PERSPEKTIF
P-ISSN 1410-3648 E-ISSN 2406-7385
Kajian Masalah Hukum dan Pembangunan
Volume 25 Nomor 1 Tahun 2020 Edisi Januari
Sekretariat:
Fakultas Hukum Universitas Wijaya Kusuma Surabaya
Jl. Dukuh Kupang XXV No. 54 Surabaya
e-mail & Telp: perspektif_hukum@yahoo.com (08179392500)
Diterbitkan oleh:
Lembaga Penelitian dan Pengabdian Masyarakat (LPPM)
Universitas Wijaya Kusuma Surabaya

THE URGENCY OF ENACTING PERSONAL DATA PROTECTION LAW AS A PATRONAGE FROM THE DEVELOPMENT OF COMMUNICATION AND INFORMATION TECHNOLOGY IN INDONESIA

Ghansham Anand
Faculty of Law, Airlangga University
e-mail: ghansam@fh.unair.ac.id

Agus Yudha Hernoko
Faculty of Law, Airlangga University
e-mail: yudha_fhunair@yahoo.co.id

Antonius Gunawan Dharmadji
Faculty of Law, Airlangga University
e-mail: doni.advokat@gmail.com

ABSTRACT

The development of information technology might control the pattern of people's behavior in digital era. The presence of internet as the main platform for online activities, including electronic transactions, was now increasingly attracting the interest of Indonesian people although it was vulnerable to be hacked by irresponsible parties as a cyber-attack. One cyber-attack targets individual's personal data. This study, therefore, took some issues related to that matter. First, it discussed the regulation of personal data protection in Indonesia applied in recent days, and second, it proposed an appropriate law to regulate such issue in the future.This study was a normative research with statute and case approaches. The result showed that, first, the existing regulation for personal data protection was less effective as it was still scattered in some sectorial setting, and thus, the system of appropriate regulation under a comprehensive law was considerably important. Second, the disharmony of regulatory legislation in regulating people personal data protection needed to be solved through a specific regulation which particularly regulated on personal data protection.

Keywords: personal data protection; cyber crime; privacy

INTRODUCTION

In this recent modern era, Indonesia is striving to a the World Web of through which communication is transformed into mobile one, particularly through smartphones and tablets connected to internet, to connect to the real world in a network.

Information technology involves an effective and efficient data collection, storage system. In its development, technology and information has been influencing any aspects of life, from simple to complex matters. For instance, the presence of a new market has evoked the development of societal economic system from manufacture-based traditional economy into digital economy using information, intellectual creativity, and science as the basis, known as Creative Economy.[1]

It is undeniable that the development of information technology demonstrates the growth

[1] Edmond Makarim. (2010). *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Jakarta: Raja Grafindo Persada, h. 2.

of various technology-based activities, such as e-government, e-commerce, e-education, and so on which all of them are electronic-based.[2] The existence of such development makes a brand new world called cyberspace or a world through electronic media in computerized network for online communication.

An issue on the importance of personal data protection is increasingly loud along with the increasing number of cellphone and internet users. A number of cases have increased, especially those related to the leakage of individual's personal data and leading to criminal actions such as deception and pornography, reinforcing the importance of providing a regulation to protect people personal data.

The personal data is very vulnerable with the violation of privacy on personal rights, especially to personal data collected without having any permission from the owner of the data, and it may be transferred to other parties for their interests out of the original one.

An idea on personal data protection derived from a concept of privacy. The concept itself is an idea to protect individual's integrity and prestige.[3] In the history of its development, privacy was a universal concept and well-known worldwide both verbally and non-verbally in the form of moral norms.[4]

The concept of privacy was, at first, developed by Warren and Brandeis. They claimed, "Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition".[5]

The right of privacy engaged in data protection is the key to have a freedom right as well as protecting individual's prestige. Data protection is a driver leading to political, spiritual, religious, and even sexual freedoms. Those are the basic rights that any individual should have.

Much worries derived from technology development over personal data protection evoked the following practices: digital dossier, personal data collection in huge number using digital technology since 1970 by government in Europe and USA,[6] direct selling, a practice by sellers to market their products through direct marketing; and Location-Based Messaging, a message with advertisement within.

The main problem related to data leakage is on a misunderstanding that, first, personal data is not like properties or assets with property rights, and, second, that the right of protecting personal interest and life is not a part of human rights. In recent days, unfortunately, the regulation on personal data protection in Indonesia is still partial and sectorial, not providing an optimal and effective protection for personal data.

One component of revision on Law in 2016 No. 19 about Electronic Transaction and Information is to implement the verdict of the Constitutional Court No. 20/PUU-XIV/2016 that regulates on (a) the amendment of article 31 subsection (4) which previously provides the regulation of interception or tapping in governmental regulation and turns into laws; and (b) the additional explanation on article 5 subsection (1) and (2) about the availability of electronic information and/or electronic document as a legal evidence. Looking into the verdict of the Constitutional Court which material have been mentioned in a revision of on Law in 2016 No. 19 about Electronic Transaction and Information makes any individual believe that their personal right recorded without their permission may not be violated, and they may use it as a legal evidence in criminal procedure law.

Besides on Law in 2016 No. 19 about Electronic Transaction and Information, it is also mentioned in Governmental Regulation in 2012 No. 82 about the organization of electronic system and transaction (later called PSTE) according to article 15 subsection (3) and further mentioned in Regulation of the Minster of Information and Communication of the Republic of Indonesia in 2016 No. 20 about Personal Data Protection in Electronic System. However, the regulation is not quite enough to accommodate personal data protection.

[2] Wawan Wardiana. (2002). "Perkembangan Teknologi Informasi di Indonesia". disampaikan dalam *Seminar dan Pameran Teknologi Informasi 2002.* tanggal 9 Juli. Bandung: Universitas Komputer Indonesia (UNIKOM), h. 1.

[3] Wahyudi Djafar dan Asep Komarudin. (2014). *Perlindungan Hak Atas Privasi di Internet*. Jakarta: Elsam, h. 2.

[4] Sinta Dewi Rosadi. (2009). *Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional*. Bandung: Widya Padjadjaran.

[5] Samuel Warren and Louis D. Brandeis. (1890). "The Right To Privacy". *Harvard Law Review,* 4 (1), 212.

[6] Daniel J. Solove. (2004). *The Digital Person - Technology and Privacy in the Information Age.* New York: New York University Press, h. 13.

In short, Indonesia is still lack of regulations that specifically organize personal data protection. Many problems previously described require Indonesian government to protect people personal data and set various types of protecting laws. Thus, the authors were interested to study the urgency of enacting personal data protection law as a patronage from the development of information and communication in Indonesia.

METHODOLOGY

This study was a normative legal research (doctrinal legal research). As it was normative, it used statute and case approaches. The data source derived from the primary and secondary legal materials collected through library research supporting the description of this recent study. Document research was also used as means for data collection on written regulation using *content analisys*.[7]

This study used a particular data analysis technique with deductive logic or organizing legal materials through deductive way by describing a general issue and then taking conclusion in more specific manner.

RESULT AND DISCUSSION

Personal Data Protection Law in Indonesia

In recent days, there is no guarantee of security against the easy activities of the exchange of personal data information. Such assurance contains, at least, seven basic principles as mentioned in EU Data Protection Directive: 1. the General Principle-Processing with Consent; 2. Lawfulness, necessary and not excessive; 3. Collection and Notice Principle; 4. Use and Disclosure Principles; 5. Sensitive Personal Data; 6. Security Principle; and 7. Data Retention Principle and Rights to Block Processing.[8]

However, it is still unavailable. Referring to a survey by APJII (an organizing association of Internet network in Indonesia) in 2016, it showed that Indonesia had reached 132.7 million people, indicating that more than half of the total number of Indonesian people (256.2 million people) had been connected to internet. That number should be followed by the development of e-commerce activities in Indonesia. Among 132.7 million users, 98.6% of them or 130.8 million users had already acknowledged internet as means to do merchandising, while 84.2 million people or 63.5% had already made online transaction.[9] This indicated that e-comemrce had been supporting people business activities. In fact, however, e-commerce also brings particular threat besides its positive impact. Valuable information recorded within is vulnerable to be misused by irresponsible parties aiming to disrupt other business or take benefits from it.

In addition to merchandising bank customers, a fraud by misusing the customers' personal data of online transportation on behalf of e-commerce activities are some sample cases of violation of personal data we often see in Indonesia. In fact, e-commerce users need assurance for their personal data in organizing e-commerce activities.

Although e-commerce, in fact, has positive impact, but it also neatly brings a threat in the form of the vulnerability of personal information data to be misused by irresponsible parties aiming to disrupt particular business or take benefits from it.

Thus, Indonesian people are worried due to the leakage of their personal data which evokes several criminal cases such as the leakage of Wikileaks' personal document, short message, credit offer, pornography, credit card number, corporate's private information or data, and so on. Some examples are as follow:

a. On May, 8th 2012, ATM break-ins happened in Bali and East Borneo by monitoring a particular PIN number and copy and paste the data of the customer's ATM card.
b. On September, 7th 2012, the merchandising of bank account with fake data had revealed.
c. On April 17th 2014, a hacker of a corporate's security system in East Java was revealed.
d. On May, 6th 2015, the hijacking of credit card in cyber space was revealed.

To resolve such problems, some products of law regulating the protection of people personal data in Indonesia had been mentioned under several

[7] Peter Mahmud Marzuki. (2011). *Penelitian Hukum.* Jakarta: Kencana Pernada Media Group.

[8] Rasiah D. (2010). "Review of Literature and Theories of Determinants of Commercial Bank Profitability". *Journal of Performance Management*, h. 23.

[9] APJIL. (2016). Hasil Survei Penetrasi dan Perilaku Pengguna Internet Indonesia 2016. *https://apjii.or.id/survei2016.*

regulations in sectorial and incomprehensive manner. Those regulations were as follow:

a. Law in 1971 No. 7 about the basic regulation of archival matters;
b. Law in 1997 No. 8 about Business Documents;
c. Law in 1998 No. 10 about the amendment of Law in 1992 No. 7 about Banking;
d. Law in 2009 No. 36 about Health;
e. Law in 1999 No. 36 about Telecommunication;
f. Law in 2006 No. 23 about Population Administration, in particular to personal data directly related to electronic data; and
g. Law in 2008 No. 11 *juncto*. Law in 2016 No. 19 about Electronic Transaction and Information.

Law in 2016 No. 19 about Electronic Transaction and Information does not mention the provision of personal data protection in specific way. However, this implicitly sets a new understanding about the protection of electronic data and information, both public and personal. Personal data protection in electronic system mentioned in on Law in 2016 No. 19 about Electronic Transaction and Information includes: the protection from any usage without permission, the protection from illegal access and interference, and the protection from the host of electronic system. In regard to personal data protection in terms of the usage without permission, Article 26 on Law in 2016 No. 19 about Electronic Transaction and Information requires that the utilization of any personal data in a particular electronic media should have permission from the owner of the data. Every individual violating this provision can be sued due to the damage it evokes. Even in its development, the enactment of Law in 2016 No. 19 along with Article 26 (right of forgotten) mentioned that the host of electronic system should delete any irrelevant electronic information and/or document under its control due to the customers; request based on the provision of the court. The wording of Article 26 on Law in 2016 No. 19 about Electronic Transaction and Information is as follow:

a. Unless otherwise provided by Law, the utilization of any information through electronic media relating to an individual's personal data should be executed under the owner's permission.
b. Every individual whose right is violated as mentioned in subsection (1) may request for lawsuit on any disadvantages that evoke based on this regulation.
c. Every host of electronic system is required to delete any irrelevant electronic information and/or document under their control according to the owner's request based on the provision of the court.
d. Every host of electronic system should provide a mechanism of deleting any irrelevant electronic information and/or document according to the provision of Law.
e. The provision on the procedure of deleting electronic information and/or document as mentioned in subsection (3) and (4) under the government regulation.

In its explanation, article 26 on Law in 2016 No. 19 about Electronic Transaction and Information mentioned that in taking benefit from information technology, personal data protection was a part of privacy rights. More detail explanation of article 26 on Law in 2016 No. 19 about Electronic Transaction and Information on privacy right is as follow:

a. Privacy rights are rights to enjoy privacy life and feel free from any disruption,
b. Privacy rights are rights to communicate to others without having worried of being spied.
c. Privacy rights are rights to control the access of own personal data information.

Sonny Zulhuda from International Islamic University Malaysia argued that Law in 2016 No. 19 about Electronic Transaction and Information was still insignificant in regulating the use of individuals' personal data as it was general and not comprehensively accommodating people personal data. The limitation of this Act was that the term of "the utilization" of any information was vague, whether it involved the term "collecting," "processing," "filing," "disseminating," or any other similar terms. In regard to the term *consent*, he questioned whether this Act classified the utilization of personal data under the owners' permission into the implied consent or explicit consent.[10]

Looking into other countries, this issue of personal data protection had been seen as a part of human rights to be protected and thus, it had a

[10] Sonny Zulhuda dan Iwan Satriawan. (2007). "The Integration of Islamic Law Into Indonesian Legal System: The Issues and Developments". *Jurnal Media Hukum*, 1(1), h. 3.

specific law as the regulation. Europe, for instance, had already a legal regulation that protected the personal data of its people since one decade ago.[11] This present study, therefore, provided two countries with comprehensive law on personal data protection as the examples.

England provided a regulation about personal data protection for its people in Data Protection Act 1998 and it had been applied since March 1st 2000. This act provided a protection for people privacy rights through which any subject might be able to whether access or block any information about personal data processing. However, there were some exceptions for particular issues related to national security, crime, taxes, health, education, and social working.[12]

The subject also had some open options to keep an eye on any organization that processed their personal data. First, they might require the user not to process their personal data if it would bring into unreasonable and substantial damages for them or others. However, this would not work if the subject had already given their permission to process their personal data necessary for implementing a contract through which the subject was obliged to obey the law in claim or for protecting a crucial matter. Second, the subject might block the processing of their personal data aimed for direct marketing, including the distribution of electronic mail to individuals for promoting any particular products or services and directed to ones' email accounts. Third, based on Article 14 of Data Protection Act 1990, the Court found that when a personal data was processed by inaccurate data controller, the court had authority to revise, block, omit, or corrupt the data. Forth, the user of the data could be blocked automatically as the owners' request. Fifth, ones who believed that they were being directly affected by personal data processing might request the commissioner to evaluate the processing in order to determine whether it had met the provision of Data Protection Act 1998. This evaluation could establish the announcement of particular information or legal action.[13]

Our neighbor country, Malaysia, had also set individual personal data protection in a specific Act. In 2010, the Parliament of Malaysia had legitimate Malaysia Personal Data Protection Act, later called PDPA. The primary aim of PDPA was to the processing of personal data processing by users, in the context of commercial transaction, in order to protect the subjects' privacy.

This Act also regulated cross-border transfer by mentioning that there would be no data transfer occurred out of Malaysia unless it had been set by the Minister of Information, Culture, and Communication. And, the destination countries of the data transfer should have a particular level of protection which was equal to PDPA.

Specifically, this Act applied jurisdiction in 3 (three) conditions. First, the utilization of data was hosted in Malaysia and the user may process the data, whether it related or not to the process of hosting. Second, the data processing was conducted by any individual registered as data users in Malaysia. Third, when the use of data was not hosted in Malaysia, it should use the infrastructure of Malaysia to process the data.

The processing and protection of personal data in this Act contained seven principles of data protection. The principles were more influenced by EU Data Protection Directive[14] rather than OECD Guidelines or APECF framework.[15] Those principles were as follow:

a. The General Principle-Processing with Consent. It was a general principle by Article 6 of PDPA and it regulated that the data user might not process personal data unless they had permission from the data subject.
b. Lawfulness, necessary and not excessive. Article 6 subsection (3) PDPA mentioned 3 (three) additionally general boundaries for data processing based on its purposes: (a) the processing should have legal objectives and directly related to the activities of the data users; (b) the implementation of data processing should be directly related to the objectives of the data processing; and (c) personal data processing should be appropriate to its objectives, but not exceeded.

[11] Gupinder Assi. (2013). *"South East Asia: Data Protection Update"*. http:// www.bryancave.com/bulletins, h. 1.

[12] Laurel J. Harbour, Ian D. MacDonald, and Eleni Gill. (2003). "Protection of Personal Data The United Kingdom Perspective". *Defense Counsel Journal*, h. 104.

[13] Laurel J. Harbour, et.all. *op.cit.*

[14] Edmon Makarim. *op.cit.*

[15] Rasiah D. *op.cit.*

c. Collection and Notice Principle. The data users should have permission from the data subject.
d. Use and Disclosure Principles. Article 6 subsection (3) PDPA required that personal data processing would not be executed unless: a.The personal data was organized for a legal purpose and directly related to the activities of the data users, and b.Personal data processing was necessary and having a direct relation with the purpose of collecting the personal data.
e. Sensitive Personal Data. It was personal data about medical and mental condition, politic choices, religion and other faith, accusation of crime, and other personal data which the authorize minister defined it as sensitive personal data.
f. Security Principle. It required the users to 'take several procedures to be applied' to meet the six security factors.
g. Data Retention Principle and Rights to Block Processing. Personal data might not be saved any longer if the fulfillment of the objectives had been received.

While the principles of protecting personal data set out in the EU are:

a. Personal data must be obtained honestly and legitimately.
b. Personal data must be owned only for one or more specific and legitimate purposes. And may not be further processed in a way that is inconsistent with those objectives.
c. Personal data should be feasible, relevant, and not too broad in relation to the purpose or purposes of its processing.
d. Personal data must be accurate and if necessary always up-to-date.
e. Personal data shall be processed in accordance with its purpose and shall not be controlled longer than the time required for the purposes of such purpose or purposes.
f. Personal data must be processed in accordance with the rights of the data subject set forth in this law
g. Adequate security measures shall be taken to deal with the unauthorized processing of personal data and for any unexpected loss or damage to personal data.
h. Personal data shall not be transmitted to other countries or regions outside the European Economic Area unless such country or territory assures with a degree of protection of the rights and freedoms of data subjects in connection with the processing of personal data

OECD Principles: Collection Limitation Principle; Data Quality Principle; Purpose Specification Principle; Use Limitation Principle; Security Safeguards Principle; Openness Principle; Individual Participation Principle; Accountability Principle.

Compared to other countries, Indonesia had been far left in providing a specific regulation to assuring individuals' personal data protection. Indonesia immediately needed to set such specific regulation on personal data protection. One reason was to improve its economic value in international business relation. If Indonesia had set a firm regulation on personal data protection, other countries would no longer worry to have business relation with Indonesian people through cyberspace, as it would be automatic through data transfer. Developed countries confirmed that data transfer might only be conducted in countries with firm privacy protection.

In addition, a specific regulation on personal data protection was a part of law of human rights. In Indonesia, anxiety on privacy and personal data protection did still exist as no specific and certain regulation had been set yet. Thus, it should be an urgent agenda for this modern era.

Scope and Materials of Regulation of Personal Data Protection

Regulating personal data protection in Indonesia had been set sporadically and incomprehensively in some provisions based on particular sectors, which brought problems for consumers. Furthermore, it was only a cover without a passion of fair play, and even likely to ignore individual rights.[16]

The disharmony of the regulation in regulating personal data protection made them need a specific rule for it. The specific regulation should, at least, accommodate some matters as follow:

[16] Ualikhan A. Akhatov, *et.all.* (2018). "Harmonization of Enviromental Legislation". *Journal of Legal, Ethical and Regulatory Issues,* 21(1), 1-6.

1. **The Obligation of The Host of Personal Data**

The primary obligation of the host of personal data before organizing the data was asking for permission from the data subject/ costumers. The permission involved:

a. The legality for the host of personal data;
b. The purpose of organizing the personal data;
c. Kinds of personal data to be organized;
d. The period of retention of the document which contains the personal data;
e. The detail of information to be collected;
f. The period of time of organization and deletion of personal data by the host; and
g. The rights of the data subject to change and/ or refuse the consent.

The obligation of the host was not stop as they had the personal data they seek for. Other additional obligations that they should hold were:

a. Not publishing their customers' personal data;
b. Deleting the personal data if they had reached their purposes, or if the customers requested for deletion; and
c. Making sure the security of the personal data they organized, including: Designing the best procedures to protect any personal data from alteration, damage, and publishing; Implementing the operating technical procedures to protect the personal data they organized; and Determining the level of security for personal data by considering the features of personal data to be protected, the size of the data, and the risk of organizing the data.

In addition, the host should monitor any individuals that got engaged in personal data processing under the authority and control of the host itself.

2. **International Transfer of Personal Data**

In globalization era, an issue to be concerned is to optimally accommodate both national and international interests. In regard to international transfer of personal data, several international documents such as OECD Guideline, EC Directive, and AFTA Privacy Framework might be able to be used as reference to provide nationally legal norms.

The hosts of personal data were not allowed to make international transfer out of the Republic of Indonesia unless it had a firm regulation dealing with personal data protection. Another issue to be concerned was that the hosts of personal data should ask for and get permission before conducting data transfer to the third party inside the Republic of Indonesia.

In relation to the ease of governmental business activities, it needed to make a specific policy to prevent any violation on personal data and to improve the standard of security for personal data in international setting, as well as the policy on personal data so that the subjects' rights might not be disrupted due to cross-border data transfer.[17]

Regulations on data protection might strengthen the function of Indonesia as a credible business center and creating conducive condition for the development of management of global data in data processing industry.

3. **The Organization of Supervision Committee**

A firm regulation remained ineffective if it was not supported by an authority of good implementation and the procedures of well compensation through a specific organization.

Reflecting to countries worldwide, we might see two patterns of organizing a supervision committee. First, the organization of the committee was held independently with some primary tasks and functions based on the act of personal data protection. Malaysia is one applying this pattern. The authorized minister, under the provision of Law, assigned a party to be Personal Data Protection Commissioner. Second, the organization was by assigning tasks and functions related to personal data protection to the existing committee. In this case, for instance, it would join public information committee. England was one with this pattern through The Information Commissioner's Office.

Indonesia might organize a supervision committee of personal data by selecting one of those two patterns; given that Indonesia had already had KIP (central information committee)

[17] Ualikhan A. Akhatov, *et.all.* (2017). "Digital Goverment Model: Theory and Practice of Modern Public Administration". *Journal of Legal, Ethical and Regulatory Issues,* 20(3),1-10.

organized under the Act of 2008 No. 14 about the openness of public information.

4. **Public Participation**

In recent days, fee people saw the importance of protecting their personal data. Therefore, to facilitate the organization of personal data protection and to empower people participation, public needed to have better understanding on issues that dealt with personal data protection.

Empowering public was through education and/or training, advocate, technical course, socialization by various media.

5. **The Provision of Sentences**

Sentences were charged in the form of both criminal and common sentences to ones misusing personal data. Criminal sentences might be charged to every individual stealing and/or falsifying any personal data for criminal purposes. Both jail and fine were sentences for such crime.

In addition to the provision of criminal sentences, ones feeling disadvantageous due to the misuse of their own personal data by a host of personal data might file a claim to the public court.

The subject of the data might, at first, report the misuse of their personal data to the supervision committee, and the committee was obliged to facilitate the solution and provide assistance toward the subject.

CLOSING

Conclusion

The regulation on personal data protection was still ineffective as it was scattered into some sectorial regulations, and thus, a firm and comprehensive regulation for such issue was crucial. Compared to other countries that had already provided some Acts for personal data protection, Indonesia was far left behind.

The disharmony on regulations that set the protection of personal data created a necessity of specific regulation that specifically regulated such issue. At least, the latter regulation might regulate the obligation of the host of personal data, international data transfer, the organization of supervision committee, public participation, and the firm provision of sentences.

It needs a specific regulation that is capable to support both e-commerce and other information-based activities through Personal Data Protection as the current Act is not yet capable to provide security toward consumers' personal data.

Given the urgency of regulation that sets personal data protection, this study needs further investigation such as: conducting in-depth comparison study that compares some countries applying personal data protection, having coordination, discussions, and socializations with various related interests.

Recommendation

There is a need for a separate law capable of supporting e-commerce activities and other activities based on information exchange through Personal Data Protection as a result of existing laws and regulations that have not been able to provide protection for consumer Personal Data.

Given the urgency of the existence of laws regulating the protection of personal data, this study needs to be followed up with activities such as: comparative studies of several countries that have regulated more in-depth protection of personal data, coordination, discussion, and socialization with various related interests.

REFERENCES

Books:

Daniel J. Solove. (2004). *The Digital Person - Technology and Privacy in the Information Age*. New York: New York University Press.

Edmond Makarim. (2010). *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Jakarta: Raja Grafindo Persada.

Peter Mahmud Marzuki. (2011). *Penelitian Hukum*. Jakarta: Kencana Pernada Media Group.

Sinta Dewi Rosadi. (2009). *Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional*. Bandung: Widya Padjadjaran.

Wahyudi Djafar dan Asep Komarudin. (2014). *Perlindungan Hak Atas Privasi di Internet*. Jakarta: Elsam.

Journals:

Laurel J. Harbour, Ian D. MacDonald, and Eleni Gill. (2003). "Protection of Personal Data The

United Kingdom Perspective". *Defense Counsel Journal*, h. 104.

Rasiah D. (2010). "Review of Literature and Theories of Determinants of Commercial Bank Profitability". *Journal of Performance Management*, h. 23.

Samuel Warren and Louis D. Brandeis. (1890). "The Right To Privacy". *Harvard Law Review*, 4 (1), 212.

Sonny Zulhuda dan Iwan Satriawan. (2007). "The Integration of Islamic Law Into Indonesian Legal System: The Issues and Developments". *Jurnal Media Hukum*, 1(1), h. 3.

Ualikhan A. Akhatov, et.all. (2017). "Digital Goverment Model: Theory and Practice of Modern Public Administration". *Journal of Legal, Ethical and Regulatory Issues*, 20(3),1-10.

_____. (2018). "Harmonization of Enviromental Legislation". *Journal of Legal, Ethical and Regulatory Issues*, 21(1), 1-6.

Others:

APJIL. (2016). Hasil Survei Penetrasi dan Perilaku Pengguna Internet Indonesia 2016. *https://apjii.or.id/survei2016*.

Gupinder Assi. (2013). "South East Asia: Data Protection Update". *http:// www.bryancave.com/bulletins*.

Wawan Wardiana. (2002). "Perkembangan Teknologi Informasi di Indonesia". disampaikan dalam *Seminar dan Pameran Teknologi Informasi 2002*. tanggal 9 Juli. Bandung: Universitas Komputer Indonesia (UNIKOM).