Shahrullah, Rina Shahriyani, Jihyun Park and Irwansyah. "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment," *Hasanuddin Law Review* 10 no. 1 (2024): 1-20. DOI: 10.20956/halrev.v10i1.5016

HasanuddinLawReview

Volume 10 Issue 1, April 2024
P-ISSN: 2442-9880, E-ISSN: 2442-9899

Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment

Rina Shahriyani Shahrullah[1], Jihyun Park[2], Irwansyah[3]

[1] *Faculty of Law, Universitas Internasional Batam, Indonesia. E-mail: rina@uib.ac.id*
[2] *Faculty of Law, Youngsan University, South Korea. E-mail: shabd@ysu.ac.kr*
[3] *Faculty of Law, Hasanuddin University, Indonesia. E-mail: irwansyah@unhas.ac.id*

Abstract: Personal data leakages have been experienced by both Indonesia and South Korea. To ensure the protection of privacy rights relating to personal data, both countries have promulgated special laws, namely the Indonesian Personal Data Protection Law (PDP Law) and the South Korean Personal Information Protection Act (PIPA). This study aims to compare the two laws to ascertain their similarities and differences by adopting a comparative law approach. The study found that similarities exist in the two laws. They are to protect personal data and confer rights on data subjects. In the absence of explicit consent given by data subjects, data controllers and processors are prohibited from collecting and processing the data with some exceptions. They also mandate a special institution that is tasked to investigate and sanction data controllers and processors when they conduct data infringement. There are inherent differences in the two laws. PIPA is designed to be the framework legislation and PDP is designed to be a special statute. Additionally, PIPA mandates the institution dealing with personal data protection without referring to any other law but the Act itself. PDP Law clearly states that further provisions relating to this institution will be governed by Presidential Regulation.

Keywords: Data Protection; Personal Data; Privacy Rights; Indonesia; South Korea

1. Introduction

Personal information rights constitute human rights, namely the right to privacy which is stated in the Universal Declaration of Human Rights. Article 17 of the International Convention on Civil and Political Rights (ICCPR) states that every individual has the right to get protection from all forms of threat or disturbance to family privacy, honor and reputation. It is further stated under article 28G that citizens have the right to protection for themselves, family, honor and dignity.[1] Indonesia has ratified the ICCPR by Law No. 12 of 2005. Similarly, South Korea has also ratified the ICCPR in April 2019.

In the globalization and Industrial Revolution 4.0 era, protection of personal data has become very important, and it is closely related to the protection of personal and private rights.[2] Indonesia enacted a new law to specifically govern personal data protection

[1] Ahmad Gelora Mahardika, "Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi Dalam Sistem Ketatanegaraan Indonesia," *Jurnal Hukum* 37, no. 2 (2021): 101–18, https://doi.org/http://dx.doi.org/10.26532/jh.v37i2.16994.

[2] Upik Mutiara and Romi Maulana, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi," *Indonesian Journal of Law and Policy Studies* 1, no. 1 (2020): 42–54, https://doi.org/http://dx.doi.org/10.31000/ijlp.v1i1.2648.

under Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). South Korea was ahead of Indonesia in introducing such a law, since it promulgated the Personal Information Protection Act (PIPA) in 2011.

Data leakage or hacking of personal data occurs frequently both in Indonesia and South Korea. For example, a vital data leakage of Indonesian residents in 2020 caused as many as 1.3 billion customers of a SIM card was leaked.[3] Tokopedia, a famous e-commerce platform in Indonesia also experienced this issue as its customer data consisting of names and family registration cards were leaked. Twenty-six million data of the Indiehome's customers also leaked.[4] Not only has data leakage occurred in the private sector, the Indonesian government also suffered when the Social Security Agency (*Badan Penyelenggara Jaminan Sosial*/BPJS) members' data leaked.[5]

Data leakage cases also occurred in South Korea. The latest incident occurred in January of 2023 when LGU+ leaked personal information of customers. This time, the leakage included of database of a member who has withdrawn. An urgent investigation was conducted by the personal information protection commission. LGU+ should have taken active measures when they found the leakage to prevent the spread of damage.[6] In 2014, Homeplus, a Korean distribution company, sold personal information of its customers collected by lottery by stating on the prize ticket in one mm size font that "personal information can be used for insurance company business", thus making it difficult to recognize has been judged as a fraudulent means to obtain personal information which is not socially acceptable.[7] SK Telecom, the largest communications company in South Korea, was jointly indicted with some of its employees for using the information of its 150,000 customers without their consents (separate consents) in 2014.[8] A Korean pharmaceutical software company was investigated by the Prosecutor's Office for attempting to sell stolen patient medical records (approximately 700 million items) to a pharmaceutical consulting firm. Although the use of personal information without anonymization was a breach of the Personal Information Protection Act, the use of the prescription database program PM2000 was considered a collection of statistics giving no liability for damages. The President of this pharmaceutical software company was arrested in 2014 but released without penalty.[9]

[3] Singgih Wiryono, "SAFEnet: 1,3 Miliar Data Pengguna SIM Card Diduga Bocor Jadi Kasus Terbesar Di Asia," KOMPAS.com, 2022, https://nasional.kompas.com/read/2022/09/09/16180311/safenet-13-miliar-data-pengguna-sim-card-diduga-bocor-jadi-kasus-terbesar-di.

[4] Zulfikar Hardiansyah, "Rentetan Aksi Hacker Bjorka Dalam Kasus Kebocoran Data Di Indonesia Sebulan Terakhir," KOMPAS.com, 2022, https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker-bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan?page=all.

[5] BBC News Indonesia, "BPJS Kesehatan: Data Ratusan Juta Peserta Diduga Bocor - 'Otomatis Yang Dirugikan Masyarakat', Kata Pakar," BBC News Indonesia, 2021, https://www.bbc.com/indonesia/indonesia-57196905.

[6] Cho Jung-Woo, "LG U+ Customer Data Hacked, 180,000 Affected," Korea JoongAng Daily, 2023, https://koreajoongangdaily.joins.com/2023/01/10/business/industry/korea-LG-U-data-breach/20230110184232830.html.

[7] The Supreme Court of South Korea Judgement 2016Do13263.

[8] The Supreme Court of South Korea Judgment 2016Do10102.

[9] Civil Case Division 26.

Due to the problems of data leakage and the enactment of personal data protection laws in both countries, this study aims to analyze the similarities and differences between Indonesia's Personal Data Protection Law (PDP Law) and South Korea's Personal Information Protection Act (PIPA), so that the two countries being compared may learn from each other. In this regard, the study explains the development of personal data protection in both countries and their similarities and differences.

2. Method

This study adopts normative legal research,[10] which aims to find and formulate legal arguments through an analysis of norms".[11] It specifically adopts comparative law research to ascertain their similarities and differences.[12] Normative legal research uses research sources in the form of legal materials which consists of primary and secondary legal materials. The primary legal materials are those that have authority to govern legal matters which consist of legislation, official records or treatises in making laws and judges' decisions.[13] The primary legal materials used for this study are Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) of Indonesia and the Personal Information Protection Act (PIPA) (the amended Act) of South Korea. It also utilizes secondary materials since they use law journals and books as references and utilizes tertiary legal materials such as the non-law article journals and research results, news from electronic newspapers and an Indonesian dictionary. It adopts qualitative data analysis by presenting the analyzed results descriptively.

3. Personal Data Protection Law in Indonesia

Personal data protection is related to the concept of privacy, which aims to ensure personal integrity and dignity.[14] Collecting and sharing of personal data constitutes a violation of privacy,[15] because personal data constitutes an asset with high economic value.[16] Direct marketing practices in Indonesia, particularly in credit card management, have utilized personal information of consumers which have been traded through agents without seeking permission from the owner of the information. A fraud card case conducted by Imam Zahali (IZ) caused a loss to a bank of around Rp. 250 million after using a customer's credit card for cash swipe transactions. He obtained the customers' data from the internet for IDR 800 thousand for 25 data. He contacted the victims

[10] Soetandyo Wignjosoebroto, *Hukum, Konsep, Dan Metode* (Malang: Setara Press, 2013).

[11] Philipus M. Hadjon and Tatiek Sri Djatmiati, *Argumentasi Hukum* (Yogyakarta: Gadjah Mada University Press, 2017).

[12] Ibid, P. 106-124.

[13] Irwansyah, *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel* (Yogyakarta: Mirra Buana Media, 2021).

[14] Wahyudi Djafar and Asep Komarudin, *Perlindungan Hak Atas Privasi Di Internet: Beberapa Penjelasan Kunci* (Jakarta: Elsam, 2014).

[15] Pusat Bahasa Departemen Pendidikan Nasional, *Kamus Besar Bahasa Indonesia* (Jakarta: Balai Pustaka, 2001).

[16] Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta: Raja Grafindo Persada, 2003).

(customers) by claiming that he was a credit card salesman and offered to increase the credit card limits of the victims.[17]

Article 28G of the 1945 Constitution of the Republic of Indonesia is the highest hierarchy of laws pertaining to personal data protection.[18] Prior to the promulgation of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) on 17 October 2022, privacy and personal data protection was governed by various laws, namely banking law, telecommunications law, consumer protection law, population law, human rights law, population administration law, electronic transaction information law, public information disclosure law, health law and other relevant laws and regulations.[19] PDP Law has established more comprehensive approaches to personal data protection; consequently, since the promulgation of this law, any matters relevant to personal data protection must be referred to it. In short, PDP Law is comprised of:

a. Data Categorization. Article 4 states that personal data is divided into two, namely general data and special data. General data consists of full name, nationality, marital status, religion, gender. Special data consists of data genetics, biometrics, health information, crime records, finance, and other data in accordance with the provisions of the law.
b. Data Subject Rights. Articles 5 to 15 are regarding subject data rights relating to legitimate identity and interests, to gain access to and copies of data privacy and to withdraw consent to data disclosure, restrictions and suspension of processing of personal data and filing of complaints about use of personal data until compensation is received and suing for a personal data breach.
c. Data Controller Obligations. Article 20 to Article 50 contain data verification obligations which consist of indicating the consent of the subject data, recording all data processing of privacy activities, protecting and ensuring the security of personal data, and conveying consent, intent, purpose and relevance when transferring personal data.
d. Authority of the Protection Agency. Articles 58 to Article 60 provide the institution which has duties to formulate and establish personal data protection policies and strategies. Article 60 explains the authority of the institution, namely formulating and adopting policies in the field of personal data protection, supervising the compliance of the processing supervisor of personal data, and imposing administrative fines to protect personal data violations.

[17] Mei Amelia R, "Duh! Sales Kartu Kredit Gadungan Ini Gunakan Uang Haram Buat Naik Haji," detiknews, 2016, https://news.detik.com/berita/d-3158671/duh-sales-kartu-kredit-gadungan-ini-gunakan-uang-haram-buat-naik-haji.

[18] Anggriawan, Rizaldy, Andi Agus Salim, Yordan Gunawan, and Mohammad Hazyar Arumbinang. "Passenger Name Record Data Protection under European Union and United States Agreement: Security over Privacy?." *Hasanuddin Law Review* 8, no. 2 (2022): 95-110.

[19] Academic Draft of Personal Data Protection Bill.

4. Personal Data Protection Law in South Korea

South Korea's Constitution does not explicitly stipulate rights to data privacy, but it declared that "data privacy rights are constitutional rights through a ruling in a Constitutional Court case in 2005 (the Fingerprint case)".[20] This case was a landmark case in South Korea because it was the first time that the South Korean Constitutional Court declared that "privacy rights are fundamental constitutional rights and that the right to self-determination is the most crucial aspect of data privacy rights".[21]

The International Association of Privacy Professionals records that South Korea's data privacy law has evolved rapidly and it is considered one of the strictest regulations on personal data protection.[22] In March 2011, the government enacted the Personal Information Protection Act (PIPA) which came into force on September 30, 2011. Prior to the enactment of the PIPA, the government of South Korea had established a number of laws and regulations on data privacy. For example, the Public Agency Data Protection Act (PADP Act) of 1995, and the Promotion of Information and Communications Network Utilization and Information Protection Act (IC Network Act) of 1986,[23] and the Credit Information Use and Protection Act (Credit Information Act) of 1995.[24]

In 2011, the Personal Information Protection Commission (PIPC) was formally established based on the law. Personal information covers the area of credit, finance as well as statistics. This Privacy Protection Law was enacted with the vision of integrating the standard for all when handling personal information. Before this first fundamental law became the core Act in the area of personal information, the public and private sectors had different standards. After enactment, the public and private sectors including beauty shops, and alumni associations handling personal information were required to be adjusted to the same standard. Since enforcement of the law, residence registration number is categorized as sensitive information which is prohibited from collection. This also applies to any person handling credit card information, thereby stopping them from requesting sensitive information. A major change was needed since personal information has enormous economic value and had become the target of misuse and abuse resulting in mental and financial damage such as identity theft and phone fraud as well as invasion of privacy of people. This law adjusted the standard of international society at the time.

5. Alignment of the Indonesian PDP Law with ASEAN Framework on Personal Data Protection

Indonesia as an ASEAN member state is also committed to strengthening the protection of personal data in the ASEAN region by facilitating cooperation among other ASEAN member states. This is because personal data security is one of the important agendas for ASEAN because several ASEAN member states are regarded as the "centers" of

[20] The Constitutional Court of South Korea Decision 99Hunma513, 2004Hunma190.

[21] Haksoo Ko et al., "Structure and Enforcement of Data Privacy Law in South Korea," *International Data Privacy Law* 7, no. 2 (2017): 100–114, https://doi.org/https://doi.org/10.1093/idpl/ipx004.

[22] Ibid, p. 1.

[23] Ibid, p. 4.

[24] The Credit Information Use and Protection Act (Credit Information Act) of 1995.

dangerous internet activities.[25] This occurs due to low security capabilities and regulations regarding cyber security in these states. In addition, several other reasons such as the lack of industry capability in the field of cyber security and the assumptions of entrepreneurs who think that cybercrime is not a priority must be taken seriously. To respond to the cyber security issues, ASEAN member states have agreed to form a joint agreement, namely the "Framework on Personal Data Protection" which is the basis for personal data protection.

Among the ten member states of ASEAN, namely Viet Nam, Brunei, Malaysia, Singapore, Thailand, Indonesia, Cambodia, Laos, Myanmar and the Philippines, only five states have passed personal data protection regulations, namely, Malaysia under the Personal Data Protection Act 2010 (PDPA 2010), Singapore under the Personal Data Protection Act (PDPA) 2013), Philippines under Republic Act No 10173: Act Protecting Individual Personal Information in information and Communications Systems in the Government and Private Sector, Creating For this purpose A National Privacy Commission, and for other Purposes (2013), Thailand under the Personal Data Protection Act B.E 2562 (2019) and Indonesia under Law Number 27 2022 concerning Protection of Personal Data (2022).

Despite the issuance of the laws on personal data protection in the five ASEAN Member States, data leakages continue to exist in Malaysia in 2019,[26] Singapore in 2021,[27] the Philippines in 2021,[28] Thailand in 2021[29] and Indonesian in 2022.[30] The incidents are evidence that the ASEAN region is an area facing the threat of cyber security.[31] ASEAN has realized the importance of protecting personal data since the digital world is very easy to access by anyone.[32] Hence, the "ASEAN Framework on Personal Data Protection"[33] is expected to reduce and increase the awareness of its member states to protect the personal data of their citizens.

[25] Trisa Monika Tampubolon and Rizki Ananda Ramadhan, "ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital Pada Asia Tenggara," *Padjadjaran Journal of International Relations* 1, no. 3 (2020): 270–86, https://doi.org/https://doi.org/10.24198/padjir.v1i3.26197.

[26] Caesar Akbar, "Data Malindo Air Bocor, Kominfo: Lion Air Indonesia Tidak Terkait," Tempo.co, 2019, https://bisnis.tempo.co/read/1253100/data-malindo-air-bocor-kominfo-lion-air-indonesia-tidak-terkait.

[27] Serafina Indah Chrisanti, "Kronologi Kebocoran Data Pelanggan RedDoorz Singapura Dan Asia Tenggara," The South East Islands Times, 2021, https://seitimes.com/kronologi-kebocoran-data-pelanggan-reddoorz-singapura-dan-asia-tenggara/.

[28] Vittoria Elliott, "345,000 Sensitive Legal Documents from the Philippines Government Have Been Exposed Online," Rest of World, 2021, https://restofworld.org/2021/philippines-data-exposure/.

[29] A. H. Kholis, "Data Pribadi 100 Juta Turis Yang Datang Ke Thailand 'Bocor,'" Indonesiainside.id, 2021, https://indonesiainside.id/tekno/2021/09/23/data-pribadi-100-juta-turis-yang-datang-ke-thailand-bocor.

[30] Ifra Wahyuni, "Kemunculan Kasus Hacker Bjorka, Begini Payung Hukumnya," Suara Kampus, 2022, https://suarakampus.com/kemunculan-kasus-hacker-bjorka-begini-payung-hukumnya/.

[31] Trisa Monika Tampubolon and Rizki Ananda Ramadhan, "ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital Pada Asia Tenggara," *Padjadjaran Journal of International Relations* 1, no. 3 (2020): 270–86, https://doi.org/https://doi.org/10.24198/padjir.v1i3.26197.

[32] Nurul A. Shamsuri, "Proposal on Regional Data Protection for ASEAN" (Utrecht University, n.d.).

[33] ASEAN Framework on Personal Data Protection, 2016.

The commitment of Indonesia as an ASEAN member state has been reflected by incorporating the "ASEAN Framework on Personal Data Protection" into the PDP Law even though the wording of the ASEAN Framework is not the same, as follows:

a. Consent, Notification and Purpose under the ASEAN Framework are integrated under Article 20 of the PDP Law.
b. Accuracy of Personal Data under the ASEAN Framework is also narrated by Article 6 of the PDP Law.
c. Security Safeguards under the ASEAN Framework is clearly stipulated by Article 35 of the PDP Law.
d. Access and Correction under the ASEAN Framework is governed by Article 7 of the PDP Law.
e. Transfers to Another Country or Territory under the ASEAN Framework is also similarly regulated by Article 56 of the PDP Law.
f. Retention under the ASEAN Framework requires an organization should cease to retain documents containing personal data if it is reasonable to assume that the retention is no longer necessary for legal or business purposes. This requirement can be found under Article 43(1) of the PDP Law.
g. Accountability under the ASEAN Framework as reflected by Article 5 of the PDP Law.

6. Alignment of the South Korean PIPA with EU General Data Protection Regulation

After the enforcement of the General Data Protection Regulation (GDPR)[34] in 2018, binding all member states of the European Union (EU), South Korea also had to adjust to the new international standard. The EU's GDPR became the model for the revision, Korea also set the principles for the law and rules for their applicability outside of Korea. Focusing more toward protection of personal information than data economy, industry voiced difficulty in their ability to be ready for the changes, because it required technical equipment and software that needed a sizeable budget, whereas consumers became more cautious of their rights on privacy seeing the performance of protecting personal information as part of quality of the company. Inconsistency of performance among companies is still an ongoing process of adjustment taking time.

In 2020, the so-called three Data Acts, namely the PIPA of 2011, IC Network Act, and Credit Information Act went through major amendments. This merging of the three Data Acts amendments created major changes for companies.[35] Before the three Data Acts amendment, public entities held a major liability for data protection. Since this amendment, the responsibility of the company handling personal information became

[34] Paul Sutton, "Data Protection in South Korea: Why You Need to Pay Attention," Vistra, 2018, https://www.vistra.com/insights/data-protection-south-korea-why-you-need-pay-attention.

[35] Kim & Chang, "Major Amendments to Three Data Privacy Laws: Implications," Kim & Chang, 2020, https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=20726.

official. This became the headstone of the data-based economy of Korea until the major revision which will apply in September 2023.

This amendment made it a little easier for companies handling personal data and providers of information and communication services or similar services in handling information because the concept of pseudonymised information was introduced. The use of pseudonymised information,[36] in this case, made it possible to use personal information without the data subject's consent thereto, for scientific research purposes, statistical purposes, and archiving purposes in the public interest, and so on. Pseudonymised information is a type of personal information whereby individuals cannot be identified without additional information by deleting part of the personal information or replacing part of or all the personal information.

Hence, the data controller must decide whether the information should be handled without anonymization or not, then pseudonymisation or not. Criteria are given in article 3. It states "If it is still possible to fulfil the purposes of collecting personal information by processing anonymized or pseudonymised personal information, the personal information controller shall endeavour to process personal information through anonymization, where anonymization is possible, or through pseudonymisation, if it is impossible to fulfil the purposes of collecting personal information through anonymization". An example of anonymized information might read 'xx Park, having date of birth Jan. 3rd, 1999, living in Busan, Korea, spending Shinhan credit card 3,000 dollars, Samsung credit card 2000 dollars in 2023, January' making it difficult for the information user to specify the individual. Pseudonymized information is 'female, fortysomething, spending Shinhan credit card 3,000' making it impossible to specify the individual and thus the data has no economic value.

This amendment also introduced a major improvement by expanding the scope of sensitive information. Sensitive information is information on ideology, creed, affiliation with/withdrawal from a labor union and political party, political opinions, health, sex life, etc. The 2020 Amended (Enforcement Decree of the Personal Information Protection Act) additionally included information generated through certain technical means for the purpose of identifying a particular individual, for example, information on the physical, physiological, and behavioral characteristics of individuals, and information about a race or ethnic group, in the existing scope of sensitive information. Art. 23 set the limitation where the controller has to stop when information is within the scope of sensitive information. The criterion for the decision is 'likely to markedly threaten the privacy of any data subject'. Unless the process is approved by another law or separate consent, the controller must stop at this point from collecting the personal information.

PIPA has a similar structure to the GDPR. In June 2021, the European Commission published its draft adequacy decision for South Korea and the European Data Protection Board made a decision based on this report. As a result of the adequacy decisions[37],

[36] Shin & Kim, "PIPC's Amendment to the Guidelines on Processing Pseudonymized Data," Shin & Kim, 2022, https://www.shinkim.com/eng/media/newsletter/1834.

[37] European Commission, "Data Protection: European Commission Launches the Process Towards Adoption of the Adequacy Decision for the Republic of Korea," European Commission, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.

personal data collected at the EU can be used in Korea without further restriction. Korea is now heading to the second regular adequacy review since the adequacy decision is re-examined every four years. More amendments to PIPA[38] were expected to be made for the second adequacy decision by the EU.

On March 14, 2023, a complete amendment was announced. It is expected to be enforced on September 15 of 2023, except for some provisions which will only be enforced in 2024. Individuals, enterprises and government, all three interested parties, are considered for the revision as well as the EU GDPR second review. When the new law applies, data subjects will have a right to request the transfer of personal information to a personal information management institution, or a facility that fulfills the obligation to take safety measures and meets the facilities and technical standards prescribed by the Presidential Decree. This right to data portability is going to be adopted in the second complete amendment. This is similar to GDPR Art. 12, Art. 20, Recital 68 right to portability.

Automated individual decision-making including profiling can be objected to by the data subject with the adoption of the second complete amendment. Recently, ChatAI program has evolved greatly, and automated decision-making using artificial intelligence may have a significant impact on the rights of the data subject[39] who may reject it or request an explanation of the decision. GDPR Art. 22 states that "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling…." Compared to the GDPR, PIPA included a process of rejection and explanation instead of the inherent right of not being the object of automated processing. Non-Government Organizations (NGOs) in Korea claim that this is a big retreat giving much more favorable outcomes to enterprises. GDPR blocks automated individual decisions on principle, allowing exceptions, whereas the 2023 revision of PIPA allows automated individual decisions as a principle unless the data subject uses his right to reject or request an explanation.

Furthermore, the 'same action-same rule' principle became reality. When the new law is enforced, online service providers and offline service providers will be regulated by the same rule. Currently, online service providers who are 'providers of information and communication service' which is defined through the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc have special provisions.[40] Preparing for the great popularity of the portable device service, the definition of movable image data processing devices is introduced. The drone and autonomous vehicle industry are welcoming the change.

[38] Jisun Kim, "'Data Law Amendment a Priority for Introducing Korean Version of "ChatGPT,"'" Korea IT News, 2023, https://english.etnews.com/20230131200003.

[39] Jihyun Park and Dodik Setiawan Nur Heriyanto, "Immigration Exemptions Provision of UK Data Protection Act and Personal Information Protection," *Hongik Law Review* 23, no. 3 (2022): 391–417.

[40] Personal Information Protection Act (PIPA-Second Amendment).

The scope of criminal sanctions will be changed.[41] Some of the criminal sanctions imposed on the processor will be lifted and changed to administrative penalties.[42] However, a processor who uses the personal data of a child below the age of 14 without consent and a processor who refuses, interferes with, or evades an investigation by concealing, discarding, denying access to, or forging or altering data during access or inspection by public officials may be punished with a newly adopted criminal sanction provision.

One of the biggest changes that will be made in the near future is the use of personal data abroad. Currently, the data subject's 'consent' is the only way to use personal information outside of Korea. The revision allows special provisions in laws, and treaties to which the Republic of Korea is a party or other international agreements. It also allows cases of consignment and storage of personal information that is necessary for the conclusion and execution of contracts with data subjects when certain conditions are met. Independent decisions of the PIPC on the equivalence to the level of personal information protection under the PIPA will play a role in bridging the understanding of international society and each different country.[43] This seems to be a big retreat to the individual who does not understand the terms and conditions of the service. For this purpose, the revision will also add the possibility of a suspension order for personal data transfer.[44]

This new 2023 revision of PIPA will be enforced from September 15, 2023, with some exception clauses. Korea PIPA will become closer to the GDPR model by adopting changes made in international society.

7. Similarities and Differences of PDP Law and PIPA

Based on the examination of the two laws pertaining to the protection of personal data, it can be generally summarized as follows:

a. PDP Law consists of 16 chapters, namely Chapter I: General Provisions, Chapter II: Principles, Chapter III: Types of Personal Data, Chapter IV: Rights of Personal Data Subjects, Chapter V: Processing of Personal Data, Chapter VI: Obligations of Personal Data Controllers And Processors in Processing Personal Data, Chapter VII: Personal Data Transfer, Chapter VIII: Administrative Sanctions, Chapter IX: Institutions, Chapter X: International Cooperation, Chapter XI: Society Participation, Chapter XII: Dispute Resolutions and Procedures, Chapter XIII: Restrictions in the Use of Personal Data, Chapter XIV: Criminal Provisions, Chapter XV: Transitional Provisions, Chapter XVI: Closing Provisions.

b. PIPA contains 10 Chapters, namely Chapter I: General Provisions, Chapter II Establishment of Personal Information Protection Policies, Etc., Chapter III: Processing of Personal Information, Chapter IV: Safeguard of Personal

[41] Article 34-2 Personal Information Protection Act (PIPA-Second Amendment).
[42] Article 71(1)(3) Personal Information Protection Act (PIPA-Second Amendment).
[43] Article 28-8 Personal Information Protection Act (PIPA-Second Amendment).
[44] Article 28-9 Personal Information Protection Act (PIPA-Second Amendment).

Information, Chapter V: Guarantee of Rights of Data Subjects, Chapter VI: Special Cases Concerning Processing of Personal Information by Providers of Information and Communications Services or Similar, Chapter VII: Personal Information Dispute Mediation Committee, Chapter VIII: Class-Action Lawsuit Over Data Infringement, Chapter IX: Supplementary Provisions, Chapter X Penalty Provisions.

To be more specific regarding the alignments between the two laws, Table 1 below is presented. However, the following lists under Table 1 are not deemed to be exhaustive lists.

Table 1. Similarities and Differences of PDP Law and PIPA.

Aspects	PDP Law	PIPA	Remarks
General Provisions Definitions of Terms	Art 1. Definitions	Art.1. Purpose Art. 2. Definitions	Art.1 of PIPA contains the purpose of this Act which is to protect the freedom and rights of individuals, and further, to realize the dignity and value of the individuals, by prescribing the processing and protection of personal information. <Amended by Act No. 12504, Mar. 24, 2014> Both PDP Law and PIPA contain specific terms which are used in the two laws.
Scope of Application & Exemption	Art. 2(1) Territory and Jurisdiction of Application. Art. 2(2) Exemption of Application	Art. 58. Application of Partial Exclusion of Application Art. 58-2 Exemption from Application	Art 2(2) of PDP Law shall not apply to processing of Personal Data by natural persons in activities personal or household. Article 58-2 shall not apply to information that no longer identifies a certain individual when combined with other information, reasonably considering time, cost, technology, etc. This Article was newly inserted by Act No. 16930, Feb. 4, 2020.
Principles Type of Personal Data	Art. 3 Principles Art. 4. Types of Personal Data: Specific and General Personal Data	Art. 3 Principles Art. 2(1)(a),(b),(c) defines "personal information." Art. 23 defines sensitive information including ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life.	The same on the principles Both laws adopt the negative listing style.

Rights of Data Subjects	Art. 5. Right to Obtain Information Art. 6. Right to Correct Errors Art. 7. Right to obtain a Copy Art. 8. Right to delete Art. 9. Right to withdraw Art. 10. Right to object Art. 11. Right to delay Art. 12. Right to sue Art.13, Right to obtain e-file	Art. 35. Access to Personal information Art. 36. Rectification or erasure of personal information Art. 37. Suspension of processing personal information Art. 38 Methods and procedures for exercise of rights	Obtaining the information through e-file system is mentioned by PDP Law only.
Submission of Application	Art. 14. Submission by electronic or non-electronic to the Data Controller Personal	Art. 35 request to access to his or her personal information controller. In case of public institution, direct request to public institution or protection commission is open.	PIPA does not specify the type of submission, i.e. electronic and non-electronic.
Exclusion of Rights	Art. 15 and Art. 50 Exclusion applies with the reason of (a) national defence and security, (b) the interest of law enforcement process,(c) public interest in the context of state administration, (d) the interest of supervision of the sectors of financial services etc, (e) the interest of statistics and scientific research to the Art. 8, Art. 9, Art 10 para(1), Art. 11, Art.13 para(1), (2). The same exclusion applies Art. 30, Art.32, Art. 36, Art. 42, Art. 43 para (1), Art. 44 para(1) letter b, Art. 45, Art. 46	Art 17 states 'within the scope reasonably related to the purposes to the purposes for which the personal information was initially collected' and Art.18 states limitation to Out-of-Purpose Use. When the case fits, they do not require separate consent. Art. 28-2 (Processing pseudonymous data) states processing the data without consent. Art. 35 (access to personal information) states limitation and denying access. Chap. VI. (by providers of information and communications services or similar) has special exemption. Art. 58 (partial exclusion of application) states public institution collection, national security purpose, public safety and security, public health purpose,	PIPA specifically regulates pseudonymous data.

	para(1) letter a except (e)	reporting by the press, missionary activities by religious organizations and nomination of candidates by political parties, visual data processing devices exclusion, association for friendship such as alumni association and a hobby club exclusion.	
Processing of Personal Data	Art. 16 (1) data processing (2) personal data protection principles	Art. 3 mentions principles	The same on the principles
Installation of Processing Equipment or Visual Data Processing	Art. 17 visual data processing for: 1) Security, disaster prevention and /or traffic management 2) Prevention of crimes and law enforcement process	Art. 25 limitation to installation and operation of visual data process devices	PIPA allows installing visual data processing devices in case of 1) specifically allowed by statute 2) prevention and investigation of crimes 3) safety of facilities and prevention of fire 4) collection, analysis and provision of traffic information
2 (two) or more Personal Data Controllers	Art. 18 Two or more personal data controllers Art. 37 supervision of Data Controller	Art. 28 supervision of personal information handled by a data controller	Two controller concept is new. PIPA limits the controller to a minimum number prefe rably one controller supervises handlers.
Obligation of Personal Data Controller and Processor	Art. 20 The Personal Data Controller must have a basis processing of Personal Data	Chapter III Processing of Personal Information Section 1 Collection, Use, Provision, etc. of Personal Information.	PIPA provides a detailed elaboration relating to the obligations of the personal data controller. Yet, in principle it is similar to PDP Law which requires consent of the data subject and it must not contravene the existing laws.
Methods of Obtaining Consent	Art. 22 Methods of obtaining consent Art. 23 explicit valid consent Art. 24 proof of consent Art. 25 child personal data	Art. 22 Methods of obtaining consent	Similar in principle that a request can be clearly distinguished from other matters and made in understandable format.
Person with Disability	Art. 26 person with disability	Not Available	PIPA does not consider persons with disabilities as a separate group.
Storage Period of Personal Data	Art. 32 no later than 3 x 24 (three times twenty-four) hours	Different period applies to different entities.	PIPA allows different time frame of storage for different entities. PIPA is framework legislation so special law e.g.

	starting from the time the Personal Data Controller receives access request.		health law supersedes the privacy law. Therefore, in the case of the image Clinical Decision (CD) such as Magnetic resonance imaging (MRI), Computed Tomography (CT) scan of a patient, a hospital is allowed to keep it for 10 years.
Privacy Impact Assessment	Art. 34 Privacy Impact Assessment	Art. 33. Privacy Impact Assessment	Similar in principle.
Confidentiality	Art. 36 Confidentiality	Art. 60 Confidentiality	Similar in principle
Regulatory Body	Art. 58 Institution	Article 7 Personal Information Protection Commission	PDP Law does not clarify the name of the institution.
Dispute Resolution	Art. 64 Arbitration, courts, or other alternative dispute resolutions.	Chapter VII Personal Information Dispute Mediation Committee Article 51 (Parties to Class Action Lawsuit) may use court to file a lawsuit.	PIPA specifies that courts may entertain a class action.
Penalty	Art. 67 – Art. 73 Criminal sanctions, fines and administrative sanctions.	Art. 70 – Art.76 Criminal sanctions, fines, administrative fines.	Both Laws provide penalty provisions. Yet, the amount of fine is different. PDP regulates that an imprisonment of a maximum of 5 (five) years and/or a fine of a maximum of IDR 5,000,000,000.00 (five billion rupiah) may be imposed. PIPA states that imprisonment with labor for not more than 10 years, or by a fine not exceeding 100 (one hundred) million won may be imposed.

Source: Compiled and analyzed by researchers, 2023.

Based on Table 1, it can be deduced that both PDP Law and PIPA are similar in principle. They have a broad scope of application since they apply to personal data processing in the two countries respectively. In addition, they also regulate the transfer of personal data overseas. Both laws adopt the negative listing style in governing the type of personal data. Although there are different terms used by the two countries' laws, they both apply to personal data controllers and processors. It must be noted here that PIPA of South Korea adopts the term "personal information controller".

In relation to data subject protection, both laws render the rights of data subjects. They also recognize sensitive personal data that must be protected. However, the criteria for this particular data is somewhat different. PDP Law emphasizes that personal data that may lead to discrimination, such as religious affiliation, race, and sexual orientation falls within "sensitive personal data". The PIPA has different criteria as it stipulates personal information that may result in harm if leaked, such as medical records, financial information, and social security numbers constitute "sensitive personal information". In this regard, there is a fundamental difference between the approach of the two laws. PDP

Law stresses on "likely to markedly threaten the privacy of the data subject", whereas the PIPA emphasized more on "harm or damage", when the sensitive personal data/information is leaked. Nevertheless, they both require "explicit consent from individuals before sensitive personal data or information can be collected, processed, or transferred" with some exceptions.

PDP Law and PIPA adopt similar principles in the sense that personal data/information must be given explicit consent by data subjects prior to collecting and processing such data/information by data controllers and processors. In this regard, the two laws stipulate that the principle of lawfulness, fairness, and transparency must exist. The principle of lawfulness means that personal data/information must be collected and processed for specified and legitimate purposes, consequently it cannot be used for any other purposes unless there is explicit consent from the data subject that it can be used beyond the collected purposes.

In this conjunction, the principles of fairness and transparency are fulfilled. Although a data subject has given his/her explicit consent to use his/her data, yet both laws require that both data controllers and processors must apply appropriate and adequate organizational and technical measures to ensure that such personal data is secure and confidential. The rights of the data subject are recognized and respected, therefore the two laws provide detailed rights conferred on the data subject. However, PIPA opens the doors to the non-consensual use of personal information outside of the original consent. This is discussed below. The owner of data (data subject) may exercise the rights and he/she has full access to the data which is held by data controllers and processors. Accordingly, he/she has also rights to correct, delete or block his/her personal data if such data is considered to be "inaccurate, incomplete, outdated, or unlawfully processed".

Both the PDP Law and PIPA provide that an institution is established to investigate and sanction data controllers and processors that violate these laws. It is unfortunate that PDP Law does not specifically name the institution, unlike PIPA which states that the Personal Information Protection Commission (PIPC) has the authority to deal with matters relating to personal data regulated under the PIPA. In relation to the violation of the PDP Law and PIPA, they both stipulate that alternative dispute resolutions (APS) and courts may be used as dispute settlement mechanisms. Yet, the PIPA limits the APS to the use of mediation only. PDP Law permits the utilization of arbitration to deal with personal data violations. Both laws impose criminal and administrative sanctions on data controllers and processors who violate the respective laws. Yet, there are differences in the amount of fines and imprisonment period provided by the two laws.

Despite the above-mentioned similarities, both laws have inherent differences which can be elaborated as follows:

a. Different terms and definitions are adopted by the PDP Law and PIPA. PDP Law uses the term "personal data controllers and processors". PIPA adopts the term "personal information controllers and processors".
b. PDP Law specifies the scope of application upon territory point (PDP Art.2). PIPA specifies in a negative way by saying that "this law shall not apply to information that no longer identifies a certain individual when combined with other

information, reasonably considering time, cost, technology, etc" (PIPA Art. 58-2). For the hierarchy, the protection of personal information shall be governed by PIPA except otherwise specifically provided for in other Acts (PIPA Art. 6).

c. PDP Law applies to both private and public entities, including government agencies that process personal data. In contrast, PIPA merely applies to private entities. Yet, it provides that there may be some exceptions for government agencies that process personal data/information for specific purposes.

d. Roles of PIPC (Personal Information Protection Commission (PIPA Chapter II). PIPC handles personal information related questions from individuals to government agencies as the controlling power with full power under direct supervision of the prime minister. Although PIPC is an independent public entity, it directly reports and receives requests from the president because personal information has become of great interest in Korea. PIPC covers policy establishment for education of the people. The Indonesian agency establishment is stated by PDP Law under Art.58, 59, 60, 61, specific provisions are referred to Presidential Regulation, not by the Law itself.

e. PIPA emphasizes that public entities have a bigger responsibility toward protection of personal information, so the PIPC supervises public entities as much as data controller other than public entity such as legal person, organization, individual. More leaks from inside than hacking from the outside at a ratio of 6:4 in 2022 in South Korea led to stricter inspection of public entities more than ever and made any public officer who breaches the personal information protection act once by leaking leads to a dismissal. This also refers to the "one-strike out system for public officers".

f. The approaches to partial exclusion of application of the two laws are different in relation to 1) Personal information collected pursuant to the Statistics Act for processing by public institutions; 2) Personal information collected or requested to be provided for the analysis of information related to national security; 3) Personal information processed temporarily where it is urgently necessary for public safety and security, public health, etc.; 4) Personal information collected or used for its own purposes of reporting by the press, missionary activities by religious organizations, and nomination of candidates by political parties, respectively. For the purpose of applying visual data processing devices, collection and use (Art.15), methods of obtaining consent (Art.22) limitation to transfer of personal information following business transfer (Art. 27(1), (2), data breach notification (Art. 34), suspension of processing of personal info provision (Art. 37) of PIPA are alien to PDP Law. Similarly, for the purpose of operating a group or association for friendship, such as an alumni association and a hobby club, collection and use (Art.15), establishment and disclosure of privacy policy (Art. 30), designation of privacy officers (Art. 31) are not adopted by PDP Law.

g. The out-of-purpose use has been articulated separately by PIPA when a data controller may use it later with a different purpose including the use by a third party. For this purpose, 1) additional consent, 2) special provision under another law 3) in case where it is deemed manifestly necessary for the protection of life,

bodily or property interests of the data subject or third party from imminent danger where the data subject or his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses. 4) where it is impossible to perform the duties under its jurisdiction as provided for in any Act, unless the personal information controller uses personal information for other purpose than the intended one, or provides it to a third party, and it is subject to the deliberation and resolution by the Commission; 5) where it is necessary to provide personal information to a foreign government or international organization to perform a treaty or other international convention; 6) where it is necessary for the investigation of a crime, indictment and prosecution; 7) where it is necessary for a court to proceed with trial-related duties; 8) where it is necessary for the enforcement of punishment, probation and custody.

Based on the detailed explanations regarding the similarities and differences of the two laws, it is obvious that both the PDP Law and PIPA are similar in principle in the sense that they apply to personal data processing and render rights to data subjects. They also adopt similar principles since they require explicit consent from data subjects before data controllers and processors collect and process such data/information. Furthermore, they provide for an institution to investigate and sanction data controllers and processors if they violate the laws. However, both laws have inherent differences because the PDP Law uses the term “personal data controllers and processors”, while the PIPA adopts the term “personal information controllers and processors”. The PDP Law has a specific provision for the disabled, which PIPA does not provide. The PIPC establishment and roles are regulated in detail under the PIPA, whereas the Indonesian agency establishment stated by the PDP Law will be further governed by Presidential Regulation.

8. Conclusion

Protection of personal data in Indonesia and South Korea has established a new approach through the PDP Law of Indonesia and the South Korean PIPA. The PDP Law has reflected and incorporated the "ASEAN Framework on Personal Data Protection", whereas the South Korean PIPA has been reviewed for its second regular GDPR adequacy by the EU. Both the PDP Law and PIPA share similarities because they apply to personal data processing, render rights to data subjects, require explicit consent from data subjects and provide for an institution to investigate and sanction data controllers and processors if they violate the laws. However, they also have differences because the PDP Law provides a provision for the disabled, but it does not exist in PIPA. The detailed PIPC establishment and roles are provided by the PIPA, whereas the establishment of Indonesian agency will be further governed by Presidential Regulation. Apart from the two laws’ similarities and differences, it is suggested that Indonesia should learn from the strategies of South Korea on how to obtain the GDPR adequacy, so it can be ensured that personal data protection in Indonesia is recognized world-wide. As for South Korea, it is suggested that the PIPA puts a strong emphasis on the performance of government agencies in handling citizens’ personal data.

Acknowledgements

We would like to convey our gratitude to the South Korean government for its grant to fund this research. This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2020S1A5A2A03040483).

References

Akbar, Caesar. "Data Malindo Air Bocor, Kominfo: Lion Air Indonesia Tidak Terkait." Tempo.co, 2019. https://bisnis.tempo.co/read/1253100/data-malindo-air-bocor-kominfo-lion-air-indonesia-tidak-terkait.

Anggriawan, Rizaldy, Andi Agus Salim, Yordan Gunawan, and Mohammad Hazyar Arumbinang. "Passenger Name Record Data Protection under European Union and United States Agreement: Security over Privacy?." *Hasanuddin Law Review* 8, no. 2 (2022): 95-110ASEAN Framework on Personal Data Protection, 2016.

BBC News Indonesia. "BPJS Kesehatan: Data Ratusan Juta Peserta Diduga Bocor - 'Otomatis Yang Dirugikan Masyarakat', Kata Pakar." BBC News Indonesia, 2021. https://www.bbc.com/indonesia/indonesia-57196905.

Chrisanti, Serafina Indah. "Kronologi Kebocoran Data Pelanggan RedDoorz Singapura Dan Asia Tenggara." The South East Islands Times, 2021. https://seitimes.com/kronologi-kebocoran-data-pelanggan-reddoorz-singapura-dan-asia-tenggara/.

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

Elliott, Vittoria. "345,000 Sensitive Legal Documents from the Philippines Government Have Been Exposed Online." Rest of World, 2021. https://restofworld.org/2021/philippines-data-exposure/.

European Commission. "Data Protection: European Commission Launches the Process Towards Adoption of the Adequacy Decision for the Republic of Korea." European Commission, 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.

Hadjon, Philipus M., and Tatiek Sri Djatmiati. *Argumentasi Hukum*. Yogyakarta: Gadjah Mada University Press, 2017.

Hardiansyah, Zulfikar. "Rentetan Aksi Hacker Bjorka Dalam Kasus Kebocoran Data Di Indonesia Sebulan Terakhir." KOMPAS.com, 2022. https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker-bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan?page=all.

Irwansyah. *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Yogyakarta: Mirra Buana Media, 2021.

Jung-Woo, Cho. "LG U+ Customer Data Hacked, 180,000 Affected." Korea JoongAng Daily, 2023. https://koreajoongangdaily.joins.com/2023/01/10/business/industry/korea-LG-U-data-breach/20230110184232830.html.

Kholis, A. H. "Data Pribadi 100 Juta Turis Yang Datang Ke Thailand 'Bocor.'" Indonesiainside.id, 2021. https://indonesiainside.id/tekno/2021/09/23/data-pribadi-100-juta-turis-yang-datang-ke-thailand-bocor.

Kim & Chang. "Major Amendments to Three Data Privacy Laws: Implications." Kim & Chang, 2020. https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=20726.

Kim, Jisun. "'Data Law Amendment a Priority for Introducing Korean Version of "ChatGPT."'" Korea IT News, 2023. https://english.etnews.com/20230131200003.

Ko, Haksoo, John Leitner, Eunsoo Kim, and Jonggu Jeong. "Structure and Enforcement of Data Privacy Law in South Korea." *International Data Privacy Law* 7, no. 2 (2017): 100–114. https://doi.org/https://doi.org/10.1093/idpl/ipx004.

Mahardika, Ahmad Gelora. "Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi Dalam Sistem Ketatanegaraan Indonesia." *Jurnal Hukum* 37, no. 2 (2021): 101–18. https://doi.org/http://dx.doi.org/10.26532/jh.v37i2.16994.

Makarim, Edmon. *Kompilasi Hukum Telematika*. Jakarta: Raja Grafindo Persada, 2003.

Mutiara, Upik, and Romi Maulana. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi." *Indonesian Journal of Law and Policy Studies* 1, no. 1 (2020): 42–54. https://doi.org/http://dx.doi.org/10.31000/ijlp.v1i1.2648.

Park, Jihyun, and Dodik Setiawan Nur Heriyanto. "Immigration Exemptions Provision of UK Data Protection Act and Personal Information Protection." *Hongik Law Review* 23, no. 3 (2022): 391–417.

Pusat Bahasa Departemen Pendidikan Nasional. *Kamus Besar Bahasa Indonesia*. Jakarta: Balai Pustaka, 2001.

R, Mei Amelia. "Duh! Sales Kartu Kredit Gadungan Ini Gunakan Uang Haram Buat Naik Haji." detiknews, 2016. https://news.detik.com/berita/d-3158671/duh-sales-kartu-kredit-gadungan-ini-gunakan-uang-haram-buat-naik-haji.

Sanusi, Muhammad Arsyad. *Teknologi Informasi & Hukum E-Commerce*. Jakarta: Dian Ariesta, 2004.

Shamsuri, Nurul A. "Proposal on Regional Data Protection for ASEAN." Utrecht University, n.d.

Shin & Kim. "PIPC's Amendment to the Guidelines on Processing Pseudonymized Data." Shin & Kim, 2022. https://www.shinkim.com/eng/media/newsletter/1834.

Sutton, Paul. "Data Protection in South Korea: Why You Need to Pay Attention." Vistra, 2018. https://www.vistra.com/insights/data-protection-south-korea-why-you-need-pay-attention.

Tampubolon, Trisa Monika, and Rizki Ananda Ramadhan. "ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital Pada Asia Tenggara." *Padjadjaran Journal of International Relations* 1, no. 3 (2020): 270–86. https://doi.org/https://doi.org/10.24198/padjir.v1i3.26197.

Wahyuni, Ifra. "Kemunculan Kasus Hacker Bjorka, Begini Payung Hukumnya." Suara Kampus, 2022. https://suarakampus.com/kemunculan-kasus-hacker-bjorka-begini-payung-hukumnya/.

Wignjosoebroto, Soetandyo. *Hukum, Konsep, Dan Metode*. Malang: Setara Press, 2013.

Wiryono, Singgih. "SAFEnet: 1,3 Miliar Data Pengguna SIM Card Diduga Bocor Jadi Kasus Terbesar Di Asia." KOMPAS.com, 2022. https://nasional.kompas.com/read/2022/09/09/16180311/safenet-13-miliar-data-pengguna-sim-card-diduga-bocor-jadi-kasus-terbesar-di.