INDONESIAN COMPARATIVE LAW REVIEW

Volume 2 No 2, June 2019
P-ISSN: 2655-2353, E-ISSN: 2655-6545

Article Info:
Received : 02-09-2019
Revised : 17-03-2020
Accepted : 07-08-2020

http://dx.doi.org/10.18196/iclr.2219

Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore

Diana Setiawati[1], Hary Abdul Hakim[2], Fahmi Adam Hasby Yoga[3]

[1, 2]*Financial and Economic Law Department, Asia University, Taiwan*

[3]*International Program of Internationa Relation, Universitas Muhammadiyah Yogyakarta, Indonesia*

Email: [1]*diana.setiawati96@gmail.com*
[2]*haryabdulhakim7@gmail.com*
[3]*fahmiadamhasbyyoga@gmail.com*

Abstract

Industrial revolution 4.0 offers both opportunities and challenges to all countries, including Indonesia. Personal data protection is necessary to encourage digital innovation. The existing regulation relating to personal data in Indonesia does not give sufficient protection especially with regard to the use of artificial intelligence and therefore is inadequate to encourage digital economic development. This paper aims to explore the importance of strong data protection regulation in Indonesia. This normative legal research employs comparative approach. Comparative study was made upon the development of personal data protection regulation in China, South Korea and Singapore. The study shows that these countries provide good lesson for Indonesia to learn in developing personal data protection regulation.

Keywords: *artificial intelligence; big data; data protection regulation; digital innovation*

1. . Introduction

Artificial Intelligence (AI) is a developing technology or system that enabling a computer to perform tasks involving a simulation of human intelligence, including decision making or learning. In order to do so, the technology or system collects voluminous amounts of data (called Big Data) and namely, personal data.[1] For example, AI may conduct for identifying images, recognizing speech, identifying relevant information in texts drawing conclusion, and forecasting. This fact strongly proves that there is no doubt that big data is an important component that cannot be separated from AI, which will be a game-changer for businesses and governments around the world.[2]

The major states hubs of AI development are the United States and China which have pioneered in many applications. ASEAN countries still lag behind,

[1] Mathias Avocats. (2017). *Artificial Intelligence and the GDPR: How do they interact?*. available from: https://www.avocats-mathias.com/technologies-avancees/artificial-intelligence-gdpr. [Accessed April 5, 2019].

[2]Corinium. (2018). *Big Opportunities for Big Data in the Asia Pacific*. available from: https://www.coriniumintelligence.com/insights/big-opportunities-for-big-data-in-the-asia-pacific/. [Accessed April 5, 2019].

but there is AI activity in each member state. Singapore has made the greatest advances, but there are also promising early signs in places like Malaysia and Vietnam, where some progress have been made.[3]

Based on research conducted by the Asian business leaders and human resource and AI professionals, AI's future will cleave much more closely to the positive outcome, moreover, in approaching quickly to such diverse sectors as manufacturing, transportation and financial services. [4] However, these same technological innovations raise important issues, including questions about how to deliver practical compliance with data protection laws and norms when building and implementing AI technology and on the tension between AI and existing data protection legal requirements.[5]

The lack of concern to data protection is currently the main problem in promoting AI, the idea of the right to privacy was first recognized during in 1890 according to Samuel Warren, and Louis Brandeis argued to the recognition of an individual's "such as right to be let alone", the right to liberty secure and privacy may be protected by the law.[6]

In this digital era, people will often use online facilities that require services to enter personal data. In reality, it is still very often encountering theft of personal data by certain individuals. Therefore, the Indonesian government tried to anticipate by pushing the Personal Data Protection Bill. With the existence of these laws, collection, storage, and utilization of personal data will be regulated in order to protect privacy rights.

The Personal Data Protection Act in Indonesia is still a bill in the parliament (DPR). The ministry of information and technology became the initiator in the proposing of the bill. This was encouraged because there were many cases related to personal data leakage. However, since 2016, in order to prevent the leakage of personal data, the Ministry of Information and Technology has made regulation on Personal Data Protection No. 20 of 2016.[7]

Nevertheless, the protection of privacy and personal data in Indonesia in specific legal instruments does not yet exist and is still sectorial, so that it is not enough to encourage digital economic development in Indonesia.[8] The urgency to respond to the issues addressed to the privacy and data protection in enactment of developing technology, also caused by the existence of Sectorial law, which does not cover the issues.

---

[3]Charlotte Trueman. (2018). How *is AI Benefiting Industries throughout Southeast Asia?*. available from https://www.cio.com/article/3311756/how-is-artificial-intelligence-benefiting-industries-throughout-southeast-asia.html. [Accessed April 5, 2019].

[4]MIT Technology Review. (2016). *Asia's AI Agenda: How Asia is speeding up Global Artificial Intelligence Adoption*. available from: https://s3.amazonaws.com/mittrasia/AsiaAI.pdf. [Accessed April 5, 2019].

[5]See Hunton Andrews Kurth. (2018). *Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice*. available from: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf. [Accessed April 5, 2019].

[6] Samuel D. Warren & Louis D. Brandeis. (1890). *The Right to Privacy*. 193 Harvard Law Review. Vol. 4, No. 5.

[7]Iwan Krisnadi. *Kajian Regulasi Perlindungan Data Pribadi di Indonesia*, available at: https://www.academia.edu/37095923/KAJIAN_REGULASI_PERLINDUNGAN_DATA_PRIBADI_DI_INDONESIA. [Accessed on April 10, 2019].

[8]Sinta & Gerry. (2018). *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia*. 90 VeJ. Vol.4. No.1.

Data protection in each nation is contrastingly directed, besides some worldwide instrument go to manage security and individual data protection, which may contain a few standards in security and protection of the data in which may impact the enactment of law in every country. This paper means to talk about the earnestness of the foundation of Personal Data Protection Law in Indonesia as the references of all need to the data protection, besides the authors utilized the lesson learning to some Asian Countries, for example, China, South Korea, and Singapore. [9]

2. Discussion and Analysis

2.1. The Important of Enactment Data Protection Regulation in Indonesia

Based on the survey result from Association of Indonesian Internet Service (APJII) in November 2016 132.7 million people of Indonesia has been connected to the internet from a total population of Indonesia approximately 256.2 million people, which is around 25,3% compared to the total population of Indonesia.[10] Internet is a new innovation that supports the development of a country in some aspect, like economic, education, industrial, etc. because of the internet development, almost all Indonesian people are using the internet for their daily life, nowadays the internet grows very fast, and almost all aspect on public services or public facilities are using the internet, such as banking, online shop, credit card and social media, etc. People are most often using their personal data and input their personal data in internet for using the facilities of AI. The development of Industrial Revolution 4.0 makes people easier to get their service from AI and the personal data as the key to use the AI properly. So the protection for personal data is needed to protect the privacy of internet users. Not only in Indonesia but also data protection is necessary for all the user around the world.

There are 110 countries in the world that already have a Personal Data Protection Act, but Indonesia is not one of them. Considering the penetration of technology in Indonesia is quite massive. Based on the data found in 2017, there were 143, 26 million internet users in Indonesia, around 54.68% compared to the total population of Indonesia, which is bigger than the data found in 2016.[11] So based on that data, we can say that the regulation is needed to protect the personal data of the internet user. In Indonesia the regulations regarding the protection of personal data are not "non-existent", but the regulations on the protection of personal data are contained in about 30 sectorial laws, such as in the Health Law, Population Administration Law, Electronic Transaction Information Law, and Public Information Disclosure Law, etc.[12]

Nowadays, the importance of enactment of Personal Data Protection Regulation in Indonesia is really needed because for some reasons. Firstly, there are

[9] The reason why the authors choose those countries as the comparative study because they successfully implemented the data protection law. Moreover, these countries have succeeded in providing convenience to the protection of their citizens' data through a single regulation.

[10] Hardianto Canggih dkk. (2018). *Urgency Legal Aspects Of Growth Information technology In Indonesia.* available from: https://osf.io/h6vp8. [Accessed April 14, 2019].

[11] Iwan Krisnadi. *Kajian Regulasi Perlindungan Data Pribadi di Indonesia*, available from: https://www.academia.edu/37095923/KAJIAN_REGULASI_PERLINDUNGAN_DATA_PRIBADI_DI_INDONESIA. [Accessed April 10, 2019].

[12] Rofiq Hidayat. (2018). *Yuk Simak Perlindungan Data Pribadi Ynag Ttersebar di Beberapa Undang-Undang,2018.* Available from: https://www.hukumonline.com/berita/baca/lt5aa2522899af7/yuk-simak--perlindungan-data-pribadi-yang-tersebar-di-beberapa-uu/. [Accessed April 10, 2019].

many cases of misuse of personal data on internet users, such as the use of social media, internet banking, public services, etc. As the example of misuse of personal data is about data abuse cases on 87 million Facebook users which is around 1 million users are from Indonesia.

Another example is at the beginning of 2016 of leakage of GO-JEK (bicycle used for public transport via online application) customer data cases. This data leak is mounting because many parties can steal the personal data of GO-JEK users and riders. Based on the opinions of technology observers as well as ICT Watch Executive Director, Donny Budi Utoyo, data leaks in the GO-JEK application are already serious and cannot be tolerated anymore. Because not only the user's personal data is leaked, but also the behavior of users can also be accessed, so it will be easier for parties with malicious intent to abuse them for crime. In GO-JEK application, the user must input their personal data, such as name, address, and telephone number, as well as user activities such as travel history while using the application. Not only GO-JEK, but also online shop customer, bank customer also has cases on stilling of data protection to criminal intentions.[13]

While the misuse of personal data is usually for criminal purposes, fraud, or just political purposes, it is certainly very detrimental to the data owner (internet user), so this becomes a special concern for the government to immediately make regulations to protect personal data, so as to provide security for users and can provide penalties that provide a deterrent effect for those who intentionally misuse the data.

Secondly, the European Union enacted the General Data Protection Regulation (GDPR) on May 25, 2018. Which, this rule applies internationally to any company that targets the inhabitants of the European Continent. This rule also includes all forms of services, products, advertisements, etc. that use the language or currency of European Union member countries. If Indonesia does not release the Personal Data Protection Act, Indonesia cannot exchange data with the European Union. This is due to the need for regulations that are equivalent to the General Data Protection Regulation in Europe, if Indonesia does not have regulations on data protection, Indonesia must make a contract for the company (which wants to process the personal data of the EU community).

Thirdly, it is related to the government's target to become the largest digital economy player in Southeast Asia with a capitalization of US $ 130 billion in 2020.[14] The digital economy in Indonesia has been initiated since the development of digital technology, so the government looks at future business opportunities through digital economy, as countries that participate in free markets, of course, Indonesia expects to become a digital economy center, it can be like China that has been successfully running digital economy and possesses data protection to protect digital (internet) users.

Moreover, due to that reason, the Minister of Information and Technology established a Regulation No. 20 of 2016 concerning Protection of Personal Data set on November 7, 2016, promulgated and effective from December 1, 2016. In this regulation, it is explained that personal data is stored and maintained by the truth, and protected by

[13] Reska K. Nistanto. (2016). *Kebocoran Go-Jek Memuncak, Rute Sehari-hari Pengguna Bisa Dilacak*, Available from: https://tekno.kompas.com/read/2016/01/20/16031307/Kebocoran.GoJek.Memuncak.Rute.Seharihari.Pengguna.Bisa.Dilacak. [Accessed April 10, 2019].

[14] Desy Setyowati. (2018). *Empat Urgensi UU Perlindungan Data Pribadi di Indonesia*. available from: https://katadata.co.id/berita/2018/04/10/4-urgensi-uu-perlindungan-data-pribadi-di-indonesia. [Accessed April 14, 2019].

confidentiality. [15] The existence of a Ministerial Regulation No. 20 of 2016 on the Protection of Personal Data only covers administrative sanctions, not including criminal sanctions for perpetrators of theft and misuse of data. Because this regulation is not enough, Indonesia needs a regulation on the law on the Protection of Personal Data. In making the law on the protection of personal data it is expected that it will cover principles, mechanisms and sanctions, can also adopt some rules in the GDPR (General Data Protection Regulation) such as data owner's agreement, accountability, the appointment of personal data management data, right to delete and access personal data. Thus it is expected to protect various parties in the misuse or theft of personal data and provide penalties for the perpetrators of these crimes.

While in making the law on the protection of personal data, of course, Indonesia can learn from several countries that already have regulations on data protection, while some countries that the authors will discuss are China, South Korea, and Singapore. The three countries have succeeded in having regulations on data protection and implies it, so that Indonesia can refer to the three countries.

2.2. Learning Lesson of Data Protection Law with Some Country

Turning to the international arena, it is worth noting the increasing focus on data protection issues in Asia and South America. Data protection legislation was recently signed in the Philippines. Taiwan has amended its data protection law, and Hong Kong is considering amendments to its law. On the opposite side of the globe, Uruguay's data protection law has been deemed adequate by the European Commission, and the Cayman Island is receiving public comments on draft data protection legislation. The European style framework is certainly influential in this international debate, but tempered by local cultural norms that may reflect a differing approach to privacy, though many similarity on the issue of data protection.[16]

Globally, South East Asia is one of the fastest-growing regions for digital innovation, spurred by better internet connectivity and smartphone adoption. Singapore has a Smart Nation vision; Malaysia, the world's first Digital Free Trade Zone; while Thailand has outlined a 'Thailand 4.0' vision that sees all sectors of the economy becoming digital. By 2025, digital commerce in the top 6 countries in ASEAN is expected to reach US$90 billion, up from US$5 billion in 2015. As cross-border data transactions grow, cyber security and data protection laws are also converging to reflect the demands of the emerging digital economy.

However, this is set to change as data protection rules become formalized. Europe's GDPR (General Data Protection Regulation) implementation in May 2018, for example, has developed a precedent that is likely to motivate Asia-Pacific governments to further tighten the screws on privacy protection by, for instance, setting punitive financial penalties when companies mishandle customer data, demanding stricter internal risk management controls, and establishing laws that codify compulsory requirements for data breach notification.[17]

[15] Yovita. (2016). *Indonesia Sudah Memiliki Aturan Soal Perlindungan Data Pribadi.* available from: https://kominfo.go.id/content/detail/8621/indonesia-sudah-miliki-aturan-soal-perlindungan-data-pribadi/0/sorotan_media. [Accessed April 8, 2019].

[16] Hunton & Williams. (2012). Privacy And data Protection. 128 West Law, P. & D.P. 2. 4.

[17] Alvin R. *preparedness and Compliance will be Key to Winning Customer Trust.* available from: https://www.fortinet.com/blog/industry-trends/the-data-protection-landscape-in-apac-.html. [Accessed April 8, 2019].

China, Singapore, South Korea, Japan, Australia, Malaysia, and the Philippines have recently updated their data protection compliance rules or will soon be introducing new privacy and cyber security laws. With the data protection compliance burden growing in the Asia-Pacific region, it's likely that the efforts to achieving compliance, and the risks associated with the failure to comply, will increase dramatically.

For many businesses, customer confidence is already being influenced by their perceived risk of conducting transactions online or whether their data is at risk of being compromised or stolen. Meeting or exceeding regulatory requirements will go a long way towards assuaging those concerns. New data compliance rules also offer an opportunity to re-evaluate their processes and improve data management and customer loyalty. Rather than seeing these new regulations as challenges or barriers, it is better to view them as an opportunity to achieve competitive differentiation, as well as a way to drive greater customer confidence and trust in their brands.[18]

Because of some realities above, the authors are interested to discuss what kind of lesson that we can learn from some countries like China, Singapore, and South Korea that have recently done updating their data protection compliance rules, to encourage Indonesia to immediately have a regulation regarding the personal data protection.

2.2.1. China Data Protection Law

In recent years, China's leadership has been increasingly thinking about how to ensure their competitive edge in the AI industry. The acceleration of China's policy efforts to advance AI development began in 2014, when President Xi Jinping called for innovation and breakthroughs in science and technology, including AI, at the opening ceremony of the 17th Congress of the Chinese Academy of Sciences.[19]

Following 2014, a series of national economic initiatives, including the 13th Five Year Plan (March 2015), Made in China 2025 (May 2016), Robotics Industry Development Plan (April 2016), and Three-year Guidance for Internet PLUS Artificial Intelligence Plan (May 2016), all provided guidelines to boost AI R&D. On October 18 2017 China is placing huge bets on big data, and a range of policies that related to the government vision. Chinese President Xi Jinping promoted the integration of the internet, big data, and AI with the real-world economy in his 19th Party Congress report.[20]

The swift development of China's economic power has accelerated its reputation as a new great power. With strong developments in technology corresponding to its rising economic status, China has been aware of the potential risks in the digital space as well as the utilization of it by other countries. China as a new center of the economic in the world is trying to develop its privacy and data protection. Both the domestic social-economic development and international trade and economic exchange will eventually push China to observe international standards of privacy and personal data protection.

Currently, China's privacy and personal data protection shows a mixed picture. On the one hand, it reflects the

[18]Alvin R. *preparedness and Compliance will be Key to Winning Customer Trust.* available from: https://www.fortinet.com/blog/industry-trends/the-data-protection-landscape-in-apac-.html. [Accessed April 8, 2019].

[19] Weining Hu. (2017). *How China Becoming a World Leader in Artificial Intelligence*. available from: https://www.china-briefing.com/news/china-world-leader-artificial-intelligence/. [Accessed April 13, 2019].

[20] Lotus Ruan. *(2018). Big data in China and the battle for privacy*. https://www.aspi.org.au/report/big-data-china-and-battle-privacy.com. [Accessed April 23, 2019].

economic demand in an increasingly globalized marketplace; on the other, it shows the people's increasing privacy awareness. [21] Unfortunately, although the Chinese Constitution acknowledges the privacy of communications[22] China does not address the protection of privacy or personal data generally.

The Chinese Constitution provides that no organization or individual may, on any ground, infringe on citizens' freedom of privacy of correspondence, with the exception that public security or prosecutorial organs are permitted to censor correspondence in accordance with the procedures prescribed by law for the purpose of safeguarding State security or investigating crimes.[23] The General Principles of the Civil Law mention the legal basis for civil rights protection but do not stipulate privacy as an independent right. In addition to the general laws, a few specific laws, to a certain extent, address the issue of privacy protection.

China has dedicated itself to collecting information on its citizens, but the country is now emerging as a surprise leader in Asia on data privacy rules. [24] China has introduced some of the most comprehensive data protection regulations. After its third deliberation, the Chinese government passed the new PRC Cyber security Law (hereinafter the "CSL") on 7th November 2016 and was enacted in June 2017. This act placing the onus on companies that conduct business in China, The new law, which comes into force on 1st June 2017, has significant implications for the data privacy and cyber security practices of both Chinese companies and international organizations doing business in China. —regardless of whether they have a physical presence in the country—to review their data protection policies and ensure compliance. In addition, from 2014 to September 2017, a total of 1,529 criminal cases of infringement of personal information were heard in courts across the country.[25]

Over the next few months, China will also be introducing e-commerce legislation to cover areas such as data anonymisation, big data, overseas data transfers, and information security. Companies that fail to comply with the law will face severe financial penalties, possibly including the loss of their rights to conduct business.[26]

Furthermore, the government make regulation on CSL is to covers relevant legislations and competent authorities, definitions, territorial scope, individual right, key principles, registrations formalities and prior approval, appointment of a data protection officer and appointment of processors that conduct in 36 jurisdictions. CSL is set out data protection requirement for network operators. Besides, CSL there are the other general legislations on data protection. There are civil and criminal legislations that have an impact on data protection. In general rule of civil law became effective on 1 October 2017, in which article 111 provides that natural persons' personal data is protected by law. Illegally collecting, using, processing or transferring the personal data of others is not allowed.

---

[21] Hong Xue. (2010). Privacy and Personal Data Protection in China: An Update for the year-end 2009. Institute for the Internet Policy & Law. Beijing Normal University. PR China. Elsevier Ltd.

[22] Invasions of residence privacy and communication privacy are crimes under the 1997 Chinese Criminal Law. See Article 245–246.

[23] See Article 40 of the Chinese Constitution (1982)

[24] Louise Lucas. (2018). *China Emerges as Asia's Surprise Leader on Data Protection*. available from: https://www.google.com/amp/s/amp.ft.com/content/e07849b6-59b3-11e8-b8b2-d6ceb45fa9d0. [Accessed April 13, 2019].

[25](2018) The Monetary Authority of Singapore's 2018 special report on the digital economy, published in the Straits Times.

[26]Lotus Ruan. *Big Data China and Battle Privacy*. available from: https://www.aspi.org.au/report/big-data-china-and-battle-privacy.com . [Accessed April 11, 2019].

The criminal law also regulated on personal data and privacy, in which article 253-(1) the offense of infringing citizens' personal information, article 286-(1) the offense of refusing to fulfill information network security responsibilities, article 177-(1) the offense of stealing, purchasing or illegally disclosing other people credit card information. Regarding the interpretation of some issues the application of law to criminal cases of infringement of citizen's personal information handled by the Supreme Court and the Supreme people's Procurator ate issued in 2017 provides further explanations regarding the offenses relating to infringing personal data and privacy. Article law of the tort liability law sets the right to privacy as one of the civil rights of citizens, along with the right to life, right to health, etc. [27]

Based on chapter V article 51 on CSL described that The State will establish a cyber-security monitoring, early warning, and information communication system. The State cyber security and informatization departments shall do overall coordination of relevant departments to strengthen collection, analysis, and reporting efforts for cyber security information, and follow regulations for the unified release of cyber security monitoring and early warning information.

On chapter VI of CSL also regulated on the legal responsibilities that mention "Where network operators do not perform cyber security protection duties provided for in Articles 21 and 25 of this Law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to harm to cyber security or other such consequences will be punished with a fined (administrative punishment)".

In addition, besides having the regulation, it is necessary to strengthen the publicity and education of the concept of privacy data protection, because the public must have knowledge of data privacy protection. There are two ways to promote this concept: the first way is through public service ads or lectures. This way will be efficient to educate the public on privacy data protection. The second way is through school education, the student also needs to educate on privacy data protection, because the young generation is much more using the internet (network). At last, privacy protection skills training should be promoted, and privacy protection and technology innovation should be supported. Through the national science and technology plan or industrial development fund, it is available to support enterprises or research institutions to innovate privacy protection technology in Indonesia. [28]

From the explanation above, Indonesia can take several important points regarding the contents of CSL and create a special institution that oversees the protection of personal data.

2.2.2. South Korea

South Korea has some of the world's strictest privacy laws. According to the International Association of Privacy Professionals, South Korea's data privacy law has evolved rapidly in particular during the past several years, despite short history of relevant legislation and enforcement. South Korea's data privacy law has exceedingly stringent consent requirements. In addition to consent, there are many other statutory provisions with onerous requirements, arguably making the overall data privacy law

[27] Susan Ning & Han Wu. *China: Data Protection 2018*. available from: https://iclg.com/practice-areas/data-protection-laws-and-regulations/china. [Accessed April 23, 2019].

[28] Hui Zao & Haoxin Dong. (2017). *Research on Personal Privacy Protection of China in the Era of Big Dat.* vol.5. 139-145 p6 scientific research publishing. online journal available from: https://file.scirp.org/pdf/JSS_2017061914491600.pdf. [Accessed April 23, 2019].

regime in South Korea one of the strictest in the world.[29]

In March 2011, the South Korean government adopted its own general Personal Information Protection Act (Here called PIPA).[30] Similarly, the law prescribes the fundamental data protection principles for the protection of personal data and applies to all individuals and organizations that process personal data.

It is of interest to note that the Korean legislation contains some innovations, including the requirement for "privacy impact assessment" in the case of "probable" and "highly probably" violations by the public and private sectors respectively, a process for the notification of leaked information and data breaches and the establishment of a Personal Information Dispute Mediation Committee to deal with disputes over personal information.

With the enactment of the PIPA in 2011, the Public Agency Data Protection Act was repealed since the PIPA would serve as a general data privacy statute for both the public and private sectors. However, the IC Network Act was not repealed after the PIPA was enacted, and now generally regulates data privacy issues related to Internet activities.

Moreover, as the main privacy Law in South Korea PIPA has a Similarity to the structure of the GDPR. PIPA gives South Koreans controls over how its personal information is collected and used. Personal information is defined as anything that identifies an individual or can easily be combined with other information to do so.[31] The PIPA is a comprehensive and omnibus data privacy statute. In terms of its basic structure, it first defines Personal Information and requires prior notice and consent from data subjects before such Personal Information can be collected and processed.[32]

Overall, the PIPA contains many features that arguably reflect the general trend that is emblematic of modern data privacy statutes. The PIPA, in particular, explicitly incorporates the eight major principles stipulated in the OECD's privacy guidelines, which laid a foundation for modern data privacy regulations[33] That is, Article 3 of the PIPA lists basic principles of data privacy that were derived from the OECD guidelines, with some modifications. In terms of its general statutory structure, and given that the PIPA is an omnibus data privacy statute, it shows many similarities to the EU's Data Protection Directive or the General Data Protection Regulation.[34]

The data privacy regulator's role under the PIPA is different from what is expected from a Data Protection Agency ("DPA") under the EU approach. Within the EU, a DPA in each member country generally assumes various specific roles related to data

[29] Haksoo ko, John Leitner, Eunsoo Kim, Jong gu jung. (2016). *Structure and Enforcement of Data Privacy Law in South Korea,* Brussels Privacy Hub, Brussel. Vol. 2, No. 7, p.1.

[30] Whon-il Park. (2013). *Data Privacy Protection, Bakerhostetler Data Privacy Law South Korea*. Available from: http://archive.edrm.net/resources/data-privacy-protection/bakerhostetler-data-privacy-laws/south-korea. [Accessed April 24, 2019].

[31] Paul Sutton. (2018). *Data protection in South Korea: why you need to pay attention*. Available from: https://www.radiusworldwide.com/blog/2018/8/data-protection-south-korea-why-you-need-pay-attention.com. [Accessed April 24, 2019]

[32] Personal Information Protection Act, Arts. 2 and 15(1)1.

[33] Organization for Economic Cooperation and Development (OECD), OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, OECD Doc. C(80)58/final (original version, 1980). In 2013, the OECD published a revised version of these original OECD guidelines which adopted the same eight privacy principles. [cite 2013 document]

[34] Principles set forth in Article 3 of the PIPA are generally analogous to the principles that are found in Article 5 of EU's GDPR

privacy, including in particular as a regulatory enforcer of data privacy law.

From the explanation above, Indonesia can take several important points regarding the contents of PIPA and adopt some good value from Korean legal act to protect Indonesians personal data.

2.2.3. Singapore

The digital era poses increasingly greater challenges to the integrity of personal informational privacy for many reasons. This is especially so in relation to private sector developments.[35] In Singapore, changes to the Personal Data Protection Act already include facets similar to Europe's GDPR, particularly in terms of mandatory breach notification and the appointment of a data protection officer. In the first five months of 2018, a number of financial and insurance organizations were fined for failing to provide adequate security arrangements to protect personal data or for breaching rules on the use of personal data. Singapore is also widely expected to pass a cyber-security bill later this year. However, Singapore's Personal Data Protection Act 2012 (PDPA 2012) has been in force since 2014 and is being implemented by the Personal Data Protection Commission. As in the case of the Philippines, the PDPA includes in its scope of personal data being processed or controlled by both private and public entities.

The objective of the PDPA is to put in place baseline standards to "curb excessive and unnecessary collection of an individual's personal data by businesses, and would include requirements such as obtaining the consent of individuals to disclose their personal information".[36]

It is also important to note that most of these countries have privacy as a constitutional right—usually a legal basis for enacting a data protection statute. Finally, as a collective, the ASEAN adopted its first regional declaration on privacy via its 2012 Human Rights Declaration. Article 21 of the instrument provides that:

> *"Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honor and reputation. Every person has the right to the protection of the law against such interference or attacks."*

This commitment led to the establishment of the ASEAN Framework on Personal Data Protection in 2016. The Framework sets out principles on data protection meant to guide member states in their respective implementation of related domestic laws and regulations.

The Framework's provision on implementation allows member states to embark on joint activities that could strengthen cooperation and collaboration in the area personal data protection. This may include information sharing and exchange, seminar or other capacity-building activity, and joint research in areas of mutual interest. Notably, the Framework gives due consideration to nations who may encounter delays in their application of the instrument's provisions, given their varying levels of development.[37]

Seen from the definition of Personal data may refer to data, whether true or not, about an individual who can be identified

---

[35] Warren B. CHIK. *The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy*. Computer Law and Security Review. 29, (5), 556 (2013).

[36] See Inside Privacy. (2013). *Singapore to Introduce Data Protection Law.* available from: https://www.insideprivacy.com/international/singapore-to-introduce-data-protection-law/. [Accessed April 15, 2019].

[37] Gie Dela. *Privacy and Data Protection Laws Southeast Asia*. Available from: http://ateneo.edu/udpo/article/Privacy-and-data-protection-laws-southeast-asia. [Accessed April 8, 2019].

from that data; or from that data and other information to which the organization has or is likely to have access. Basically, the PDPA is established as a data protection law that comprises various rules governing the collection, use, disclosure, and care of personal data. It recognizes both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organizations to collect, use or disclose personal data for legitimate and reasonable purposes.[38]

Furthermore, other general legislations that affect data protection in Singapore are:[39] First, Computer Misuse Act (CMA) prohibits unauthorized access to any program or data held in any and unauthorized modification of content of any computer. Secondly, The Spam Control Act (SCA) regulates the bulk sending of unsolicited commercial electronic messages to an email address or mobile telephone number.

Today, vast numbers of personal data are collected, used and even also transferred to third party organizations for several of reasons. While PDPA purposed for some following reasons:[40]

1. Consent: Organizations may collect, use or disclose personal data only with the individual's knowledge and consent (with some exceptions);
2. Purpose: Organizations may collect, use or disclose personal data in an appropriate manner for the circumstances, and only if they have informed the individual of purposes for the collection, use or disclosure; and
3. Reasonableness: Organizations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.

Through the establishment of PDPA, Singapore's experience is of interest for at least three reasons.[41] First, Singapore has a good position for e-commerce and yet the absence of data protection law until 2012. The PDPA was drafted for a highly connected population, drawing upon the experience of many other countries and extensive consultation with users and industry. The PDPA should be model legislation that is effective today, but also adaptable to changes in technology and user behavior.

The second reason to examine Singapore's experience is that the goals of legislation were quite different from other jurisdictions. Whereas the European Union ("EU") long approached data protection through the lens of human rights in general and the right to privacy in particular, Singapore's legislation explicitly sought to balance the legitimate needs of business and the rights of individuals.

The third of interesting point is Singapore's unique political environment and the nature of the relationship between the Government and the governed. While Public agencies are exclude to the PDPA's coverage, when the PDPA was enacted, the Minister stressed that the public sector has its own

[38] Personal Data Protection Commission Singapore. (2018). *Legislation and Guidelines*. available from: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview. [Accessed April 15, 2019].

[39] See. Winnie Chang. (2018). *Singapore: Data Protection 2018*. available from: https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore. [Accessed April 15, 2018].

[40] Legislation and Guidelines. (2018). *Overview How Does the Personal Data Protection Act Work?*. available from: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview. [Accessed May 7 2018].

[41] See Simon Chesterman. (2018). Data Protection Law in Singapore, Privacy and Sovereignty in an Interconnected World, Second Edition, Academy Publishing.

data protection rules, which he said are "guided broadly by the same principles"[42] From the explanation above Indonesia may consider to the several important points regarding the contents of PDPA.

3. Conclusion

The main point concluded from the brief discussion above are, the Important of enactment Personal Data Protection Regulation in Indonesia is really needed because of some reasons. Firstly many cases of misuse of personal data on internet users, such as the use of social media, internet banking, public services which is very detrimental to the owner of personal data. Secondly, the European Union enacted the General Data Protection Regulation (GDPR) on May 25, 2018. Which this rule applies internationally to any company that targets the inhabitants of the European Continent. If Indonesia wants to participate in international trading, Indonesia must have their own personal data protection regulation. Thirdly, is related to the government's target to become the largest digital economy player in Southeast Asia with a capitalization of US $ 130 billion in 2020, if the government looks at future business opportunity, data protection will be the concern to protect the digital user and create public trust.

Meanwhile, in making the law on the protection of personal data, of course, Indonesia can learn from China, South Korea, and Singapore that already have regulations on data protection, and those three countries have succeeded in having regulations on data protection and implies it. Based on the discussion above, Indonesia is a newly recognized developed country in Asia that often uses digital transaction in many areas which require the use and input over their personal data strictly needs to enact the personal data protection law.

And the author propose a suggestion for Indonesian lawmakers to consider some of the thing; First, Data protection laws should provide clear and meaningful guidance for determining what notice-and-consent procedures and practices can fulfill legal requirements. Legislation and regulations could provide the most clearest and standardized guidance. More immediately, courts have the opportunity to apply constitutional requirements and existing statutory language to focus on practical rules for obtaining individual consent.

Second, Indonesian government authorities should seek greater collaboration in the enforcement of data privacy laws. The threat of group litigation, substantial administrative fines, and criminal prosecution may already be constricting commercial activities.

Furthermore, the existence of the Data Protection Law is to strike a balance between the rights of individuals to privacy and the ability of organizations to use data for the purposes of their business. In fact by enacting the law will also support in promoting AI in Indonesia. On the other hand, from all of the countries that have mentioned above (China, South Korea, and Singapore) shows that by enacting the personal data protection law will efficiently protect all the AI process of Controlling, Processing and Transferring the data among businesses.

[42] Singapore Parliament Reports (Hansard) (2012). "Personal Data Protection Bill" vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts) (closing speech after the second reading of the Personal Data Protection Bill 2012, included as Appendix C in this book).

References

Books

Haksoo ko, John Leitner, Eunsoo Kim, Jong gu jung. (2016). *Structure and*

Enforcement of Data Privacy Law in South Korea, Brussels Privacy Hub, Brussel. Vol. 2, No. 7, p.1.

Hong Xue. (2010). Privacy and Personal Data Protection in China: An Update for the year-end 2009. Institute for the Internet Policy & Law, Beijing Normal University, PR China, Elsevier Ltd.

Hunton & Williams. (2012). Privacy And data Protection, West Law, P. & D.P. 12(8), 2, 4.

Invasions of residence privacy and communication privacy are crimes under the 1997 Chinese Criminal Law. See Article 245–246.

Samuel D. Warren and Louis D. Brandeis. (1890). *The Right to Privacy*. Harvard Law Review, Vol. 4, No. 5, p. 193.

See. Simon Chesterman. (2018). Data Protection Law in Singapore, Privacy and Sovereignty in an Interconnected World, Second Edition, Academy Publishing.

Sinta and Gerry. (2018). *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia*, VeJ Vol. 4, Number 1, p. 90.

The Monetary Authority of Singapore's 2018 special report on the digital economy. (2018). published in the Straits Times.

Warren B. CHIK. (2013). *The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy*. Computer Law and Security Review. 29, (5), 556.

Regulation

China's Cyber security Law (CSL 2017)

Chinese Constitution (1982)

EU General Data Protection Regulation (GDPR)

Indonesian Constitutional Act 1945

Indonesian Government Regulation Number 82 of 2012 concerning the Implementation of Systems and Electronic Transactions

Indonesian Minister of Information and Technology Regulation No. 20 of 2016 concerning of Personal Data Protection

Indonesian Minister of Communication and Information Regulation Number 11 of 2016 concerning Classification of Interactive Electronic Games

Singapore's Personal Data Protection Act 2012 (PDPA 2012)

South Korean general Personal Information Protection Act (PIPA 2011)

Internet

Alvin R. P*reparedness and Compliance will be Key to Winning Customer Trust.* available from*:* https://www.fortinet.com/blog/industry-trends/the-data-protection-landscape-in-apac-.html. [Accessed April 8, 2019].

Charlotte Trueman. (2018). *How is AI Benefiting Industries throughout Southeast Asia?*. available from: https://www.cio.com/article/3311756/how-is-artificial-intelligence-benefiting-industries-throughout-southeast-asia.html. [Accessed April 5, 2019].

Corinium. (2018). Big Opportunities for Big Data in the Asia Pacific. available from: https://www.coriniumintelligence.com/insights/big-opportunities-for-big-data-in-the-asia-pacific/. [Accessed April 5, 2019].

Desy Setyowati. (2018). *Empat Urgensi UU Perlindungan Data Pribadi di Indonesia*. available from: https://katadata.co.id/berita/2018/04/10/4-urgensi-uu-perlindungan-data-

pribadi-di-indonesia. [Accessed April 14, 2019].

Gie Dela. *Privacy and Data Protection Laws Southeast Asia*. Available from: http://ateneo.edu/udpo/article/Privacy-and-data-protection-laws-southeast-asia. [Accessed April 8, 2019].

Hardianto Canggih dkk. (2018). *Urgency Legal Aspects Of Growth Information technology In Indonesia.* available from: https://osf.io/h6vp8. [Accessed April 14, 2019].

Hui Zao & Haoxin Dong. (2017). *Research on Personal Privacy Protection of China in the Era of Big Data.* vol.5. scientific research publishing, 139-145, p.6 (2017). online journal available from: https://file.scirp.org/pdf/JSS_20170619144916 00.pdf. [Accessed April 23, 2019].

Iwan Krisnadi. *Kajian Regulasi Perlindungan Data Pribadi di Indonesia*, available from: https://www.academia.edu/37095923/KAJIAN_REGULASI_PERLINDUNGAN_DATA_PRIBADI_DI_INDONESIA. [Accessed April 10, 2019].

Legislation and Guidelines. (2018). *Overview How Does the Personal Data Protection Act Work?*. available from: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview. [Accessed April 10, 2019].

Louise Lucas. (2018). *China Emerges as Asia's Surprise Leader on Data Protection*. available from: https://www.google.com/amp/s/amp.ft.com/content/e07849b6-59b3-11e8-b8b2-d6ceb45fa9d0. [Accessed April 13, 2019].

Lotus Ruan. *Big Data China and Battle Privacy*. available from: https://www.aspi.org.au/report/big-data-china-and-battle-privacy.com. [Accessed April 11, 2019].

Mathias Avocats. (2017). *Artificial Intelligence and the GDPR: How do they interact?*. available from: https://www.avocats-mathias.com/technologies-avancees/artificial-intelligence-gdpr. [Accessed April 5, 2019].

MIT Technology Review. (2016). *Asia's AI Agenda: How Asia is speeding up Global Artificial Intelligence Adoption*. available from: https://s3.amazonaws.com/mittrasia/AsiaAI.pdf. [Accessed April 5, 2019].

Paul Sutton. (2018). *Data protection in South Korea: why you need to pay attention.* available from: https://www.radiusworldwide.com/blog/2018/8/data-protection-south-korea-why-you-need-pay-attention.com. [Accessed April 24, 2019}.

Personal Data Protection Commission Singapore. (2018). *Legislation and Guidelines*. available from: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview. [Accessed April 15, 2019].

Reska K. Nistanto. (2016). *Kebocoran Go-Jek Memuncak, Rute Sehari-hari Pengguna Bisa Dilacak*. available from: https://tekno.kompas.com/read/2016/01/20/16031307/Kebocoran.GoJek.Memuncak.Rute.Seharihari.Pengguna.Bisa.Dilacak. [Accessed April 10, 2019].

Rofiq Hidayat. (2018). *Yuk Simak Perlindungan Data Pribadi Ynag Ttersebar di Beberapa Undang-Undang*. available from: https://www.hukumonline.com/berita/baca/lt5aa2522899af7/yuk-simak--perlindungan-data-pribadi-yang-tersebar-di-beberapa-uu/. [Accessed April 10, 2019].

See Hunton Andrews Kurth. (2018). *Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice*, Centre for Information

Policy Leadership. available from: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf, [Accessed April 5, 2019].

See. Inside Privacy. (2011). *Singapore to Introduce Data Protection Law.* available from: https://www.insideprivacy.com/international/singapore-to-introduce-data-protection-law/. [Accessed April 15, 2019].

See. Winnie Chang. (2018). *Singapore: Data Protection 2018.* available from: https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore. [Accessed April 15, 2018].

Susan Ning & Han Wu. *China: Data Protection 2018*. available from: https://iclg.com/practice-areas/data-protection-laws-and-regulations/china. [Accessed April 23, 2019]

Weining Hu. (2017). *How China Becoming a World Leader in Artificial Intelligence*. available from: https://www.china-briefing.com/news/china-world-leader-artificial-intelligence/. [Accessed April 13, 2019].

Whon-il Park. (2013). Data Privacy Protection, Bakerhostetler Data Privacy Law South Korea. available from: http://archive.edrm.net/resources/data-privacy-protection/bakerhostetler-data-privacy-laws/south-korea. [Accessed April 24, 2019].

Yovita. (2016). *Indonesia Sudah Memiliki Aturan Soal Perlindungan Data Pribadi.* available from: https://kominfo.go.id/content/detail/8621/indonesia-sudah-miliki-aturan-soal-perlindungan-data-pribadi/0/sorotan_media. [Accessed April 8, 2019].