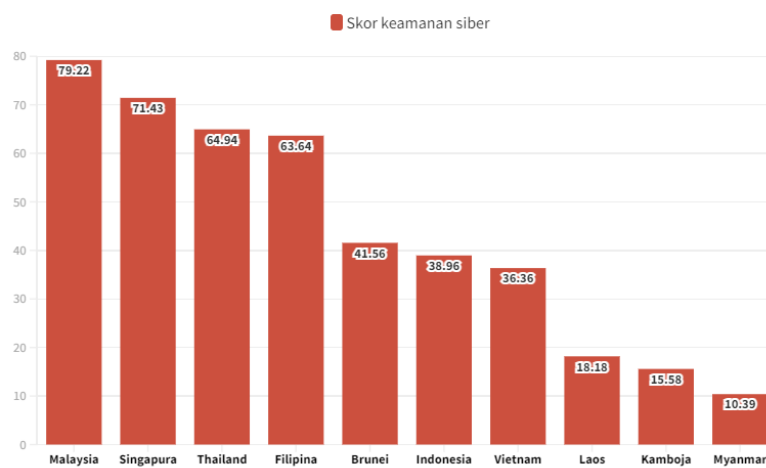


Figure 2 Index Cyber Security in SouthEast Asia per August 2022



Figure 3 National Cyber Security Index between Malaysia and Indonesia

According to the National Cyber Security Index, Indonesia ranks

¹³ Kamy Farahbod, Conrad Shayo, and Jay Varzandeh, “Cybersecurity Indices and Cybercrime Annual Loss and Economic Impacts”, *Journal of Business and Behavioral Sciences*, Vol. 32, No. 1 (2020), p. 67.

85th out of 164 countries, or 6th among ASEAN countries vulnerable to data leakage, with a score of 38.96. Malaysia, on the other hand, is the country with the best cybersecurity index in Southeast Asia, ranking 20th globally with a score of 79.22.¹⁴ The difference in the Cyber Security Index gap shows that Malaysia has a lot more experience and knowledge when it comes to protecting personal data and cyber security. Because of this, it is important to compare laws that are more detailed and complex.

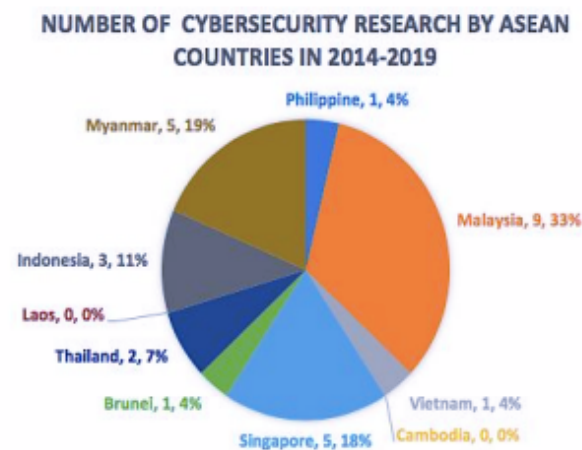


Figure 4 Number of Cybersecurity Research by ASEAN Countries in 2014-2019

From the above diagram, it's interesting to see that Malaysia is the country with the most completed studies (9.33%) between 2014 and 2019. At the same time, Indonesia has begun to study the problems and challenges in the field of cyber security.¹⁵ This makes it easier for the author to find

¹⁴ Faisal Javier, 2022, *Kebocoran Data, Bukti Keamanan Siber Indonesia yang Lemah*, <https://data.tempo.co/data/1501/kebocoran-data-bukti-keamanan-siber-indonesia-yang-lemah>, (January, 20, 2022 at 20.00 P.M).

¹⁵ Nor Shazwina Mohamed Mizan, Muhamad Yusnorizam Ma'arif, Nurhizam Safie Mohd Satar, and Siti Mariam Shahr, "CNDS-Cyber Security: Issues and Challenges in ASEAN Countries", *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 8, No. 1.4 (2019), p. 117.

more sources and research data to back up this research.

There are several studies that have been done before. Such as research in 2023 entitled “*Analisis Pengaturan Keamanan Data Pribadi di Indonesia*” by Mirnayanti¹⁶, where this research still uses the old rules, namely the ITE Law, and has not made comparisons with other countries. In 2021, research conducted by Nadia Tsamara entitled “*Perbandingan Aturan Perlindungan Privasi atas Data Pribadi antara Indonesia dengan Beberapa Negara*”¹⁷ has already made comparisons with other countries. However, this paper still refers to the ITE Law, so it differs from countries that have used the Personal Data Protection Act. Then in 2023, research conducted by Hanafi regarding “*Urgensi Pengaturan Hukum tentang Perlindungan Data Pribadi pada Sistem Digital dalam Pemenuhan Hak Privasi di Indonesia*”¹⁸ where this research used the Personal Data Protection Act but has not made comparisons with other countries

The novelty of this research lies in the identification of problems in the legal framework and challenges that Indonesia will face in implementing the newly passed PDP Act. It is in this context that a comparative approach to the regulation and implementation of the PDP Act in more developed countries needs to be taken by Malaysia as a comparison and lesson learned

¹⁶ Mirnayanti Mirna, Judhariksawan, and Maskum, “Analisis Pengaturan Keamanan Data Pribadi di Indonesia”, *Jurnal Ilmiah Living Law*, Vol. 15, No. 1 (2023), p.1.

¹⁷ Nadiah Tsamara, “Perbandingan Aturan Perlindungan Privasi atas Data Pribadi Antara Indonesia dengan Beberapa Negara”, *Jurnal Suara Hukum*, Vol. 3, No. 1 (2021), p.1.

¹⁸ Hanafi, “Urgensi Pengaturan Hukum Tentang Perlindungan Data Pribadi pada Sistem Digital dalam Pemenuhan Hak Privasi di Indonesia”, *Sultan Adam: Jurnal Hukum dan Sosial*, Vol. 1, No. 1 (2023), p.1.

because Malaysia is a country in Asia that has already regulated PDP issues and has had more experience dealing with related cases.

In the context of cyber security, there are three types of efforts that are made to deal with threats in cyberspace. These are technical efforts, legal efforts, and procedures and guidelines related to cyber security. With the help of the personal data protection law, Indonesia and Malaysia are trying to make sure that personal data is safe. So, more research needs to be done to compare how Indonesia and Malaysia protect personal data.

B. Research Problems

Considering the research background above, the research formulated two questions to be answered, namely:

1. How are the legal frameworks of the Indonesian and Malaysian Personal Data Protection?
2. What are the similarities and differences on the legal framework for personal data protection in both countries?

C. Objectives of Research

The objectives of this research are:

1. To understand the legal frameworks on personal data protection in Indonesia and Malaysia.
2. To analyze the similarities and differences of the legal framework on personal data protection in Indonesia and Malaysia.
3. To propose some recommendations to the government for a better policy relating to personal data protection in the future.

D. Benefits of Research

There are some benefits of this research, namely:

1. Theoretical Aspect

The research contributes to the development of science, particularly in the development of personal data protection. In addition, this research can be used as a source or reference material that can be added to the literature on Personal Data Protection Law, Constitutional Law, and other branches of law.

2. Practical Aspect

The research will provide recommendations for a better policy of government in the future, which addresses to House of Representatives Republic Indonesia primarily related to Personal Data Protection in Indonesia.