JAMBURA LAW REVIEW

Volume 3 Issue 02
JALREV 3 (2) 2021

July 2021
ISSN Print: 2654-9266
ISSN Online: 2656-0461

Regulation and Protection of Cloud Computing: Literature Review Perspective

Maskun1[1]
Rian Nugraha Anwar [2]

[1] Faculty of Law, Universitas Hasanuddin, Indonesia. E-mail: maskunmaskun31@gmail.com
[2] Faculty of Law, Universitas Hasanuddin, Indonesia.

Article Info

Keywords:
Cloud Computing; Regulation and Protection.

How to cite ***(APA Citation Style)****:*
Maskun & Anwar, R. N. (2021). "Regulation and Protection of Cloud Computing: Literature Review Perspective". *Jambura Law Review*. JALREV 3 (2): 336-364

Abstract

Cloud computing is one of the developments of the internet of things. It can say that it is a new industry in era revolution 4.0. particular to store data, including customer data privacy. The research aims to determine some regulations and protection of cloud computing at either international or national levels. The research methods are normative legal research which applies some regulations both international and national legal instruments. The research results show that some international instruments can be seen in general and specific international instruments. The general instruments are such as the Universal Declaration of Human Rights 1948 (UDHR) and International Covenant on Civil and Political Rights 1996; the specific instruments are such as OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980, Council of Europe Convention for the Protection of Individuals concerning the Processing of Personal Data, 1981, and United Nation General Assembly Resolution on the Right of Privacy in the Digital Age, 2014. In the Indonesian context, the regulation of it can be seen such as The Law No. 39 of 1999 Concerning Human Rights, The Law No. 14 of 2008 Concerning Public Information Disclosure, The Law No. 36 of 2009 Concerning Health, the Law No. 19 of 2016 concerning amendment of the Law No. 11 of 2008 concerning Information and Electronic Transaction and other sectoral regulation. Therefore, it can conclude that the need for regulation of cloud computing and its protection is needed to guarantee that those data are protected.

1. Introduction

Personal data protection is related to the privacy concept, which protects personal integrity and dignity.[1] In this case, everyone can determine who will hold their information and how it will use it.[2] The concept of data protection indicates that every person has the right to determine whether they will share or pass their data or not. A person has a right to decide the terms of data transferring implementation. Furthermore, it is also related to the privacy rights concept, which defines the right to protect personal data.[3] In this context, the right of privacy through data protection is a crucial element for the freedom and dignity of the individual, pushing to realize the freedom of politics, spirituality, religion, and even sexual activity. The right to determine its fate, freedom of speech, and privacy are fundamental to making us human.

Cloud computing is one place to store personal data and information via the internet. People use cloud computing services to store their data, particularly customer privacy data. Indeed, the usability and utilization of cloud computing systems require payment. According to the customer's need, Microsoft with Microsoft Azure sets $360 (three hundred and sixty dollars) per month for essential storage with 6 Terabytes of storage. BIZnet Indonesia, with its Gio Public Cloud, set 1,4 million rupiahs for a capacity of 500 Gigabytes per month.[4] Furthermore, the data entered the server will be managed and maintained by the cloud computing service provider.

It can be said that all data in cloud computing systems are safe and easy to access and retrieve worldwide. However, one of the cloud computing issues is security matters, especially the possibility of the data being hacked or misused by a third party. One of the cases was the Yahoo data breach, which announced that as many as 1 billion of their user accounts had been hacked by unknown parties in August 2013, reported on September 2016. The stolen account information included e-mail, phone number,

---

[1] Djafar, W & Komarudin, A. (2014). Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci. Jakarta: ELSAM. p. 2

[2] *Ibid. p.6*

[3] Human Rights Committee General Comment No.16. 1998. *The right to respect privacy, family, home and correspondence, and protection of honour and reputation.* Art. 17. As quoted in Privacy International Report. 2013. p. 1-2

[4] Microsoft. (ed. April 10, 2017). Microsoft Azure Pricing Calculator. Microsoft Azure Pricing Calculator. Retrieved from https://azure.microsoft.com/en-us/pricing/calculator. accessed December 11 2019.

date of birth, random password, and on several cases including encrypted or non-encrypted security questions and answers.[5]

The 2 cases show the importance of giving equal protection to personal data, especially in providing proper regulation to govern it. The possibility of data theft has often happened in the state's practices. In a broad sense, it is very likely to disrupt stability and sovereignty, damage public infrastructure, and cause material and non-material losses. Its negative side is in line with the number of internet users reaching 3.5 billion people, equal to 51.2% of the world's population, as published by the International Telecommunication Union (ITU).[6] It means that the more people use the internet, the more vulnerable they will be.

Therefore, the Article will focus on the governing of cloud computing because, in some practices, some countries do have their specific regulation on it. Currently, no particular laws regulate personal data protection in Indonesia, including data storing in cloud computing.

2. Problem Statement

Based on the analysis and description of the problem, this research will describe the governing for a law on data protection and privacy both in international dan national laws because the breach of data protection increases every year and is in line with the internet user's data.

3. Methods

This research is a normative study, which applies a statute approach to show the necessity of cloud computing regulation and protection. This research used a comprehensive study on several international and national rules, and it will be analyzed qualitatively.

[5]Info Komputer. (ed. August 10, 2017). Pembobolan Data. Retrieved from https://infokomputer.grid.id/tag/pembobolan-data/ on August 10 2017. accessed August 10, 2019

[6] International Telecommunication Union. (ed. October 18, 2020). Global security, Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. accessed April 30 2021

4. Discussion

4.1. Cloud Computing and Consumer Data Privacy: Regulation and Protection

A. Privacy and Personal Data Regulation on Cloud Computing Systems

Privacy and data protection regulation on the cloud computing systems are regulated on Service Contract Agreement and applied by Microsoft Azure and BIZNET Indonesia. It has always been a negotiation object between a service provider and user, the responsibility and liability, data integrity, data center, and restoration, service level, security, privacy and personal data protection, lock-in and exit, the right to terminate the contract and access to data contracts/service ends, unilateral changes clause, and intellectual property rights.

On the Microsoft Cloud Computing services, the user data are protected using the latest technology such as virtualization, partition, firewall, Information Rights Management, encryption and Data Center design which are spread to increasing availability. This day, Microsoft Cloud Computing Services has gained FISMA Certification (Federal Information Security Management Act) and ISO 27001:2005.[7]

In that agreement, the parties who control the user data on the Microsoft service are divided into two kinds of parties that are differentiated by user option. First are Microsoft, and second are retailers or partners in Indonesia such as PT. Telekomunikasi Indonesia and PT. Infinys System Indonesia. If the user chooses retail, the server will automatically place on Indonesia, while if the user decides Microsoft, then the access to the data controller will be on Microsoft. [8]

---

[7] Microsoft Online Privacy Statement. (ed. August 17, 2017) Retrieved from http://privamicrosoft.com/en-us/fullnotice. Accessed November 30, 2019. ISO 27001 is a management system standard published by ISO (International Organization for Standardization) collaborated with IEC (International Electrotechnical Commission) focused on security systems. This standard used a management approach based on the risk analysis. So far, this standard has been widely used throughout the world and is a management solution for information security. This standard is widely applied, especially for companies/organizations that think that information is a company asset that must protect. In Indonesia, it is estimated that there are around 40 organizations that have successfully implemented and certified ISO 27001.

[8] See Section 4 of the Microsoft Cloud Agreement, which reads that customer understands and agrees that (i) after the customer selects a Reseller, that Reseller will be the primary administrator of the Online Services during the Term and will have administrative privileges and access to Customer Data, however, you may request Additional administrator privileges of the Reseller; (ii) Customer may, at its sole discretion and at any time during the Term, terminate Reseller administrative privileges; (iii) Reseller privacy practices concerning Customer Data or any services provided by a Reseller are subject to the terms of customer's agreement with its Resellers and may differ from

The law governing the Microsoft Cloud Agreement is the Washington Act. Point (ii) of the Act states that disputes amongst customers coming from Bangladesh, Cambodia, India, Indonesia, Macau, China, Sri Lanka, Thailand, Philippines, or Vietnam should be referred to and resolved by arbitration in Singapore under the Singapore International Arbitration Center Arbitration (SIAC). As far as the fullest extent permitted by the applicable law, all parties waive their rights to appeal or challenge the same form of appeal to a court of law. For this agreement only, the People of the Republic of China does not cover Hong Kong SAR, Macau SAR, and Taiwan, as stated in the Article 9 Letter (j).[9]

This agreement is governed by Washington Act, without regard to any conflict with general law principles. Subject to sections (i) and (ii), if Microsoft wishes to bring a claim to enforce this agreement, Microsoft must do so in the jurisdiction of the Customers headquarter. If the customer wishes to file a lawsuit to enforce this agreement, the customer must file with Washington, USA. This choice of jurisdiction does not prevent both parties from seeking waiver of court decisions relating to intellectual property rights infringement.

Furthermore, the cloud computing agreement offered by BIZNET Indonesia is almost the same as Microsoft Azure, which governs the rights and obligations of both parties

---

Microsoft's privacy practices; and (iv) Retailers may collect, use, transfer, disclose and or process Customer Data, including personal data. Customer agrees that Microsoft will provide Customer Data to Resellers and information that the customer provides to Microsoft to order, procure, and administer the Online Services.

a. The customer permits the processing of personal information by Microsoft and its agents to facilitate the subject matter of this agreement. Customers may choose to provide personal information to Microsoft on behalf of third parties (including contacts, retailers, distributors, administrators and employees) as part of this agreement. Before providing personal information to Microsoft, customers will obtain all necessary consents from third parties under applicable privacy and data protection laws.
b. Additional security and privacy details can be found in the Online Terms of Service. The commitment made in the Online Service Terms applies only to the Online Services purchased under this agreement and not to any services or products provided by the Reseller.
c. According to the law, the customer must notify individual users of the Online Services that may process their data for disclosure purposes to law enforcement or other government authorities as directed by the Reseller or as required by law. The customer must get user permission for it.
d. Customer appoints Reseller as its agent to interact with and provides instructions to Microsoft for this Part 4. The customer can terminate the data access provided to the retailer so that the data on the service is then managed and controlled by the customer so that if there is an error, data leakage or misuse caused by a mistake or negligence from the customer, it becomes the responsibility of the respective customer

[9] Ibid.

as listed in Article 5 of the BIZNET Indonesia Cloud agreement:[10]

1. The customer must provide the hardware needed; hence, it could activate the facility and the service by BIZNET under the scheduled agreement.
2. Customers are not allowed to give a chance to third parties to utilize the facility and service of BIZNET without written permission from BIZNET.
3. Customers are not allowed to change the technical specification, configuration, and BIZNET service facility, including connecting to the BIZNET network in any way, except with written permission from BIZNET.
4. Customers are not allowed to connect the network or BIZNET facility with a public telecommunication network (PSTN), including but not limited to the telephone network, fax, or data communication.
5. The customer will permit BIZNET or its representative to enter the customer facility or location related to maintenance and repair needs with prior written notification.
6. BIZNET is responsible for the maintenance and repair of damage or interference to BIZNET channels and facilities. If the damage or interference is caused by a customer mistake, intentional, or negligence, then BIZNET has the right to charge a repair fee.
7. The customer is entitled to get restitution for damage or interference which is proven not caused by the customer. The compensation will be given by the applicable provisions (Service Legal Agreement – SLA) and does not apply to damage or interference induced by Customer equipment or Force Majeure.
8. BIZNET is not responsible for the accuracy, confidentiality, or quality of the information transmitted through BIZNET services.
9. BIZNET is not responsible for the losses of Customers or third parties related to the BIZNET service users.

However, the Microsoft Azure Cloud Agreement do not present restitution as seen in Article 5 Number (7) of the BIZNET Indonesia Agreement. It is essential because it is

[10] Biznet Order Form Dedicated – Confidential Information.

part of the responsibility of the cloud service provider if interference happens and is done by the provider, which can be harmful to the customer, which is regulated on Article 7 of the BIZNET Indonesia Cloud Agreement:[11]

1. Guarantee of unavailability of BIZNET Services covering the entire BIZNET Owned Network Including electricity, HVAC system, Cable System, including related facilities, the minimum service availability is 99.8% (ninety-nine point eight per cent) (excluding maintenance schedule)
2. The customer is entitled to get a replacement of up to 30% (thirty per cent) of the total bill in a month if BIZNET does not reach the promised Service Guarantee (excluding the maintenance period)
3. It shall calculate the calculation of restitution as mentioned in paragraph 2 (two) above based on the following analysis:

   Formula (X*Y)/(Z*99.8%)

   Explanation: X = Monthly fee before VAT

   Y = Total times of broken link (hours)

   Z = time that should receive in one month (hours)

   99.8% = BIZNET Service Guarantee Level.
4. Restitution can only be given if the submission is made no later than 3 (three) months after the interference occurs; if the application is made outside the time limit, the refund cannot be granted.

On several service agreement, cloud computing provider might have other option (and might be a need) to use third party provider or fourth party in order to fulfilling request of cloud computing resource:[12]

1. In the context of patent law, distribution to a third party of confidential information related to the invention through cloud computing raises at least a theoretical problem. The distribution through the cloud is in the form of public

[11] Ibid

[12] Nugraha, R.A. 2012. Skripsi: "Analisis Yuridis Mengenai Perlindungan Data Dalam Cloud Computing System Ditijau Dari Undang-Undang Informasi dan Transaksi Elektronik". Fakultas Hukum Universitas Indonesia. p.72

knowledge.

2. In the context of trademark, there appear a growing number of trademarks incorporating cloud computing. The terms of cloud computing were first proposed as a brand in 1997 but then eventually abandoned.
3. The owner of Trade Secret must have taken all reasonable action to protect the information from being disclosed to obtain this trade secret. This requirement is essential in business when storing data in cloud computing. The question that arises then is how does cloud computing service providers protect those trade secrets? At the American Bar Association meeting, Sharon Sandeen, a Hamline University law professor,[13] Discussed cloud computing services providers such as IBM, Microsoft, Google, Amazon, Dell, and Verizon refuse to be held accountable for security. They are reluctant to negotiate specific terms that become evidence of confidentiality obligation for trade secret purposes. If the confidentiality obligation does not exist, then the businessman might ignore the trade personal protection. Companies and business people should learn everything about cloud computing service providers before giving confidential business information to the service providers.
4. In the context of copyright, cloud computing could create a legal problem in the field of data stored in the "cloud", such as computer programs. In a cloud computing environment, data and information can be separated and copied in several locations.

A good Self Contract Agreement for both parties must pay attention to several aspects. The first aspect is to determine the responsibilities and clearly explain the parties responsible in the different scenarios. It is based on the identification of who will be blamed if data loss or data theft happens. In this case, the allocation of responsibility on a particular scale allows for a greater degree of accuracy and recognition that, in some cases, can be a two-way case. On the contract side of every agreement about Cloud Service must also see how the company can retrieve the information and application when the contract expires and will not be extended.

[13] Sharon Sandeen. 2014. Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection. *Virginia Journal of Law and Technology*, (19). p.18.

The second aspect is a notice provided by the cloud provider, which has to be handled differently. It is based on the characteristics of the industry or the sector where the client is operating. For this reason, it needed to eliminate the confusion in the process of contract drafting to ensure that both parties are satisfied. From the user of the cloud side, things such as data recovery if a disaster is happened to ensure business continuity might be crucial. The provider must describe how long it takes for them to perform data and application recovery. The application will be slightly interrupted or even outage to the cloud system itself. The third aspects are individual data protection and privacy. The management of cloud access and the data stored in it will be the central factor that shows trust to the provider who is given trust.

B. The Governing of Cloud Computing Users for Privacy and Personal Data

The legal protection on cloud computing has been regulated in several international and national laws about the data protection principle.[14] Data protection is a fundamental human right. Several states had recognized data protection as a constitutional right or in the form of *'habeas data'*, which is people right to gain protection on their data and for justification when a mistake was found in their data. Albania, Armenia, the Philippines, East Timor, Columbia, and Argentina are a state with different histories and cultures that already recognize data protection, facilitating a democratic process and guaranteeing the protection of their constitution. ASEAN Human Rights Declaration adopted by ASEAN countries acknowledge the right of privacy of personal data on Article 21. Today, many states, around 120 states, have their laws on data protection.[15]

1. International Instruments

The concept of protecting user privacy and data with several internationally recognized international instruments has laid the legal basis for modern national data protection. Some of these instruments were developed with specific data privacy

[14] See *the Council of Europe Convention for the Protection of Individuals concerning Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72).*

[15] Greenleaf, G. 2011. 76 Global Data Protection Laws. Privacy Laws & Business Special Report.

regulations and other instruments governing general regulations to cover several issues, including privacy. Those instruments are:

a. Universal Declaration of Human Rights 1948 (UDHR)

UDHR is the first international instrument that protects person privacy rights, which is regulated 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 means that everyone must receive legal protection because they have the right not to be disturbed by their Privacy, family, place of residence, correspondence, or honour and reputation. Article 12 of UDHR is considered the first instrument to govern privacy matters such as family, residence, correspondence, and honour and dignity.[16] Substantively, the regulation on Privacy in Article 12 of UDHR gives broad protection because it covers about:

1. Physical Privacy

It is privacy protection-related to the place of residence. For example, a person cannot enter other people residences without permission from the owner, a state cannot rummage a person's house without a warrant, and a state cannot tap a person's house.

2. Decisional Privacy

It is privacy protection on the right to decide its own life, including its family. For example, they have a right to decide their own life and how to educate their child.

3. Dignity

It is protecting a person dignity, including their reputation.

4. Informational Privacy

[16] Eide, A. Gudmundur, A. et. al. (1992). The Universal Declaration of Human Rights: A Commentary. Oslo. p. 188-214.

It is privacy on information, which means a person's right to decide how they store their private data.[17]

b. International Covenant on Civil and Political Rights (ICCPR)1996

"1. 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.

2. Everyone has the right to the protection of the law against such interference or attacks."

The regulation of privacy in Article 17 adds the Arbitrary or Unlawful word or against the law. Hence, the countries are given responsibilities to protect their people with regulation and forbid privacy violations.[18] As known on the UDHR, on the ICCPR, the scope of the privacy regulation are:

1. The privacy protection on family and home. According to the commission from several delegates, the home's terms are a daily place to live or a place to do a job. At the same time, the terms of the family are interpreted broadly because there is no limit on the socialization between husband and wife but also related to the relation between children and parents.
2. Privacy protection of the way someone does correspondence. Privacy also protects the confidentiality of a person in correspondence whether by letter, telephone, e-mail, or other means so that other parties (state, private party, individual) are not allowed to open the letter, conduct interception through electronic, wiretapping without any justified reason by law.
3. The government conduct privacy protection on the citizen. A search on a person should be done according to the laws and regulations without violence and disrespecting a person's dignity.
4. Protection on honour and reputation. The state government should guarantee their people protection toward a reputation and dignity violence from insult or

[17] Freeman M. & Ert, G. V. (2004). International Human Rights Law. Canada. p. 70
[18] Jayawickrama, N. (2002). The Judicial Application of Human Rights Law, National, Regional, and International Jurisprudence. United Kingdom: Cambridge University Press. p. 599

disclosure of a person in mass media, damaging their reputation and dignity.

5. Protection of personal information. The influence of technological advances has caused a person private data can be accessed by others easily. Therefore ICCPR also protects a person from this kind of violation.[19]

The regulation of privacy in Article 17 of ICCPR includes a comprehensive arrangement for various privacy violations. According to Bygrave, this regulation is the most substantial legal basis in international law, and the state must protect privacy over data privacy through laws and regulation.[20]

c. European Convention on Human Rights 1950

Article 8 of ECHR stated that:

"*Everyone has the right to respect for his private and family life, his home and his correspondence*."[21]

Those rights are interpreted widely with neutral technology, so it applies to the electronic market and online environment. The European Court of Human Rights emphasized that Article 8 regulates the importance of data privacy, and article 8 consists of 2 Paragraphs. Article 8 Paragraph (1) handles four types of privacy violations (ECHR did not use privacy terms, but using private life, which is a violation of the personal life, family, home, and correspondence. The European Commission is not trying to define the terms of private life more because the interpretation will continuously evolve through time.

d. American Convention on Human Rights 1969

Article 11 of the American Convention on Human Rights 1969 stated that:

1. *Everyone has the right to have his honour respected and his dignity recognized, and his grace recognized. 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.*

[19] Ibid.

[20] Bygrave. LA (1998). Data Protection Under The Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology*, (6). p.4

[21] European Convention for the Protection of Human Rights, November 4, 1950, ETS 5, Retrieved from *http:conventions.coe.int/treaty/en/Html.005.htm*. accessed December 11 2019.

2. *Everyone has the right to protection of the law again such interference or attacks.*

On American Convention on Human Rights, it is almost the same as other international and regional instruments. The difference was in Paragraph 1, which include privacy protection as dignity.

e. Cairo Declaration on Islamic Human Rights 1990

Article 18 (b) and (c) of Cairo Declaration on Islamic Human Rights 1990 stated that:

"*Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, about 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 on the Cairo Declaration is broader than other international laws, including personal rights, place, family, property, the relation between others, and dignity. Africa also has its regional instrument, its African Charter on Human and People's Rights 1981, but it does not regulate privacy and regional instrument protection. It is the only regional instrument that is not handling privacy concerns.[22]

The protection of international law against privacy in effect in 1967 stated that at the International Conference on Privacy in Stockholm, Sweden, which was initiated by International Law Commission had made a recommendation, namely:[23]

1. Privacy included into fundamental of human right which protects a person from other party action that might be harmful (government or other individuals);
2. Privacy is a right to be alone and right to be not disturbed by others, which consist of:

[22] Bygrave. LA Op.Cit. p.21
[23] Ibid.

a. Personal life, family life and life in the neighbourhood where he lived are not disturbed;
b. Not disturbed by their physical and mental integrity or moral and intellectual freedom;
c. His honour and reputation are not compromised;
d. Not disturbed by disclosing personal things;
e. Not disturbed by being spied on all activities;
f. Freedom of correspondence with anyone is not disturbed; and
g. Privacy has to be limited by balancing between privacy and other personal rights, also limited by the interest of the public, national security, and economic interest of each country, to avoid criminal activity, protect public health and morals.

The protection of privacy is also regulated in special instruments to protect personal data, such as:

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

Most data protection regimes are inspired by OECD's 1980 concerning Privacy Guidelines. These guidelines apply to all personal data identified as information related to the individual and identifiable. These guidelines are not legally binding but have been long recognized as a statement from the norms that established personal data privacy and directed the OECD members and private organizations to make their policies.

These guidelines support the personal data collection that is obtained legally and following the law. The data is accurate, updated, and relevant, also needed for data collecting purposes. Personal data must be protected with appropriate security. They may not be disclosed or available for the public for any purpose other than the original reason the data was collected unless with the consent of the owner of the collected data or from a legal authority.

These guidelines explain that the principle below must be done when managing personal data, namely:[24]

1. Limitation of Collecting

   There must be a limitation on data collecting. Privacy data must be obtained using a lawful, fair, and known with the data subject's consent.

2. Data Quality

   Privacy data should align with the original purposes of data collection, accurate, complete, and updated.

3. Purposes of Specification

   The purpose of data collection should be specific, and subsequent use of the data must be limited to the objectives.

4. Limitation of Restrictions

   The data cannot be opened, disclosed, available to the public or used for a purpose outside of the specific purpose, except with the consent of the owner of the data or consent from the legal authority.

5. Security Measures

   The stored data must have adequate security to be protected from loss, damage, uses, alteration or unauthorized disclosure.

6. Openness

   There should be a general policy about data management that is open to the public related to private data management.

7. Individual Participation

   Individuals must have a right to gain information about their private data, including the right to erase and correct their inaccurate data.

8. Responsibilities

   The data managers are responsible for managing private data under the private

[24] Ibid.

data management principle.

Many multinational companies adhere to data protection principles as a form of assurance of minimum compliance in a jurisdiction where the data protection is not strictly regulated or event not regulated completely. Even though it is considered a foundation, unfortunately, those principles are not strong enough because it is self-regulation and does not provide a practical solution for law enforcers for states that violate them. Without a check and balances system that guarantees adherence to these principles, personal data protection is often only enshrined in the contract law. In this area, general people are rarely sued.

European Union members and European Commission has pushed to revise OECD Privacy Guidelines immediately. The revision will bring the guidelines near the European Union Data Protection standard and fill the void on the areas concerning data privacy transfer. The OECD Working Party currently reviews privacy guidelines on Information Security and Privacy (WPISP).[25]

As the first step of the review, the member of OECD has accepted the Terms of Reference as the roadmap. As listed on the terms of reference, WPISP has called the stakeholders, expert groups from the government, privacy enforcement authority, academics, business people, community organizations, and the internet user community. The expert group chaired by Jennifer Stoddart, which are the Privacy Commissioner from Canada and has been discussed several themes, such as:[26]

1. Role and responsibilities of the key actor;
2. Geographic limitation on the flow of information that crossed the national border;
3. Proactive implementation and enforcement measures.

The expert group made a recommendation as a consideration for the members of OECD in November 2012, where the recommendation is now considered. Those recommendation covers:

1. Introduction to the concept of privacy management which all data managers should maintain as all data privacy is under their control. This introduction is

[25] Ibid.
[26] Ibid.

intended not only for managing the data but also for all forms of operation that allow these data managers to be responsible.

2. Conditions that the data controller must notify the authority when there is a security breach involving the private data and notify the person concerned when a security breach happened and could endanger them.
3. Clear definition and requirements regarding privacy enforcement authorities.
4. Updating concepts and regulations regarding the flow of information across a national border.

b. Council of Europe Convention for the Protection of Individuals concerning the Processing of Personal Data, 1981

The Council of Europe Convention 1981 is an instrument that is legally binding for the first time in data protection. This convention requires the parties to take the necessary step in the domestic laws and regulations of their country to apply the principle to ensure respect for the fundamental rights of all individuals regarding the management of data privacy in their territories. The data quality must be sufficient, relevant, and not excessive (proportional), accurate, confidential, contains information from the data subject and provide a right to access and revision.

This convention grants freedom to the flow of data privacy between state parties. This flow of freedom does not hinder the protection of data privacy unless the reason of the party deviates from this provision, which can be done in two specific cases, the protection of data privacy, on the other hand, is not balanced or the data is transferred to the third country which is not a party to the convention. Council of Europe has adopted the European Convention for the Protection of Human Rights (ECHR) in 1950. Article 8 of ECHR stated that:[27]

"*Everyone has the right to respect for his private and family life, his home and his correspondence*."

Those rights are interpreted widely and with the terms of neutral technology to apply for the electronic market and online environment. The European Court of Human

[27] European Convention for the Protection of Human Rights, Loc. Cit.

Rights cases emphasized that article 8 about the importance of data privacy protection. For example, in the case of MS v. Sweden, ECHR stated that data privacy protection, especially medical data, is vital for people to enjoy their rights, especially regarding respect for private life and family, as it is guaranteed in Article 8.[28] In the case of Malone v. the United Kingdom, ECHR explained that Article 8 is not just covering a telephone conversation but also the flow of information such as telephone numbers.[29]

As technology rapidly evolved and the introduction of electronic storage facilities, the Council of Europe feels that ECHR need to be supported by more modern and more detailed laws to address the collection and processing of private data, which is considered unfair. As a result, in 1981, the Council of Europe adopted a convention for the Protection of Individuals concerning Automatic Processing of Personal Data, hereinafter known as PD Convention.[30] This convention applies to the automatic processing of data privacy both in the private and public sectors. Private data means the information relating to the individual identified (data owner).

Apart from the broad applicability of the PD Convention, which covers all types of the data regulations or users, including natural persons or companies, public authorities, agencies or authorized institutions to determine the purpose of the private data, there are many ways to distinguish from the rules for data collection that is not automatically processed and data related to an agency such as organization. Furthermore, states may reduce their obligations for the fair and lawful process of data by prohibiting automatic processing of special categories of data that reveal race, political opinion, belief and religion, health and sexual life and the existence of additional safeguards (Article 5, 6, and 8). This is permissible when the reduction of this obligation is based on the national law and considered as a step in a democratic country that is needed to protect state security, public security, the financial interest of the state or prevent criminal acts, protection of the data owner or the right and freedom of other people.

[28] Ibid.
[29] MS v. Sweden. 1997. Reports 1997-IV.
[30] Convention for the Protection of Individuals concerning Automatic Processing of Personal Data of January 28 1981, Retrieved from http://*convention.coe.int/treaty/EN/Treaties/HTML/108.*htm. accessed December 11 2019.

"*Provided for by national law and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; protecting the data subject or the rights and freedoms of other.*"

In responding to the criticism on a legal vacuum, PD Convention is equipped with the additional protocol 2001 Concerning supervisory authorities and transborder data flow across the national border.[31] In March 2010, CoE then started to modernize PD Convention to deal with the new challenge on privacy due to the usage of new information and technology and communication and strengthening the convention's continuation mechanism.[32] Then public consultation was launched in 2011.

PD Convention so far has been replaced with European Union Data Protection Directive 2016. For many European Union Members, this directive is the new instrument even though the PD Convention is still an essential convention for many states unrelated to national regulation to protect privacy. As of today, there are many movements to invite non-European states to access the PD Convention.

c. United Nation General Assembly Resolution on the Right of Privacy in the Digital Age, 2014

On November 25 2014, The Third Committee of the United Nations General Assembly adopted a resolution that invited the states to respect and protect the right of privacy in the digital era. This resolution responds to a movement started by Germany and Brazil related to the Edward Snowden case. Germany and Brazil successfully pushed the adoption of this resolution supported by more than 30 countries, including Indonesia. The resolution adopted is about The Right to Privacy in the Digital Age.

Before, on November 2013, Germany and Brazil proposed a draft of resolution regarding on:[33]

---

[31] Additional Protocol to the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. Available on https://rm.coe.int/1680080626 accessed December 11 2019.

[32] CEO Response to Privacy Challenges, Modernization of Convention 108. Retrieved from http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/CoE_response_to_privacy_challenges_modernisation_of_convention_108_EN_May_2011.pdf. accessed on December 11 2017.

[33] United Nations General Assembly. (2013). Brazil and German: Draft Resolution.

1. The goal and principle of the United Nations Charter;
2. Human rights and fundamental freedom which written on Universal Declaration of Human Rights and relevant international human rights treaties, including International Covenant on Civil and Political Rights and International Covenant on Economic Social and Culture Rights;
3. The technology development enables individuals around the world to use the new information and communication technologies and at the same time increase the capacity of governments, companies and individuals to carry out surveillances, interceptions, and data collections which may violate human rights, especially rights on privacy as regulated on the Article 12 of Universal Declaration of Human Rights and Article 17 of International Covenant on Civil and Political Rights, and therefore an issue of increasing concern;
4. That there are human rights in the absence of arbitrary or unlawful interference with privacy, family, home, or correspondence, and there is a right to legal protection against such interference, and recognize that protection of the right to privacy is vital for the realization of the right to freedom of expression and to express opinions without disturbance and one of the foundations of a democratic society;
5. Whereas the full respect on the freedom to seek, receive and deliver information, including the importance of accessing information and democratic participation is essential;
6. That unlawful or arbitrary surveillance and communication interception as well as an illegal or arbitrary collection of private data, as a highly intrusive act, violates the rights to privacy and freedom of expression and might be contrary to the principles of a democratic society;
7. Although concern about public security might justify the collection and protection of certain sensitive information, the state should ensure full compliance with their obligations under the international human rights law;
8. There is a concern about the negative impact resulting from the surveillance and interception of communication, including extraterritorial surveillance and

interception of extraterritorial communication, as well as collecting privacy data, especially when done on a mass scale, might be affecting human rights;

9. That states must ensure every action taken to combat terrorism under their obligations under the international law, particularly international human rights, refugees, and humanitarian law.

German and Brazil proposal finally adopted by The Third Committee of United Nations General Assembly in 2014 and decided several things such as:[34]

1. Reaffirming the Right to Privacy, no one can intervene arbitrarily or illegally against privacy, family, home, or correspondence. Whereas there is a right to legal protection against such acts, as stated in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights;
2. Recognize the global and open feature of the internet and the rapid advance in information and communication technology to accelerate the development in any form;
3. Emphasize that the same right which enjoyed offline must also be protected online, including the right to privacy;
4. Call out all the countries;
    a. To respect and protect the right to privacy, including in the context of digital communications;
    b. To take steps to end the violation of rights and create conditions to prevent such violations, including ensuring that relevant national law complies with their obligations under international human rights law.
    c. To review the procedure, practices and laws regarding the surveillance of communications, interceptions, and collecting of privacy data, including mass surveillance, interception and collecting them, with the intention to upholding the right privacy by ensuring the full and effective implementation of all their obligations under international human rights law.

[34] United Nations General Assembly. (2014). General Assembly Document No. A/C.3/69/L.26/Rev. 1

d. To establish or maintain an effective independent mechanism on domestic surveillance that can ensure transparency, suitable, and accountability for states surveillance on communication, interceptions and collecting privacy data;

e. To provide individuals whose rights to privacy have already been violated by illegal or arbitrary tapping/supervision by giving an adequate compensation, consistent with international human rights obligations;

f. Encourage the human rights council to identify and clarify principles, standards, and best practices regarding the promotion and protection of privacy rights.

2. National Instruments

The development of the use of cloud computing raises the potential for a severe violation. An example of the violations is the breach of iCloud user data (a cloud computing provided by apple), which spreads in several mass media. This case received much public attention because the data owners are famous Hollywood celebrities such as Jennifer Lawrence, Jenny McCarthy, Rihanna, Kate Upton, Mary Elizabeth Winstead, Kristen Dunst, Ariana Grande, and Victoria Justice.[35] A large number of iCloud users can multiply considering the Apple users this day around the world, including Indonesia. The current potential for privacy violence in the field of cloud computing is enormous. The amount of data stored in the 'cloud' on the network, including its relatively new development, is increased. When personal data is transmitted to the internet, the risk arises because individuals lose control over data. Once the data is stored in the cloud, other risk arises from the cloud service provider because the cloud provider can move information or data from one jurisdiction to another, or from one operator to another, or from one machine to another, without any notification to the owner of the data.[36]

[35] Merdeka FM. (ed. August 17, 2017) Retrieved from http://www.merdekafm.com/posting/read/17/iCloud_Dibobol_Ratusan_Foto_Pribadi_Celebs_Di_Expos. accessed on November 29 2019.
[36] Djafar. W. & Komarudin. A. Op. Cit.

Relating to privacy and data protection, Indonesia could ratify international law instrument which applies on a national scale. Indonesia has signed Organization for Economic Cooperation and Development (OECD) on privacy and personal data regulation in 2004. As a member of Asia-Pacific Economic Cooperation(APEC), Indonesia also following APEC Privacy Framework 2004, which is clearly stated in the introduction:

"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 in safe, secure and reliable communication, information and delivery system, and which address issues including privacy…."

This membership pushes the national legislation of each member states to identify the privacy protection for the balance and promote adequate information to promote economic cooperation, especially on the electronic market between members. Indonesia is included in the 35 (thirty-five) countries, which pushes to adopt the Resolution of United Nation General Assembly on Privacy Right on Digital Age which pushed by Germany and Brazil. Indonesia has made several laws and regulations which regulate privacy in several fields such as:

1) The Law No. 2 of 2014 Concerning Amendment of The Law No. 30 of 2004 Concerning Notary
2) The Law No. 10 of 1998 Concerning Banking
3) The Law No. 35 of 1999 Concerning Telecommunication
4) The Law No. 8 of 1999 Concerning Consumer Protection
5) The Law No. 39 of 1999 Concerning Human Rights
6) The Law No. 23 of 2006 Concerning Population Administration
7) The Law No. 11 of 2008 Concerning Information and Electronic Transaction
8) The Law No. 19 of 2015 Concerning Amendment of The Law No. 11 of 2008 Concerning Information and Electronic Transaction
9) The Law No. 14 of 2008 Concerning Public Information Disclosure

10) The Law No. 36 of 2009 Concerning Health

11) Government Regulations No. 71 of 2019 Concerning Electronic System and Transaction Operation (PP 71/ 2019)

12) President of Republic of Indonesia Decree No. 67 of 2011 Concerning Application of National Identity Card Based on Identity Number

13) Bank of Indonesia Regulation No. 7/6/PBI/2005 concerning Customer Privacy Data.

PP No. 71 of 2019 emphasizes the protection of personal data and information and web page authentication, which is intended to avoid fake web pages or web page fraud. It also focuses on the need for the government to prevent the misuse of electronic information and electronic transactions that harm individuals, society, and the state and the need to prepare facilities and infrastructure related to national cyber security.

The regulation of personal data protection, which specific on the electronic media, is stated in the Article 26 Paragraph (1) of Information and Electronic Transaction Law:

"Unless provided otherwise by Rules, use of any information through electronic media that involves personal data of a person must be made with the consent of the person concerned."

According to Sonny Zulhada from the International Islamic University of Malaysia, Article 26 Paragraph (1) of the Information and Electronic Transaction Act still does not significantly regulate personal data. It is because that Article is only a general requirement and does not explain more issues discussed internationally.[37] The Article is not explaining clearly the meaning of the use of any information, whether it includes collecting, processing, storing, dissemination, or related. Then, according to it, related to the consent where the data usage should be done on the owner of the data consent, whether this Article is classified on implied consent or explicit consent.

[37] Zelda. S. (ed. January 25, 2011). Data Privacy in Indonesia — Quo Vadis?. Retrieved from https://sonnyzulhuda.com/2011/01/25/adakah-perlindungan-data-konsumen-di-indonesia. accessed on November 29 2019.

All laws and regulations above still do not explicitly regulate privacy and personal data protection. To give a legal certainty on privacy and personal data, *Pembinaan Hukum Nasional*, the working unit with duties and functions in the field of Academic Draft on the Ministry of Law and Human Rights, carries out an update on Academic Draft of an Act. On the Academic Draft of Personal Data Protection, ideally regulated about:[38]

a. The objective of the circumstances that will be realized through the regulation of personal data protection are as follows:
    1. The protection and guarantee of fundamental rights of citizens regarding privacy and personal data.
    2. The increasing number of legal awareness on the society to respect others privacy right.
    3. Ensuring the society to get a service from government, business actors, and other social organizations.
    4. The avoidance of the Indonesia Nation from all kinds of exploitation by other nations on the personal data of Indonesian Citizens.
    5. The increasing development of Technology, Information, and Communication industry.

The aim is as the consideration to make the Academic Draft of Personal Data Protection. The aim can be seen in the "Considering" part, which contain the main ideas of philosophical, sociological and juridical thoughts that became the background for the Personal Data Protection act, such as:[39]

1. The protection of personal data is the recognition of fundamental human rights that have been protected under International Law, Regional, and National;
2. The protection of privacy, including personal data, is a direct mandate of the constitution of the Republic of Indonesia.

[38] Academic Draft of Personal Data Protection Act.
[39] Ibid.

3. The protection of personal data is a necessity to protect individual rights in the society related to the collecting, processing, managing, dissemination of personal data;
4. Adequate protection of privacy regarding personal data will give the public trust to provide personal data for the broader interest of the community without being misused of violating their rights.

b. Scope and Direction of the Regulation

The scope and direction from the Draft of this Regulation are to give a limitation on rights and obligation on every action obtained and utilizing every form of personal data both carried out in Indonesia and personal data of Indonesian citizens abroad, whether carried out by individuals or legal entities (Public Institution, Private Institution and Society Organization).

c. Scope and Material

1. General Provisions

Contain academic terms regarding the interpretation and phrases. The limitation of definition and other things on general characteristics that reflect the principle, purposes and objective is contained in the provisions of the regulations. The definitions and limitations of the terms used are:[40]

a. Personal Data

The terms of personal data are every data about a person's life both identified or could be identified individually or combined with other information directly or indirectly through the electronic system or non-electronic. According to PDPL, personal data means name, date of birth, National ID Number, Passport Number, characteristics, fingerprint, marital status, family, educational background, job, medical record, medical treatment, genetics information, sexual life, medical examination, criminal record, contact information, financial condition, social activity and other information which directly or indirectly used to identify a person who still alive.

[40] Ibid

b. Information

As the definition on the Law no. 14 of 2008 Concerning Public Information Disclosure, information is an explanation, statements, ideas and signs that contain values, meaning, messages, both data, facts and explanations that can be seen, heard and read, which are presented in various packages and formats following the development of information and communication technology, electronically and non-electronic.

5. Conclusion

In the digital age, the usage of cloud computing is extensive both in the public sector, private sector, and even society. However, it has some weaknesses. The data leak, in the end, violates the privacy of an individual because the public then knows about this sensitive data. Therefore, international and national instruments governing privacy and personal data number, particularly in the cloud computing system, could be reduced or even stopped.

References

Books

Achmad Ali, (2002), *Menguak Tabir Hukum (Suatu Kajian Filosofis dan Sosiologis*), Jakarta: Tokoh Gunung Agung.

Badan Pembinaan Hukum Nasional. Rancangan Undang-Undang Perlindungan Data Pribadi

BIZNET. BIZNET Order Form Dedicated-Confidential Information.

Council of Europe. (1981). "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108); the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)"

Djafar, Wahyudi & Komarudin, Asep. (2014). "Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci". Jakarta: Elsam.

Eide, Asbjorn, Gudmundur, Alfredsson (et. al). (1992). "The Universal Declaration of Human Rights: A Commentary". Oslo.

Freeman, Marc & Ert, Gibran V. (2004). "International Human Rights Law). Toronto.

Greenleaf, Graham. (2011). "76 Global Data Protection Laws". Privacy Laws & Business Special Report.

Human Rights Committee. (2013). "General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17)" Quoted from Privacy International Report.

Nugraha, Radian A. (2012). *"Analisis Yuridis Mengenai Perlindungan Data Dalam Cloud Computing System Ditinjau Dari Undang- Undang Informasi dan Transaksi Elektronik".* Fakultas Hukum Universitas Indonesia.

Journal Article

Bygrave, Lee A. (1998). "Data Protection Pursuant to The Right to Privacy in Human Rights Treaties". International Journal of Law and Information Technology, 6

Sharon Sandeen. (2014). "Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection". Virginia Journal of Law and Technology, 19

Jayawickrama, Nihal. (2002). "The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence". United Kingdom: Cambridge University Press.

Official Web

Council of European. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. Retrieved from https://rm.coe.int/1680080626 (accessed December 11, 2019)

Council of European. CoE Response to Privacy Challenges, Modernization of Convention 108. Retrieved from http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/CoE_response_to_privacy_challenges_modernisation_of_convention_108_EN_May_2011.pdf (accessed December 11, 2017)

Council of European. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of January 28 1981. Retrieved from http://convention.coe.int/treaty/EN/Treaties/HTML/108.htm (accessed December 11, 2019)

Council of European. European Convention for the Protection of Human Rights, November 4, 1950, ETS 5. Retrieved from http:conventions.coe.int/treaty/en/Html.005.htm (accessed December 11, 2019)

Info Komputer. Pembobolan Data. Retrieved from https://infokomputer.grid.id/tag/pembobolan-data/ (accessed August 10, 2019)

International Telecommunication Union. 2020. Global security, Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed April 30 2021)

Merdeka FM. iCloud Dibobol Ratusan Foto Pribadi Seleb di Expose. Retrieved from http://www.merdekafm.com/posting/read/17/iCloud_Dibobol_Ratusan_Foto_Pribadi_Celebs_Di_Expos (accessed November 28, 2019)

Microsoft. Azure Pricing Calculator. Retrieved from https://azure.microsoft.com/en-us/pricing/calculator/ (accessed December 11, 2019)

Microsoft. Microsoft Online Privacy Statement. Retrieved from http://privamicrosoft.com/en-us/fullnotice (accessed November 30, 2020)

Sonny, Zulhada. (2011). Data Privacy in Indonesia – Quo Vadis?. Retrieved from https://sonnyzulhuda.com/2011/01/25/adakah-perlindungan-data-konsumen-di-indonesia (accessed November 29, 2019)

Laws and Regulations

United Nation. (2013). United Nation General Assembly, Brazil and German: Draft Resolution

United Nation. (2014). United Nation General Assembly Document No. A/C.3/69/L.26/Rev.1