International Journal of Sciences: Basic and Applied Research (IJSBAR)

ISSN 2307-4531
(Print & Online)

http://gssrr.org/index.php?journal=JournalOfBasicAndApplied

Legal Protection of Cloud Computing User on Privacy and Personal Data

Muh. Firmansyah Pradana[a]*, Judhariksawan[b], Maskun[c]

[a,b,c]*Law Faculty, Hasanuddin University, Makassar 90245, Indonesia*

[a]*Email: dhana.indp@gmail.com*

[b]*Email: judhariksawan@yahoo.com*

[c]*Email: maskunlawschool@yahoo.co.id*

Abstract

This research was a normative research that is based on library research regarding to the prevailing laws and regulations, and legal literatures such as books, journals, articles on the internet and other legal materials. The results of this study indicate Legal Protection Against to Cloud Computing Users on Privacy and Personal Data regulated in International, regional and national regulations. The international instruments can be found in Universal Declaration of Human Rights 1948 (UDHR), the International Covenant on Civil and Political Rights 1966 (ICCPR), the European Convention on Human Rights 1950 (ECHR), American Convention on Human Rights 1969 (American Convention on Human Rights), and Cairo Declaration on Human Rights 1990. In the regional context, Malaysia is known by with the Personal Data Protection Act. Meanwhile for the national context, Indonesia itself has not been clearly regulated.

Keywords: Cloud Computing; Personal Data Protection.

1. Introduction

Indonesia is a state law, the term of state law is similiar with *rechtsstaat* atau *rule of law*, those three terms contain the same purposes which are prohibit absolute power for the sake of recognition and human rights protection [1].

---

* Corresponding author.

It can not be denied that the advancement of information and communications technology change society's attitudes and behaviour in the way of communication and interaction. Nearly all the aspects of society life always surrounded by technology and it is proven that technology is beneficial for the human advancement and civilization. Technological advancement results some circumstances that society never consider before [2]. Technological advancement particularly in computing has given convenience for society in their daily activities. The advancement that has been achieved always go hand in hand between software and hardware.

Cloud Computing is a combination of computing element, internet and server. Users use service from cloud computing company to save data including costumer's privacy data that is sensitive and has to be protected. Issues regarding the importance of protection on personal data is getting strong along with the increase number of mobil phone and internet users. Some of prominent cases particularly regarding personal data leakage and induce fraud action or criminal acts of pornography, thus strengthen the importance to create regulation to protect personal data.

Protection on personal data is related to the privacy concept. Privacy concept is an idea to protect integrity and dignity of individual. Right to privacy is the ability of individual to decide who is eligible to keep their information about them and the way the information is used [3]. The concept of data protection intimates individual to have rights for deciding whether they will share or exchange their personal data. Moreover, individual also has rights to decide the requirements to transfer their personal data. Furthermore, data protection also related to the concept of right to privacy. Right to privacy has been developed, thus it can be used to create rights for protecting personal data [4]. Rights to privacy through data protection is the key element for freedom and dignity of individual. Data protection becomes a booster for the realization freedom of politics, spiritual, religions and even for sexual activity. Right of self-determination, freedom of expression and privacy are significant rights to make us as human.

Considering the benefits of cloud computing system, the costumers are required to pay based on their needs. For instances, Microsoft Azure company put up a price about $360 (three hundred and sixty dollar) per month for *Basic Storage* for the capacity of 6 (six) *Terabyte* and BIZnet Indonesia for *Gio Public Cloud* Service put up a price around Rp. 1.400.000,- (one million and four hundred thousand rupiah) for the capacity of 500 (five hundred) *Gigabyte* per month [5]. Furthermore, data that has already logged into the server will be managed and protected by *cloud computing* service providers.

Cloud computing system is one of the thing that related to personal data which should be protected. One of the prominent case is the break-in data that occured to Yahoo. Yahoo announced that about one billion of their user accounts have been hacked by unknown parties in August 2013 and just reported the case on September 2016. The stolen account information includes usernames, email addresses, phone numbers, birth dates, random passwords and in some cases security questions and answers that are encrypted or not encrypted [6].

From that case, there is an interest to provide protection of personal data that equivalent to other countries. Regulation about personal data protection is intended to protect the interest of consumers and provide economic benefits for Indonesia. Indonesia has not yet had regulation that specifically regulates personal data. The various

problems above require Indonesian government to protect society and manage the issue of personal data protection and prepare various forms of legal protection.

3. Research Question

How is the legal protection of Cloud Computing Users on privacy and personal data?

4. Research Method

4.1 Research Model

The research model to be used in this paper is normative legal research. Normative legal research uses normative case studies of legal behavior, such as reviewing laws. The subject of the study is the law that is conceptualized as the norm or rule that is applicable in the society and becomes the reference of society's behavior. Thus, normative legal research focuses on the inventory of positive law, legal principles and doctrines, legal discovery in concreto, systematic law, synchronization level, comparative law and legal history [7].

4.2 Models and Sources of Law

4.2.2 Primary Law Sources

- Law No. 11 of 2008 on Electronic Information and Transactions
- Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions
- Government Regulation No. 82 of 2012 on the Operation of Electronic Systems and Transactions
- Malaysia Personal Data Protection Act 2010.

4.2.3 Secondary Law Sources

Obtained through the study of research results, books, scientific journals, jurisprudence and other literatures that discusses about the protection of personal data. In order to obtain more comprehensive understanding, comparative study of secondary data related to the protection of personal data in another country such as Malaysia is also made.

4.2.4 Tertiary Law Sources

Sources that provide guidance as well as explanation of primary and secondary law sources.

4.2.5 Data Collection Techniques

Tertiary Law Sources, is sources that provide guidance and explanation of law materials.. The technique of collecting the data that used in this research is done by library research on legal materials which are primary, secondary and tertiary legal materials.

4.2.6 Data Analysis Techniques

The data that have been collected will be analysed by using content analysis technique. This technique will be used to search and examine more deeply about the content in the regulations.

5. Discussion

5.1 Legal Protection of Cloud Computing User on Privacy And Personal Data

The advancement of computer systems and internet create information to be more convenient to be found and shared. The basic concept of personal data protection first appeared around 1960. In 1970, Hesse State in Germany was the first state to enforce regulation about data protection, followed by national law in Sweden in 1973, West Germany in 1977, United States of America in 1974, France in 1978 and England in 1984 [8]. The concept of data protection often be considered as part of privacy protection. Data protection basically relates to privacy as proposed by Allan Westin who for the first time defines privacy as individual, group or agency rights to determine whether information about them will be communicated or not to other parties, thus the definition stated by Westin is called information privacy as it involves personal information [9].

Considering the wide scope of privacy, then according to Abu Bakar Munir, privacy can be categorized into 4 (four) groups namely [10]:

- Information privacy, related to the method of collection and management of personal data such as credit information and medical records;
- Bodies privacy, related to the physical protection of individual such as procedure of anesthetic-use, biometric data retrieval such as fingerprints and eye retinas;
- Communication privacy, consist of the protection of individual communication, for instances mail, phone, email or other forms of communication;
- Territorial privacy, for instances privacy in domestic or residential environment, privacy in the workplace.

Several international instruments have regulated principles of data protection and many national rules have included them as part of national law. Data protection is a fundamental human right, several countries have recognized data protection as a constitutional rights or in the form of '*habeas data*' which is the right of individual to obtain security towards their data and for justification when errors are found in their data. Albania, Armenia, Phillipines, Timor Leste, Colombia and Argentina are countries with historical dan cultural differences that have recognized the role of data protection which can facilitate the democratic process and have guaranteed its protection in their constitution.

ASEAN Human Rights Declaration that has been recently adopted by ASEAN countries also recognizes the right to privacy of personal data in Article 21. Nowadays, there are many countries have laws about data protection, at least more than 120 countries that have laws on data protection [11].

5.1.1 International Instruments

The concept of protection on privacy data and users have been stated in several international instruments that have been recognized internationally, thus made the legal foundation for modern national data protection. Some of those instruments evolve with settings of specific data privacy and some other instruments regulate the general rules that cover issues including privacy. Here are various international conventions that protect privacy:

- Universal Declaration of Human Rights 1948 (UDHR). Universal Declaration of Human Rights 1948 is the first international instrument that protect right to privacy of individual, specifically stated in Article 12 :

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honours and reputation. Everyone has the right to the protection of the law against such interference or attacks."

It implies that everyone should have legal protection since they have right not to be disturbed for their privacy, their family, their residence and their correspondence or their honor and reputation. Article 12 mentioned the terms of privacy that shall be regarded as umbrella terms since it is related to the protection of other rights of the family, residence, correspondence also including honor and reputation.

- International Covenant on Civil and Political Rights (ICCPR) 1966. The regulation about privacy in Article 17 adds the words of arbitrary or unlawful, so then the states are not only given the obligation to protect their citizens through regulations but also to prohibit such privacy violations.

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

- European Convention on Human Rights (ECHR, 1950). Privacy is legally protected and culturally recognized in Europe since the end of World War II when privacy for the first time was regulated in Universal Declaration of Human Rights in 1948, Council of Europe has adopted the European Convention on Human Rights in 1950. Article 8 of ECHR stated that:

"eveyone has the right to respect for his private and family life, his home and his correspondence"

The rights are widely interpreted in the terms of neutral technology so that can apply to the electronic market and online environment. The cases in the European Court of Human Rights (ECHR) confirm that Article 8 provides for the protection of data privacy. Article 8 consist of 2 paragraphs. In Article 8 paragraph (1) regulates four types of privacy violations (ECHR does not use the term of privacy, but uses the term of private life) which are violation of private life, family, residence and correspondence. European Commission does not attempt to define the meaning of personal life more deeply since the meaning of personal life will always evolve as the society develops.

- American Convention on Human Rights (ACHR), 1969. Human rights protection in America also follows the developments of international regulation about privacy, which regulated in Article 11:

"Everyone has the right to have his honour respected and his dignity recognised and his dignity recognised. No one may be the subject of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation. Everyone has the right to protection of the law again such interference or attacks."

The regulation about privacy in ACHR is similar to other international and regional instruments, only in Article 1declares that one of the privacy protection is dignity.

- Cairo Declaration on Islamic Human Rights, 1990. Islamic world also recognizes privacy as a right that must be protected as regulated in the Cairo Declaration on Human Rights in Islam in the Article 18 (b) and (c):

"everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships it is not permitted to spy on him, to place him under surveillance or to besmirch his good name. the state shall protect him from arbitrary interference. A private residence is inviolable in all cases. It will not be entered without permission from its inhabitants or in any unlawful manner nor shall it be demolished or confiscated and its dwellers evicted."

The scope of privacy regulation in the Cairo Declaration is broader when compared to other international instruments, which includes his private affairs, in his home, among his family, with regard to his property and his relationships his good name. Africa also has regional instrument namely African Charter on Human and People's Rights 1981, but it does not regulate privacy protection and this is the only regional instrument that does not regulate about privacy.

5.1.1.1 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980

These guidelines support the collection of data privacy that obtained lawfully and the data is accurate, updated and relevant, also necessary according to the purpose of collecting such data. Data privacy must be protected with appropriate security and should not be open or made publicly available for any reason other than the initial reason why such data is collected, except with the consent of the data owner and legal authority. These guidelines explain that the following principles should be implemented when undertaking data privacy management, those principles are Collection Restrictions, Data Quality, Specification of objectives, Disclosure Restriction, Security Measures, Openness, Individual Participation and Responsibility.

5.1.1.2 Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data ,1981

The Council of Europe Convention 1981 is the first legally binding instrument in the field of data protection. This Convention requires the parties to take necessary steps in their national law to apply the prescribed

principles to ensure the respect of the basic fundamental rights for all individual concerning the management of data privacy in their territory. The principles concern about data collection fairly and process of automated data, storage of data for legitimate purposes and not for use against the purposes or stored longer than it needed. Related to the quality of data, it should be sufficient, relevant and not excessive (proportional), accurate, confidential; contains information from the data subject and provides right to access and improvements. This convention provides freedom to the flow of the data privacy between state parties. The freedom of this flow does not preclude the protection of data privacy except the reasons of the parties deviating from this provision, which may be created two specific cases, the protection of data privacy in other parties is unbalanced, or data transferred to the third country which is not the party of the Convention.

5.1.1.3 United Nations General Assembly Resolution on Right to Privacy in the Digital Age, 2014

On 25 November 2014, The Third Committee of the United Nations General Assembly adopted resolution calling on states to respect and protect the right to privacy in the Digital Age. This resolution is a movement response that led by Germany and Brazil related to the case of Edward Snowdent. Germany and Brazil succeeded in encouraging the adoption of resolution that supported by more than thirty-five states including Indonesia. The adopted resolution is about The Rights to Privacy in the Digital Age.

5.1.2 Regional Instruments

In 1998 periodically, Malaysian minister consistently implemented draft of legislation concerning data protection. Finally, in 2010 Malaysian government ratified Personal Data Protection Act (PDPA). Subsequently, Malaysian government established a new privacy Data Protection Department under the Ministry of Information Communication and Culture which has authority to supervise the implementation of PDPA 2010.

Principle of Data Privacy Protection in PDPA 2011 Section 5 to Section 12 contain 7 (seven) principles of data privacy protection, namely: general principles-processing with consent, notification and option, disclosure, security, data integrity, retention and access. Those principles are more affected by the EU Data Protection Directive than OECD Guidelines or APEC Framework [12].

The General Principle-Processing with Consent that regulated in Section 6 PDPA stated that data users cannot process data privacy unless the subject of data has given consent. Processing has a broad definition, covering everything from the initial collection, storage, use and disclosure, also the destruction of data privacy. The processing of data privacy without consent is possible, for instance when it concerns about the vital interest of the subject of data and the management of data privacy based on statutory order or for the interest of the judiciary. This exclusion does not apply to the data privacy that is sensitive, which only can be processed in accordance to Article 40 PDPA 2011 [13].

Section 3 on Personal Data Protection Regulation 2013 regulates relative details of consent . Consent must be made in the form of that can be recorded and maintained properly. For children under age of 18, consent may be granted from their parents or their guardian [14].

- *Lawfulness, necessary and not excessive*. Section 6 paragraph (3) PDPA adds 3 (three) other general limits on processing of data privacy, based on the purpose, which are : (1) processing must be carried out for legitimate purposes and directly related to the activities of data usage. (2) the implementation of data processing must be directly required or related to the purpose of data processing. (3) Data privacy that has processed must be sufficient to achieve the purpose of data processing, but must not be excessive [15].
- Collection and Notice Principle: The data users that will perform data processing in advance shall obtain approval from the data subject. The data users are required to provide written notice concerning the purpose of data privacy collection . Notice must be given as soon as possible when the data that is collected from data subject implies notification.
- Use and Disclosure Principles: The use of data privacy in Section 6 paragraph (3) PDPA that requires data privacy cannot be process except data privacy is processed for legitimate purposes and directly related to data users activity, and the processing of data privacy is required or directly related to the purpose of data privacy collection.

- Secondary use is based on consent, not based on direct relationship to the purpose of collection. On the other hand, data privacy can only be disclosed for the initial purpose, and also must include the third party that has been notified by the data users that they can disclose the data. The data users must still determine that the notice is an agreement of data subject to process the data. Since the notice is not a blank check for data users to disclose data privacy to whomever they choose. Additionally, disclosure is also possible due to the exceptions that regulated in Section 6 PDPA.
- Section 5 PDPA 2013 requires data users must create list of data privacy disclosure that relate directly to the purpose of disclosure. However, disclosure list is not required if disclosure is made based on exceptions in Section 6 PDPA.

- Sensitive Personal Data. Sensitive data privacy is data privacy concerning health or physical condition, mental, political choice, religion, and other beliefs. The allegation of conducting violation and any other data privacy which the authorized minister decides it as sensitive data privacy. Sensitive data should also be a privacy data since data privacy is limited to information about commercial transactions, thus it limits the scope of protection of data privacy that is sensitive. Malaysia only uses some from all sensitive data category in European Union, eliminating racial categorization as well as trade union membership and sexual orientation from sensitive privacy data, even if those are sensitive topics in Malaysian society.
- To be able to perform sensitive privacy data processing requires explicit consent. Sensitive privacy data processing is also possible without consent if the process falls into the category of exceptions. Among the broad exceptions list of consent, there is an exception that sensitive data is processed to perform the functions that given to any person with or under regulation or for any other purposes established by authorized minister. There is also exception when someone has published their own sensitive privacy data. However, there is a doubt that the provision about the management of sensitive privacy data will be misused by Malaysia (which is no bound to PDPA) [16].
- Security Principle requires data user to take measures that can be implemented to meet the 6 (six) security factors. Section 6 Personal Data Protection Regulations requires data users to have security policy that

complies to security standards which establish periodically by the Commissioner in the protection of data privacy in Malaysia. They also must ensure that any data processor acting on their behalf complies to the policy.

- Data Retention Principle and Rights to Block Processing. Data privacy cannot be stored any longer if legitimate fulfillment has been reached. Data users have responsibility to ensure that the data privacy is subsequently destroyed or permanently destroyed. Data users must comply to the standard retention established by Commissioner of data privacy protection. Data subject based on Section 38 PDPA may withdraw their data processing consent at any time and for this situation, the users shall comply. This related to the exceptions that stated in the Section 6 PDPA, when consent for processing data privacy is not required. Data subject may also make a notice to request a processing termination or prohibition to conduct the processing, for certain period of time or for particular purposes, if (for other reasons) the processing may cause substantial loss or pressure to the data subject or others. The right to withdraw the processing permits under Section 38 PDPA is highly important especially in the practice of direct marketing. The use of data privacy for direct marketing practices is not one of the exceptions to the requirements of data processing agreement, thus data subject may retract the approval of data privacy management in the direct marketing practice. In other words, data subject has the right to opt out of direct marketing practice at any time and regardless from the consent that they have given before.
- Data Integrity Principle, data user must take reasonable steps to ensure that data privacy is accurate, complete, not misleading and up-to-date by taking into account the purposes, including related direct purposes. Data privacy also must comply to the integrity of standard data that established by the Commissioner of data privacy protection.
- Access and correction Principle. Data subjects who have right to access their data and to fix if there is inaccurate, incomplete, misleading or outdated data privacy. This is excluded if the request from data subject is denied under the regulation. The reason is the access and correction rejection procedure are regulated in Section 30-37 PDPA. Furthermore, Personal Data Protection Regulations 2013 established the requirements that data subject have rights of access and correction, for instance the data subject must include name, address and identity card unless Commissioner of Personal Data Protection determines otherwise.

5.1.3 National Instruments

Related to the privacy and data protection in Indonesia, Indonesia may ratify all the international instruments that applicable at the national level. Indonesia has signed OECD (*Organization for Economic Cooperation and Development*) in 2004, enforcing the implementation of regulation concerning privacy and data protection. As the member of APEC *(Asia-Pacific Economic Cooperation*), Indonesia follows *APEC Privacy Framework* 2004, that clearly states in its preamble:

"the potential of electronic commerce cannot be realized without government and business cooperation to develop and implement technologies and policies, which build trust and confidence unsafe, secure and reliable communication, information and delivery system, and which address issues including privacy…"

This membership encourages state members in their national legislation to recognize the protection of privacy for balance and the promotion of effective information to promote economic cooperation especially in electronic commerce among members and Indonesia is one the 35 (thirty-five) states that encourage the adoption of United

Nations General Assembly Resolution on Right to Privacy in the Digital Age that proposed by Germany and Brazil. Indonesia has established several regulations that regulated about privacy in various fields such as:

- Law No. 2 of 2014 on Amendment To The Law Number 30 of 2004 on Position of Notary.
- Law No. 10 of 1998 on Banking System.
- Law No. 36 of 1999 on Telecommunications.
- Law No. 8 of 1999 on Consumer Protection.
- Law No. 39 of 1999 on Human Rights.
- Law No. 23 of 2006 on Population Administration.
- Law No. 11 of 2008 on Electronic Information and Transactions
- Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions
- Law No. 14 of 2008 on Public Information Disclosure.
- Law No. 36 of 2009 on Health.
- Government Regulation No. 82 of 2012 on Electronic System and Transaction Operation (PP ITE 2012).
- Presidential Regulation No. 67 of 2011 on The Implementation of Identity Card Based on National Registration Number.
- Bank Indonesia Regulation No. 7/6/PBI/2005 on Transparency in Bank Product Information and Use of Customer Personal Data.

Related to the placement of electronic data, Article 17 paragraph (2) and paragraph (3) in the Government Regulation No. 82 of 2012 on Electronic System and Transaction Operation, requires the Provider of Electronic System for public services to place *Data Center* (DC) and *Disaster Recovery Center* (DRC) in Indonesia. Article 17 paragraph (2) and (3) stated that:

- The operator of electronic system for public services must place Data Center and Disaster Recovery Center in Indonesia for the purposes of law enforcement, protection and enforcement of state sovereignty over the data of its citizens.
- Further provisions regarding the obligation for the placement of Data Center and Disaster Recovery Center in Indonesia as referred to paragraph (2) are regulated by the Supervisory Agencies and Sector Management according to the provisions of regulations after coordinating with the minister.

If a cloud computing provider is included in the category of Public Service PSE, then the cloud computing service provider shall place Data Center and Disaster Recovery Center in Indonesia. Data Center referred to Article 17 paragraph (2) of PP PSTE is defined in the explanation of Article 17 paragraph (2) PP PSTE, the definition is a facility that is used to place Electronic Systems and its related components for the purposes of placement, storage and data processing. Meanwhile, Disaster Recovery Center is a facility that is used to recover the data or information as well as the important functions of Electronic Systems that are disturbed or damaged by the natural or man-made disasters.

Sanctions for the violation of Article 17 paragraph (2) of PP PSTE are not expressly regulated. Article 84 of PP PSTE on administrative sanctions only impose sanctions if the PSE public services do not have a continuity plan to deal with disruptions or disasters in accordance with the inflicted risks. Meanwhile, non-compliance to the obligation in placing DC/DRC in Indonesia can be categorized as an act of not having continuity plan as stated in Article 17 paragraph (1) OF PP PSTE but there is no further explanation about it.

Article 17 of PP PSTE certainly still requires more comprehensive explanation in the form of Ministerial Regulation or Regulations from each related sector, since the placement of DC or DRC in the Article 17 is not sufficiently clear about the technical limitation on what kind of facilities that can be referred to as DC/DRC. Furthermore, what if the PSE for public services do not have DC/DRC (for instance, using hosting services due to the electronic data is stored only on a small scale), whether all facilities that contained in DC/DRC are required to be located in Indonesia or only some of them that related to the public service data and how the arrangement if located virtually in the cloud service.

According to Sonny Zulhuda from International Islamic University Malaysia stated that Article 26 of Law No. 11 of 2008 which now becomes Article 26 paragraph (1) of Law No. 19 of 2016 is still insignificant in regulating the use of personal data since that Article only contains general provision and does not explain various issues that have been discussed internationally [17]. That Article is not clearly intended for the use of any information whether it includes collection, processing, storage, dissemination and etc. Furthermore, according to Zulhuda, in relation to the consent which the use of data shall be made with the consent of the concerned person which the consent in this case classified as implied consent.

All the regulations have not been set explicitly to mention about privacy and protection of personal data. To provide legal certainty on the privacy of personal data, National Legal Development as a working unit that has duties and functions in the field of the alignment of Academic Draft at the Ministry of Law and Human Rights, conducting alignment of Academic Draft of Bill, in the Bill of Personal Data Protection, ideally arranging the following:

- Protecting and ensuring the basic rights of citizen related to the privacy of personal data.
- Increasing legal awareness in society to make them respect to the right to privacy of everyone.
- Ensuring society to obtain service from government, business actor and other social organization.
- Preventing Indonesia from all kinds of exploitation from other nations towards personal data of Indonesian citizens.
- Increasing the growth of technology, information and communication industries.

6. Conclusion and Recommendation

6.1 Conclusion

International regulations on privacy and personal data can be found in the Universal Declaration on Human Rights 1948 (UDHR), the International Covenant on Civil and Political Rights 1966 (ICCPR), European

Convention on Human Rights 1950 (ECHR), American Convention on Human Rights 1969 and Cairo Declaration on Islamic Human Rights 1990. In the regional context, Malaysia is known for the Personal Data Protection Act. In Indonesia, privacy and personal data protection have not been clearly regulated.

6.2 Recommendation

Government of Indonesia shall immediately establish and enforce regulation on the protection of personal data in order to prevent misuse from irresponsible parties including *Cloud Computing* service providers, third parties or even government. Also, the internal mechanism that must be conducted by data collectors and action after the violation occurs. In addition, the existence of the regulation on personal data protection is expected to encourage the development of *Cloud Computing* in Indonesia.

Reference

[1] Muhammad Tahir Azhary. Negara Hukum. Jakarta: Pranada Media, 2010.

[2] Diaz Gwijangge. Pemanfaatan Jejaring E-Pendidikan. Makassar: Pusat Teknologi Informasi dan Komunikasi Pendidikan Kementerian Pendidikan Nasional.

[3] Wahyudi Djafar and Asep Komarudin. Perlindungan Hak Atas Privasi di Internet - Beberapa Penjelasan Kunci. Jakarta: Elsam, 2014.

[4] Privacy International Report, 2013.

[5] Azure Price, Internet https://azure.microsoft.com/en-us/pricing/calculator [Des. 11, 2017].

[6] Adam Rizal. “Password Akun 500 Juta Pengguna Yahoo Dibobol Peretas, Internet https://infokomputer.grid.id/2016/09/berita/berita-reguler/password-500-juta-pengguna-yahoo-dibobol-peretas/, Sep. 23, 2016 [Aug. 11, 2017].

[7] Bahder Johan Nasution. Metode Penelitian Hukum. Bandung: Mandar Maju, 2008.

[8] Makarim, E. Pengaturan Hukum Telematika (Suatu Kompilasi Kajian). Jakarta: Raja Grafindo, 2003.

[9] Alan F. Westin. Privacy and Freedom. New York: Antheneum Press. 1967.

[10] Abu Bakar Munir. The Malaysian Personal Data Protection Bill, Internet http://profabm.blogspot.com/2009/12/malaysian-personal-data-protection-bill.html, Dec. 4, 2009 [Nov. 30, 2017].

[11] Graham Greenleaf. ” Privacy Laws & Business International Report.” Global data privacy laws: Special Report – Forty years of acceleration, vol. 112, pp. 11-17, Sep. 2011.

[12] Graham, G. Asian Data Privacy Laws – Trade and Human Rights Perspectives. New York: Oxford University Press, 2014.

[13] Section 3 Personal Data Protection Act (PDPA) Malaysia, 2011.

[14] Section 3 Personal Data Protection Act (PDPA) Malaysia, 2013.

[15] Section 6 Personal Data Protection Act (PDPA) Malaysia, 2013.

[16] Section 40 Personal Data Protection Act (PDPA) Malaysia, 2013.

[17] Sonny Zulhuda, Data Privacy in Indonesia-Quo Vadis, Internet: https://sonnyzulhuda.com/2011/01/25/adakah-perlindungan-data-konsumen-di-indonesia, Jan. 24, 2011[Nov. 29, 2017]