Proceeding 2nd International Conference on Law, Economy, Social and Sharia 2024 Vol. 2
https://icless.net/ ISSN: 2985-4679
Page: 395-408

Protection of Personal Data Confidentiality in the Era of Digital Economy: A Legal Framework in Indonesia

Imam Aji Ubaidah
Master Study of Law, Universitas Islam As-Syafi'iyah, Jakarta, Indonesia
iubaidah11@gmail.com

Abstract

Background: The development of the digital economy and several cases of personal data leaks that have occurred in the last five years have made Indonesians more aware of their personal data. Not once or twice, our personal information is gathered, disseminated, and distributed without our agreement, within the enterprises and the government. This article examines Indonesia's legislative framework for individual information privacy. Despite the existence of laws protecting the privacy of personal data, the legal framework is still evolving with a highly sectoral nature. This paper attempts to examine the national and international legal frameworks related to personal data protection. Purpose: The main aim of this research is to dissect various legal aspects in Indonesia that are relevant to the confidentiality of personal data, especially those involving people's personal data. By doing this, this research aims to contribute valuable insights to the ongoing discourse regarding the confidentiality of personal data in the digital era of the economy in Indonesia. Design/Methodology: The paper uses a normative juridical method, which examines the consistency between Indonesia's constitution and laws on personal data protection. Findings: The result is that Indonesia needs to immediately make a special law on the protection of personal data privacy to further strengthen Indonesia's position in the world electronic commerce. Research Limitation: The research is constrained by the availability and accessibility of legal data across different jurisdictions. Variability in legal systems and the scope of available case studies may limit the generalizability of the findings. Originality/Value: This research contributes to academic and practical understanding of the legal aspects in Indonesia regarding personal data confidentiality, offering a unique perspective that can inform policy development and legal reform to improve personal data confidentiality.

Keywords: *Protection, Personal Data, Digital Economy, Legal Framework*

I. INTRODUCTION

Indonesia has a huge and rapidly growing digital economy potential. The digital economy is expected to be worth about USD 100 billion to the country's GDP by 2025, and Indonesia will become one of the greatest digital economic powers with e-commerce transaction value reaching USD 130 million. This is possible due to the behavior of Indonesian people who are currently very dependent on the internet. APJII (Association of Indonesian Internet Service Providers) data states that there are more than 220 million internet users in Indonesia and on average they access the internet four hours per day. This large number of users must be balanced with the security of

personal data Privacy as a component in increasing trust and security in the digital economy ecosystem.

Security and trust are critical to the implementation of the digital economy. Therefore, it is important to encourage the development of a system that protects personal data nationally, among others in the form of a regulatory framework and corporate culture. Personal data protection in Indonesia is still a big question considering the number of complaints and reports filed by individuals and groups/organizations about violations of personal data privacy in the banking industry, especially credit cards, where credit card holders without the consumers' knowledge, private information is able to be distributed, accessed, exchanged among banks, and even traded. Not to mention the cases of leaked data that were hacked throughout 2022, including the case of leakage of PLN customer data, leakage of Tokopedia customer data, and leakage of Ministry of Social Affairs data where 102 million data containing photos of Identity Cards (KTP), Family Cards (KK) and BPJS (National Security Organizing Agency) cards were successfully hacked and widely spread.

In line with Sophos Report, Indonesia is now among the top ten spammers in the world, accounting for an estimated 10.6% of spam e-mails originating from Indonesia. APJII data also states that there are more than 3800 complaints related to spam e-mails without the e-mail account owner's permission. This shows that personal data violations are increasing. This happens because there is no regulation that specifically protects the confidentiality of personal data. Personal data regulations are not combined in a single statute, instead the government has established sectoral rules on personal data privacy with insufficient legal protection. In comparison with the remaining ASEAN countries, Indonesia lacks explicit laws on personal data privacy. As a result, the Indonesian government must addopt regulations governing the protection of personal data privacy and determine the most appropriate protection concept to defend the interests of Indonesia and foreign parties over personal data.

II. LITERATURE REVIEW

Alan Westin defines privacy as "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Cate, 2000). The definition put forward by Westin is referred to as information privacy because it involves personal information (Rosadi & Gumelar Pratama, 2018).

The concept of privacy as a human right to be protected is recognized in Article 12 of the General Declaration of Human Rights (1948), which states that: "No one shall be

subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attack. Everyone has the right to legal protection against such interference or violation)".

This provision is further affirmed in Article 17 of the International Covenant on Civil and Political Rights (1966), which states that: "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation; (2) Everyone has the right to protection of the law against such interference or attack (1) No one may arbitrarily or unlawfully interfere with his personal, family, home or correspondence matters, or unlawfully attack his honor and good name;(2) Everyone has the right to legal protection against such interference or attack as aforesaid)".

Although privacy is part of human rights, privacy has some exceptions or in other words, privacy is not absolute. Referring to the applicability of personal data protection guidelines issued by the OECD, exceptions to the application of personal data protection guidelines are possible for national sovereignty, national security, and public policy as long as they are carried out as little as possible and must be known to the public (OECD, 2013).

Privacy restrictions also provided by Warren and Brandeis reveal that privacy is not absolute, but there are limits, namely: (1) it does not rule out the possibility of publishing someone's personal information for the public interest; (2) no privacy protection if no harm is suffered; (3) there is no privacy if the person concerned has expressed consent that his personal information will be shared with the public; (4) Consent and privacy deserve legal protection because losses suffered are difficult to assess. Because it involves a person's mentality, the loss is felt far greater than the physical loss because it has interfered with personal life (Warren Samuel D, 1890). Furthermore, according to the General Assembly of the United Nations in The Right of Privacy in the Digital Age acknowledges that the development of communication technology allows people to be connected throughout the world, but on the other hand the development also increases the ability of governments, companies and individuals to conduct surveillance, eavesdropping and data collection that potentially threaten human rights. Therefore, privacy protection is needed for both online and offline activities (UN, 2016). Literally, data is the plural form of the word "datum" which in Latin means part of information. In the Knowledge Hierarchy compiled by Russell L. Ackoff (1919-2009), data is defined as symbols that are properties of observables, while information is defined as description.

The difference between the two is functional where information is inferred from data (Dammann, 2018). In the context of personal data protection, the terminology that is often used is "personal information" and "personal data". The United States uses the term personal identifiable information, while Europe uses the term personal data. In the current regulations in Indonesia, the terminology used is personal data. Personal data is defined as "any information relating to an identified or identifiable individual (data subject)" (OECD, 2013).

The General Data Protection Regulation (GDPR) defines the specific scope of personal data, including name, identity number, location data, online identifier, or one or more specific components related to the physical, physiological, genetic, mental, economic, cultural or social of a person. Furthermore, included in the scope of data that identifies oneself personally in the GDPR is data that is unknown (pseudonymization) but by using additional information, is able to identify a person (GDPR, 2016). The limitation of information included in personal information and not personal information (no-personal information) was developed by Jerry Kang.

Classified as personal information is information that can identify a person through 3 (three) ways, namely can show (1) the relationship of ownership (authorship) with individuals; (2) describe the permanent characteristics of the individual; or (3) information that can be used as an instrument to describe a person (Kang, 2006). The meaning of non-personal information is if the information is not data related to individual privacy, namely information that is not about a person, information about a person but is anonymous so that it cannot refer to a particular individual, information refers directly to the group and does not directly refer to individuals who are part of the group (Kang, 2006).

In the discussion of personal data protection, it is also known as grouping based on data sensitivity or called sensitive data. The classification of sensitive data may vary by country. In particular, the GDPR provides special protection for certain types of personal data that are considered sensitive in the form of information related to ethnicity, political choice, religion or belief or membership in a trade organization, biometric data for the purpose of identifying an individual, data on health or sex life or sexual orientation. Such sensitive data is prohibited from processing unless it meets a series of requirements explicitly stated in the GDPR, including the written consent of the data owner and data collection limited to the purposes that have been definitively stated in the GDPR (GDPR, 2016).

Although personal data protection arrangements vary from country to country, they generally refer to similar data protection principles. In general, the data protection regime is inspired by the OECD in 1980 Guidelines Governing the Protection of

Privacy and Transborder Flows of Personal Data which applies the first principles of privacy recognized internationally (OECD, 2013). Here are the principles of personal data protection according to the OECD (OECD, 2013)

III. METHODOLOGY

In examining the legal framework for safeguarding personal information, this paper uses the normative juridical method, which examines the compatibility between the Indonesian constitution and laws on personal data protection.

The legal instruments reviewed include:

- Universal declaration of human rights
- Constitution of the Republic of Indonesia in 1945
- Law No. 36/1999 on Telecommunications
- Law No.39/1999 on Human Rights
- Law No. 29/2004 on the Practice of Medicine
- Law No. 17 of 2007 on National Development Planning Policy
- Law No. 11 Year 2008 on Electronic Information and Transactions.

IV. RESULT AND DISCUSSION

The Concept of Personal Data Privacy in the Indonesian Legal Framework.

Privacy of personal data has not been specifically regulated in the Indonesian legal system. The attempt to guarantee personal data privacy protection stems from the constitution's Human Rights (HAM) regulations. It is additionally influenced by the increasing awareness of Indonesians of the importance of personal data privacy, given that so many digital practices collect personal data in the absence of clear legislation. Another motivator is the growing international determination, owing to Indonesia's vital position in worldwide trade, notably internet commerce. The creation of laws that guarantee the confidentiality of personal data is taken from the following sources:

i. 1945 Constitution (UUD ’45)

   Private information security is seen as a component of human rights in Indonesia. The basic source of legislation in Indonesia, the UUD '45, does not clearly include the safeguarding of private information confidentially. However, the UUD '45 clearly mentions the Human Rights protection.

   The Preamble from the '45 Constitution also states Indonesia's national goals, aiming to defend the whole Indonesian people and all the bloodshed of Indonesia , improve the well-being of all people, educate the lives of the people, and to

contribute in the implementation of a global order built on independence, social justice, and lasting peace.

The concept of protecting the confidentiality of personal data can also be found in the Amendment to the Constitution '45 article 28F "*Everyone has the right to communicate and obtain information to develop their personal and social environment, and has the right to seek, obtain, own, store, process, and convey information by using all available channels*" and article 28G "(1) *Everyone has the right to protection of themselves, family, honor, dignity, and property under their control, and is entitled to a sense of security and protection from threats of fear to do or not do something that is a human rights*". These articles do not directly mention the confidentiality of personal data, but have the same essence so that they can be considered as a legal basis for making regulations related to the confidentiality of personal data.

ii. Law No.39 0f 1999 on Human Rights

Indonesia adopted the Universal Declaration of Human Rights (UDHR) through Law No.39/1999 on Human Rights (Law 39/1999). Articles in Law 39/1999 that emphasize that Indonesia honors human rights related to the confidentiality of personal data, include:

Article 12 of Law/1999:

"Everyone has the right to protection for his or her personal development, to obtain education, to educate himself or herself, and to improve his or her quality of life in order to become a human being of faith, devotion, responsibility, noble character, happiness, and prosperity in accordance with human rights."

Article 21 of Law 39/1999:

"Everyone has the right to personal integrity, both spiritual and physical, and therefore should not be subjected for research without his or her consent."

Article 29 of Law 39/1999:

" (1) Everyone has the right to the protection of his or her person, family, honor, dignity, and property; (2) Everyone is entitled to recognition before the law as a personal person wherever he or she is."

Article 32 of Law 39/1999:

"*Freedom and confidentiality in correspondence including communication through electronic facilities cannot be interfered with, except by order of a judge or other lawful authority in accordance with the provisions of laws and regulations."*

iii. Law No. 36 Year 1999 on Telecommunications

Proceeding 2nd International Conference on Law, Economy, Social and Sharia 2024 Vol. 2
https://icless.net/ ISSN: 2985-4679
Page: 395-408

Law No. 36 of 1999 on Telecommunications (Law 36/1999) describes the government's protection of citizens' rights related to telecommunications. The protection of personal data confidentiality can be seen in the following articles:

Article 40 of Law 36/1999:

"Every person is prohibited from intercepting information transmitted through telecommunications networks in any form."

Article 42 of Law 36/1999:

(1) Telecommunication service providers are are required to protect secret information supplied as well as obtained by telecommunication service clients via their telecommunication network and or telecommunication services organized by them.

(2) Telecommunications service providers are able to record data delivered and or obtained by telecommunications service providers for any reason of the procedure for criminal justice and might supply the information required about: a. written inquiry of the Attorney General and or the Chief of the Indonesian National Police for certain criminal offenses; b. ask for about detectives for certain criminal offenses in compliance with the applicable Laws.

(3) Government Regulation shall govern the processes for obtaining and supplying recorded information mentioned in paragraph (2).

Criminal provisions for violations of Article 42 have also been stipulated in Article 57 of Law 36/1999 which reads: *"Telecommunication service providers who violate the provisions as referenced to in Article 42 paragraph (1), should be penalized by imprisonment for a maximum of 2 (two) years and or a maximum penalty of Rp200,000,000.00 (two hundred million rupiah)."*

iv. Law No. 29 Year 2004 on Medical Practice

The protection of personal data privacy is also regulated in Law No. 36 of 2004 on Medical Practice (Law 36/2004), specifically in the following articles:

Article 47 of Law 36/2004:

(1) Medical record documents, as defined in Article 46, belong to doctors, dentists, or health care institutions, whereas medical record contents belong to the patient.

(2) Medical records, as defined in paragraph (1), shall be retained and kept secret by doctors or dentists, as well as the head of health care institutions.

(3) The provisions concerning medical records mentioned in paragraphs (1) and (2) are governed by Ministerial Regulation.

v. Law No. 36 Year 2009 on Healthcare

Law No. 36 of 2009 concerning Healthcare also regulates the confidentiality of personal data, as mentioned in article 57 as follows:

(1) Everyone has a claim to privacy regarding his or her personal health status that has been revealed to a health care professional.

(2) The provisions mentioned in paragraph (1) on the right to secrecy of personal health problems do not apply in the following circumstances:

a. order of law;

b. court order;

c. permission is concerned;

d.interests of society; or

e.the interests of the person.

vi. Law No. 11 Year 2008 on Electronic Information and Transactions

Because of the increasing expansion of the internet and technical breakthroughs, Law No. 11/2008 on Electronic Information and Transactions, generally known as the ITE Law, was enacted.

The ITE Law forbid the utilization of personal data obtained via digital media with no permission of the person concerned. ITE Law also regulates electronic confidentiality on personal information pertaining to an individual without the person's permission. ITE Law further prohibits anyone from intentionally and without rights to change, add, reduce, move, destroy, eliminate or hide information or electronic/digital documents owned by individuals or the public.

Concept of Personal Data Protection Regulation for Indonesia

Regulatory approach for ensuring the confidentiality of personal data, each country has its own concept. From a practical point of view, there are considerable differences in regulatory concepts related to personal data privacy between the European Union and the United States. Despite similarities in historical, political, economic and cultural perceptions, there are essential disparities regarding the role of government in information regulation. This is because they have different legal approaches.[1]

In the United States, the regulation of personal data privacy is still sectoral, meaning that the government only governs areas that are deemed vital for being safeguarded by law. Other territories are self-regulated.

The European Union (EU), on the opposite, governs personal data privacy more thoroughly under a single piece of law that includes all sectors, both private and public. The EU has clearly placed the confidentiality of private information secrecy as a basic right secured through human rights. Given that each EU member has its own laws and

[1] Paul M. Schwartz and Karl-Nikolaus Peifer, *'Transatlantic Data Privacy Law'*, (2017) 106 Georgetown Law Journal, .2.

sets various standards, this comprehensive approach is adopted to facilitate the seamless flow of information and trade between EU member states.

Currently, there are similarities in personal data privacy regulations at the multilateral, regional and national levels in certain countries. This shows:

1. There is a strong desire to standardize regulations on the confidentiality of personal data;
2. There is a common meaning of the terms used, such as: data, personal data confidentiality, sensitive personal data, personal data, data processing, etc;
3. There is general agreement on the principles in maintaining the confidentiality of personal data;
4. ersonal data privacy regulations are not only applied to the public sector, but also to the private sector through legislative, *self-regulatory* and *co-regulatory* approaches*;*
5. To facilitate international trade, the protection of the confidentiality of personal data, particularly in relation to the "trans-border flow of data", is a prerequisite that should be considered.

Each regulatory concept has advantages and disadvantages. The advantages of the concept of comprehensive regulation include the following:

1. Legal certainty, because the confidentiality of personal data is a basic or human rights right that should be protected by the state;
2. Strictly regulate the protection of personal data in the government, public and private sectors;
3. Suitable for countries that have a civil law system and make laws the main source of law;

To anticipate the consequences of the rapid changes/convergence of telecommunications and information technology, it is important for Indonesia to establish an effective and integrated information technology law framework in order to attain legal clarity and discipline. This legal certainty and order can be achieved by: (1) recognizing and balancing between private and public rights; (2) determining the limits of these rights; and (3) regulating these rights.[2]

This viewpoint is consistent with Lawrence M. Friedman's belief that while constructing a legal system, three aspects must be met: structure, substance, and legal culture [3]. Structure refers to the point that Indonesian judiciary can decide matters involving violations of personal data privacy. This is not an easy task as it involves the

[2] Roscoe Pond, My Philosophy of Law, (Julius Rosenthal Foundation Northwestern University, 1941), 249.
[3] Lawrence M. Friedman, American Law: An Introduction, (Norton, W. W. & Company, Inc, 1997), 19

resource capabilities of all parties concerned, including judges. Judges are expected to understand technological developments and be able to apply the law to these cases of compensation for breach of personal data privacy.[4]

The concept of regulation also requires standards of practice to guarantee that that gather and employ private information offer proper protection. Such standards of practice have the following principles:

a. The limiting principle in information collecting. Only for legal purposes may information be gathered, processed, and distributed, with the knowledge and agreement of the data/information owner.
b. Information quality principles. The personal data/information collected must be kept accurate, complete and up-to-date.
c. Purpose/objectivity principle. Personal data/information may be disclosed if it is in accordance with the purpose for which it was collected/used.
d. Retention principle. Information should not be kept for longer than is necessary for a given reason.
e. Principle of maximum security of personal information. Private data should be safeguarded by suitable security systems to prevent loss or illegal activities such as unauthorized access, deletion, use, alteration, or exposure of this kind of data by third parties.
f. The principle of transparency. The system should ensure that the owner of the information knows what personal data is held by the information manager.
g. Principle of individual participation. Information owners should have the rights to access and make corrections to personal information stored by data managers.
h. Accountability principle. Data managers are fully responsible for implementing the aforementioned principles.

The involvement of institutions, both public and private, in drafting regulations on the confidentiality of personal data is very important.

Public institutions have the following functions:

1) The court, a sort of adjudicative institution is empowered to resolve the claims of persons whose personal data privacy has been breached;
2) The information commission has the duty to:
    a. Dissemination of the legislation to the general public, especially the commercial/industrial sector, so that they understand and respect the rights and responsibilities related to the confidentiality of personal data;
    b. Provide advice to the Minister on issues concerning the law application;

[4] Philippe Nonet and Philip Selzenick, Law & Siciety in Transition, (Transaction Publishers , 2001), 97

c. Conducting study as well as tracking to identify adverse impacts on personal data confidentiality due to the development of information and technological advances;
d. Support institutions and groups to socialize the code of ethics governing private information confidentiality;
e. As a mediator to resolve disputes/violations of personal data confidentiality outside the trial.

Independent organizations are expected to participate in implementing on personal data privacy regulations/rules. Private institutions are expected to create rules of ethics to be applied within the scope of their business in compliance with the mandate of the law.

In terms of the process, there are two techniques that may be used to ensure that a law is implemented and followed by all parties:

1. *Top-down* approach; when a new regulation is established, the government, public sector, private sector, all must jointly socialize, disseminate about the regulation, create a code of conduct and set sanctions if the rule is violated. The industry/commerce sector also needs to ensure that the regulation is implemented down to the lowest level. Thus, the public knows and understands about the new regulation.
2. *Bottom-up* approach; i.e. via education and dissemination, encouraging the people to study and comprehend the law. Education to the public can be done through discussions, seminars, training, educational institutions. The publication can be done through academic community publications, print media, electronic, online and many other communication channels. Everything aims to increase public understanding of personal data privacy protection regulations[5].

Several nations that currently have regulations governing personal data confidentiality have established institutions in charge of overseeing the implementation and enforcement of the law. The establishment of this institution aims to ensure the effective implementation of the law.[6] Although established and funded by the government, the jurisdiction to review the law's execution, issue guidelines on the protection of personal data privacy that should be complied with by each sector, conduct investigations into complaints of violations of personal data privacy, oversee

[5] Warren B. Chik. 'The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on personal data on the Internet', (2005), 14 1, International Journal of Law and Information Technology, 22-23.
[6] Handbook on European Data Protection Law (Publications Office of the European Union, 2014), 114.

the implementation of the code of conduct implemented by the industry/commerce sector. It also serves as a mediator to resolve disputes outside of court, if the problem cannot be addressed through the institution's mechanisms, it can be brought before the court.

International and Regional Obligations

Indonesia has signed and ratified several international treaties such as conventions, *statutes*, *agreements*, and others. Therefore, Indonesia actually has the legal foundation to enact laws that apply at the national level. For example, as a member of APEC, Indonesia has ratified the 2004 APEC Personal Data Privacy Framework, which states unequivocally that "the prospective of e-commerce is difficult to realize without cooperation between governments and businesses, including the development and implementation of technologies and policies that address problems connected to the safety and cinfidentiality of individual information."[7]

The European Union is Indonesia's biggest non-oil and gas marketplace for export. The cooperation so far has proven that European investors are stable and reliable partners. Therefore, it is critical for Indonesia to fulfill EU business requirements, including standards for protecting the secrecy of personal information. The absence of clear legislation on this matter may become an obstacle and disrupt economic cooperation between Indonesia and other countries.

Many Asian countries, including Indonesia, are unfamiliar with the term "privacy.". Most Asians reside in community cultures that place little emphasis on personal data confidentiality. Personal data privacy as a human right is a concept that originated in the 'west' and as science and technology progressed, the protection of personal data privacy has become very important.

V. CONCLUSION

The best appropriate regulatory model for Indonesia is one that combines several approaches in regulating the confidentiality of personal data, so that personal data information can be easily processed, compiled, accessed, and transferred to others.

To strengthen Indonesia's position in global e-commerce, Indonesia needs to improve and take a proactive approach in protecting the confidentiality of personal data in accordance with international standards. Therefore, Indonesia needs to:

[7] Sinta Dewi, Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional, (Widya Padjadjaran, 2009), 70

1. Create a particular legislation for the protection of personal data confidentially. This is crucial for the national interest and to facilitate Indonesia's international interactions, particularly in facilitating transnational trade, industry and investment;
2. Establish a mechanism for resolving violations of personal data confidentiality, especially those related to commerce/industry/services;
3. The implementation of E-Government programs, particularly E-KTP, where the government collects people's personal data without adequate safeguards leading to high potential for breaches.
4. Promoting Good Governance and realizing clean government.

ACKNOWLEDGEMENT

Finally, I would like to thank everybody who was important to the successful realization of this paper. This paper is far from perfect, but it is expected that it will be useful not only for the researcher, but also for the readers. For this reason, constructive thoughtfull suggestion and critics are welcomed.

REFERENCE

Cate, F. H. (2000). Principles of Internet Privacy. Connecticut Law Review, 32(3), 877–896.

Dammann, O. (2018). Data, Information, Evidence, and Knowledge: A Proposal for Health Informatics and Data Science. Online Journal of Public Health Informatics, 10(3). https://doi.org/10.5210/ojphi.v10i3.9631

Djafar, W. (2017). Big data and large-scale data collection in Indonesia: An introduction to understanding the challenges actual protection of the right to privacy (Internet and Human Rights). Jakarta.

Djafar Wahyudi, Sumigar Bernhard Ruben Fritz, S. B. L. (2016). Protection of personal data in Indonesia. Jakarta. Retrieved from http://weekly.cnbnews.com/news/article.html?no=124000

Economist, T. (2017). The worlds most valuable resource is no longer oil but data. Retrieved from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Friedman, M, Lawrence, American Law: An Introduction, (Norton, W. W. & Company, Inc., New York, 1997).

GDPR. Directive 95/46/EC General Data Protection Regulation (2016).

Geistiar Yoga Pratama*, S. A. (2016). Legal Protection of Personal Data of Transportation Service Users Online from misuse of service providers based on Law Number 8 Year 1999 On Consumer Protection, 5(3), 1–19.

Holvast, J. (2008). History of Privacy *. In The Future of Identity in the information society (pp. 13–42)

Kang, J. (2006). Information Privacy in Cyberspace Transactions. Stanford Law Review, 50(4), 1193–1293. https://doi.org/10.2307/1229286

Nonet, Philippe and Selzenick, Philippe, Law & Siciety in Transition, (Transaction Publishers, 2001)

Pond, Roscoe, Jurispridence Vol IV, (West Publisihing, 1959).

Schwarts, M, Paul and Nikolaus, Karl, Peifer, 'Transatlantic Data Privacy Law', (2017) 106 Georgetown Law Journal

Sinta Dewi, Privacy Protection of Personal Information in E-Commerce According to International Law, (Widya Padjadjaran, 2009)

Solove, D. J. (2002). Conceptualizing Privacy. California Law Review, 90(4), 1087–1156. https://doi.org/10.15779/ Z382H8Q

Su, K., Li, J., & Fu, H. (2011). Smart city and the applications. 2011 International Conference on Electronics, Communications and Control, ICECC 2011 - Proceedings, 1028–1031. https://doi.org/10.1109/ ICECC.2011.6066743

Taylor-Sakyi, K. (2016). Big Data:Understanding big data. Research Gate, 1–9.

Waldo, James, Lin, S, Herbert, Millet, I, Lynette I. (ed) Engaging Privacy and Information Technology In A Digital Age, (The National Academy of Science Press, 2007)

Warren B. Chik, 'The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on personal data on the Internet" (2005) 14 1, International Journal of Law and Information Technology

Laws and Regulations

Constitution of the Republic of Indonesia Year 1945 and Amendments to Law '45

Law No. 36 of 1999 concerning Telecommunications

Law No.39 of 1999 concerning Human Rights

Law No. 29 of 2004 concerning Medical Practice

Law No. 17 of 2007 concerning National Development Planning Policy

Law No. 11 of 2008 concerning Electronic Information and Transactions