International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 4, August 2019, pp. 3175~3184
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i4.pp3175-3184

Personal data protection and liability of internet service provider: a comparative approach

Ni Ketut Supasti Dharmawan[1], Desak Putu Dewi Kasih[2], Deris Stiawan[3]
[1,2]Faculty of Law, Udayana University, Indonesia
[3]Department of Computer Engineering, Faculty of Computer Science, Universitas Sriwijaya, Indonesia

Article Info

Article history:

Received Jun 10, 2018
Revised Mar 17, 2019
Accepted Mar 21, 2019

Keywords:

Cloud computing
Electronic provider
Liability
Personal data protection
Security attact

ABSTRACT

The users of electronic service provider often suffered losses caused by internet services did not work properly including losses due to leakage of personal data protection stored in cloud computing. The study aims to examine electronic service provider liability upon their failure performing internet services properly and security attacks on cloud computing. This study was normative legal research by examining national and international legal materials. The finding shows that the electronic provider shall be responsible based on right and obligation agreed under the agreement. Related to cloud computing, providing adequate security to avoid security attacks and misuse of private data that caused losses to the users becoming the liability of service provider. Based on the Federal Trade Commission Act, the liability arises on the grounds of deceptive and unfair trade practices. Under the General Data Protection Regulation of the European Union, the liability arises on the basis as the controller then provider liable for compensation for user's suffered damage. In Indonesia, based on the Electronic Information and Transaction Law Amendment, the liability to the owner of personal data whose rights are violated and suffered losses arises due to a failure of ISP protect the data security. For better protection in Indonesia, the protection of big data and clear territorial scope of protection become necessary to consider.

Corresponding Author:

Ni Ketut Supasti Dharmawan,
Faculty of Law,
Udayana University,
Pulau Bali Street, No.1, Kota Denpasar, Bali 80114, Indonesia.
Email: supasti_dharmawan@unud.ac.id

1. INTRODUCTION

Internet Service Provider (ISP) or Electronic Provider is also commonly referred to as Internet Access and Service Provider (IASP), categorized as an intermediary company that plays important role in various activities in the digitalization era such as e-Government, e-Learning, e-Banking, e-Business and several other activities. Through ISP various information-based technology can be enjoyed by the community as end users. Electronic data and information will be transformed when there is an internet network. Thus, the existence of this company that provides internet service as well as electronic information for users, is constituted as avital component in the implementation of electronic transactions. Through ISP, users can enter the gate of cyberspace and access a variety of interesting and important information. Indonesia as an example, currently internet cannot be separated from the daily life of communities, especially urban communities. It seems similar with the communities live in developed countries such as Europe and the United States (US) who have been first utilizing the sophistication of the internet as a means solely to access information and in more specific for storing personal data.

Cook (1996) argues that ISPs have been claimed to be the gatekeepers for access to the web [1], to illustrate how important the ISP existence in many activities during the ongoing process of digitalization. As an intermediary corporation, the ISP functionality, on the one hand, is linked to the responsibility of its obligations to provide internet access service to users who manage sites and the web in cyberspace. In this context, its function is related to provide proper quality of internet service for the users, both who come from the sectors of government, campus, business as well as other users in organizing electronic transactions connected via the internet. On the other hand, ISP functionality is also often associated with its responsibility in Cloud Computing Service relating to personal data storage. Progressively, users not only take advantage of cyberspace's progress solely to access information over the internet, but users also use it to store both business data and personal data that are highly vulnerable to target security attacks. In this context, ISP is also linked to responsibilities related to security attacks in association with cloud computing services. Anna Vamialis (2013), argues that Online Service Providers should pay attention to the security breaches of information data [2]. Security attacks tend to increase both internationally as well as regionally and nationally [3]. Accordingly, data protection is needed. As an example, in the EU it is very important to be understood that the concept of its protection based on the concept of privacy that in Europe is catagorized as a fundamental right [4]. This personal right, even considered as important as others human rights, particularly in the modern information society, this protection is growing internationally and regionally [5].

From a business perspective, communication failure or error in providing internet service from the ISP cannot be denied that this resulted loss to Users. It is because the breach of ISP will also lead to the failure of the Users in presenting a variety of important digital information to the public. In this context, a loss is not solely suffered by Users - who have a contractual relationship with the ISP, but also the broader society that should have the facilities and information from Users. For example, a bank customer suffers loss since he cannot pay E-Ticket through E-Banking because of the non-functioning of E-Banking due to the failure of ISP to perform properly its internet service to the Bank as its User.

On the other hand, the occurrence of security attacks related to Cloud Computing Service is also no less crucial in causing loss to people who already entrust all their affairs including the storage of personal data in cyberspace. For example, the personal data leakage scandal on facebook in April 2018, shows how vulnerable Facebook user data is misused, including abuse for political purposes. Learning from the Facebook case should be used to educate and increase awareness of the people of Indonesia regarding the importance of protecting their personal data on the internet, considering Indonesia is the fourth highest Facebook user in the world [6]. People are also vulnerable not only on losses due to security attacks but also the abuse and leakage of personal data related to government policies. For example, the Indonesian government's policies through the Ministry of Communication and Telematic in early 2017 which requires mobile phone users to register their number by requiring them to include their personal data. In this contects, Indonesian identity card namely *Kartu Tanda Penduduk* as well as Family Card namely *Kartu Keluarga* are needed. In connection with the registration obligation, an Indosat card customer, Aninda Indrastiwi, disclosed and reported that her Residence Identity Number (*Nomor Identitas Kependudukan)* and Family Card were used for registration of more than 50 other cellular numbers [7]. Communities suffering losses resulting from the disclosure of confidentiality and personal misuse of data stored in cloud computing managed by the provider or for compliance with government policies have the right to hold accountable from the parties causing the loss. This article focuses on the ISP responsibility for the loss suffered by the communities or Users.

In association to above phenomenon, first, this article examines to what extent ISP as intermediary company should be held liable for its failure in performing internet service properly on the contractual legal basis; can ISP be relieved from its responsibility on the basis of *force majeure* notion; then in what extent ISP should be held liable in relation to its duty as intermediary company from tort law perspective in regard to Indonesian Consumer Protection Act, more specifically Information and Electronic Transaction Act in comparison to the European Union Regime (EU Regime) and the US Regime. Second, this article examines whether ISP should be held liable for the security attacks of cloud computing service committed by the third party as well as government policies causing the disclosure of confidentiality and misuse of personal data that lead to losses to the Users. In order to understand properly the responsibility of ISP, several responsibility notions will be discussed in the next chapters, started from the contractual legal basis, force majeure, and oblication to provide appropriate security in avoiding personal data misuses.

2. RESEARCH METHOD

This article employs normative legal research method by examining in depth the responsibilities of ISP regarding the loss of Users both in contractual relationships in providing internet access to the Users as well as intermediary company related to personal data protection in cloud computing service that are not

directly bound in contractual relations with users, including liability related to the disclosure of confidentiality and personal misuse of data resulting from weak security measure. The legal materials studied in this article consist of primary and secondary legal materials. Primary legal materials include: Law Number 11 of 2008 on Information and Electronic Transaction, Law Number 19 of 2016 on Amendment to Law Number 11 Year 2008 on Electronic Information and Transaction (hereinafter referred to as the EIT Law Amendment), Law Number 24 of 2013 regarding Amendment to Law Number 23 of 2006 on Population Administration, Indonesian Civil Code, Ministry of Communication and Telematic Regulation No. 20 of 2016 on Protection of Personal Data in Electronic System, The Data Protection Directive (DPD), the e-Privacy Directive, the General Data Protection Regulation (GDPR), the Federal Trade Commission Act (FTC), the Computer Fraud and Abuse Act and various legal documents related to the responsibility of the ISP. Secondary law materials studied from various literatures and journals that are relevant to legal protection of personal data and ISP responsibilities. This study used normative legal research with statute and comparative approaches by employing qualitative analysis.

3. RESULTS AND ANALYSIS

3.1. ISP's role as intermediary company in electronic transaction

Indonesia as one of the most densely populated countries in the world can not be denied has been utilizing the development of information technology in many activities based on electronic transactions, such as in the field of commerce (e-commerce), government (e-government), finance (e-payment), education (e-learning), and other sectors. The definition of electronic transaction regulated under Article 1 (2) of EIT Law Amendment. In various electronic transactions, the Internet plays an important role, so in that context, there is an active interaction between individuals and communities as Users with Internet ISP. One of the biggest ISPs in Indonesia is PT Telkom. ISP through its services can create international communication that involves many parties. In the context of law, it is not impossible that a legal conflict exists between one country and another, especially when a web surfer from a country accesses content hosted from another. The development of the internet requires the harmonization of laws. It means the new legal framework related to the contract cross borders are needed, that cover related issues such as intellectual property rights enforcement, remedies for breach of privacy, including other vulnerabilities [8]. The existence of Convention or International Agreement which comprehensively regulates the legal relationship of the parties in the electronic transaction in cyberspace, including the role and responsibility of ISP, becomes very urgent, so that the implementation of the electronic system could work properly and minimize the dispute.

Reed (2004) argued that the parties and their respective roles in the implementation of a global electronic system consist of principal actors, Infrastucture Providers, Intermediaries Party such as Internet Service Provider (ISP), and Distributed Enterprises [9]. The role of intermediary parties mentioned above, including ISP, is very crucial to the functioning of electronic transactions. In essence, ISP is a business entity that can be managed by the government or private. ISP is an Internet service company that acts as an intermediary facilitating the internet, connecting users to the World Wide Web information service or connecting users to the nearest internet gateway. ISP facilitates individual or group, whether they are government institution, business entities or others, to connect them to any information or data that they need through internet provided by such ISP. For this role of ISP, it is common that the ISP is deemed as a gatekeeper to connect people into the internet. ISP as an intermediary company in cyberspace is actually not much different from an intermediary company in the real world. In short, ISP constitutes a business entity that acts as a media that provides services to connect with the Internet in implementing electronic transactions.

As a business entity, ISP can be owned by the government or privats company that provides connection service facilities to the internet network. There are two types of ISP, the closed and open ISP. The closed ISP only serves the internet network facilities for the local network of the institution in concerned. The examples for this type are ISPs in some departments owned by the government, big companies, research institution or educational institution. Meanwhile, the open ISP serves a function to provide internet network facilities for the public, both for individuals and groups. ISPs that are general in character, like any business activity, are commercial. In Indonesia, people are familiar with the ISP such as WasantaraNet, LinkNet, D-net, TelkomNet, RadNet, and Indosat. ISP that serves the role of providing basic internet services to users or subscribers, has an important function in transformiting electronic information from one party to another party. The success of sending and receiving information or data facilitated by the internet has positive and negative impacts. The negative impacts can be seen in a case where a copyright owner suffers losses related to copyright infringement, illegal content or even defamation which in turn brings the ISP to its responsibility as an intermediary company. The responsibility of ISP is also often associated with losses suffered by users such as website management companies due to ISP failures in properly facilitating the internet as agreed in contractual relationships.

3.2. The liability of isp related to its role as intermediary company

The liabilities of companies that conduct intermediation activities in cyberspace include at least two things, namely: 1. liability for communication failure and other services; and 2. liability related to data including illegal content that is distributed over the internet, such as copyrighted materials, obscenity and indecency, and defamation [10]. Broadly speaking, ISP liabilities can be associated with contractual and non-contractual liability [11].

In the Indonesian context, contracts are generally regulated through the Indonesian Civil Code, particularly Book III. Under Article 1320 the Indonesian Civil Code, an agreement will be valid if it meets the subjective and objective requirements, namely: there must be consent of the individuals who are bound thereby, there must be the capacity to conclude an agreement, there must be a specific subject, there must be an admissible cause. Indonesia embraces the freedom of contract principles as stipulated under Article 1338 paragraph (1) of the Indonesian Civil Code, which essentially stipulates that the parties are free to determine the content of the agreement they wish so long as it is not contrary to public order and morality. In addition, according to such Article, all legally executed agreement shall bind individuals who have conducted them by Law. The provision contained in Article 1338 also reflects the *Pacta Sunt Servanda* Principle, namely the agreement must be kept. Although Indonesia embraces the freedom of contract principle, however Article 1338 Paragraph (3) of the Indonesian Civil Code also emphasizes good faith principle that is an agreement shall be executed in good faith. In this context, good faith principle can be interpreted to mean that any contract made by the parties should be intended for a good cause, reflecting the balance of rights and obligations between the parties, as well as the realization of a fair contract.

Contractual relationship based on electronic transaction in Indonesia is governed by Article 1 number 17 of EIT Law Amendment. It means an agreement is performed through the electronic system as regulated under Article 1 number 5 of EIT Law Amendment. In a contractual relationship with cyberspace, Indonesia has also regulated the freedom of contract, *Pacta Sun Servanda*, and Good Faith principles through Article 18 Paragraph (1) and Article 17 Paragraph (2) of Law Number 11 of 2008 on Electronic Information and Transaction (EIT Law). The *Pacta Sun Servanda* principle that embodied in the electronic agreement shall bind on parties. Good Faith principle also regulated under Article 17 Paragraph (2) of the EIT Law that emphasizes the parties should have good intentions interacting in their transaction. Based on these provisions it can be observed that the obligations agreed in electronic transactions contain the expressions of the freedom of contract that shall be conducted in good faith. In this context, such obligations include the obligations of the Electronic System Provider such as the ISP. Hence, maintaining security personal data of the user in the cloud managed by ISP become his or her liability.

Furthermore, the liabilities of the Electronic System Provider are explicitly governed in Articles 15 and 16 of the EIT Law. As for the *Force Majeure* circumstances which may exclude liabilities in electronic-based contractual relationships are governed in Article 15 Paragraph (3) of the EIT Law. In the situation compelling circumstances *(force majeure*) occurs, no one should a responsibility, including ISP.

The ISP's liabilities as the Intermediary company having contractual relations with the User shall refer to the agreed contractual clauses between the ISP and the User. This context is relevant with *Pacta Sunt Servanda* Principle where clauses agreed shall constitute as Law for them. In the situation that the ISP cannot perform his obligation including to support Internet access to the User which resulting in loss to the User due to communication failure, malfunction or misuse of internet access (liability for communication failure and other services), which should be professionally performed with operating mechanisms, procedures or guidelines in the administration of electronic systems and in good faith by the ISP, may result in ISP's liability to the User in the form of indemnity due to a breach of contract.

The EIT Law provides for the possibility of applying *Force Majeure* in contractual relationships. The ISP may transfer its liability in connection with its failure to provide internet access services which causing harm to the User under the legal ground of *Force Majeure*, as long as the ISP is able to prove that it cannot perform its obligations by fulfilling the elements of *Force Majeure*. If the elements of *Force Majeure* are not met, then an obligation to provide indemnity due to a breach of contract shall arise. Force Majeure based on the Indonesian Civil Code covering: unforeseen event by the parties, for which he is not responsible, beyond the debtor's fault as well as beyond the fault of the parties. The circumstances of *Force Majeure* that can divert the liabilities of the parties are as follow 1. natural disaster, such as floods, earthquakes, fires, and hurricanes; 2. State of war; 3. Riot; and/or 4. government policies in the financial or monetary and economic fields that directly affect the implementation of the work.

The above-explained matters also important to be seen from a comparative perspective. For example, in the US, the development of electronic information has been regulated through many legislations approaches such as the Uniform Computer Information Transaction Act (UCITA) and the Uniform Electronic Transaction Act (UETA) since 1999, the Electronic Signatures in Global and National Commerce Act (E-SIGN) in 2000 [12], the USA PATRIOT Act of 2001, the Electronic Communications

Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA). The last two provisions are federal privacy laws in the context of government investigations [13].

The role of ISP in electronic transactions is crucial. In the context of ISP that acts solely as the intermediary such as facilitating internet access for users in a contractual relationship, its liabilities related to rights and obligations of course refer to the agreement between the ISP and the user that shall bind them as the law. The basic notion of contract is the consensus in the agreement shall become the Law for the parties who have concluded it. In relation to the notion, when the ISP does not comply with his duties based on the contract then liabilities may arise. Furthermore, the ISP's liabilities arise not solely because it has made a breach, but can also be filed for a breach of service agreement, ie the inability of the ISP to fulfill implied warranty of serviceability. The ISP's liabilities related to the breach of service agreement can be seen in the case of American On-Line (AOL) that failed to perform a good quality of service. AOL was sued on the breach the contract by not providing an agreed service and was considered to have committed fraud. In this case, although AOL was not held liable, however, the lesson learned from this case is that ISP should only promise to their customers what they can deliver [14].

3.3. Cloud computing and liability of electronic provider: security attacks and misuse of personal data a comparative approach

At the beginning of the development of ISP, the role of ISP generally solely offered service for Internet access. However, nowadyas ISP also expands its role toward providing Hosting and Extra Value including the role of hosting Cloud Computing which is understood as service provider as well as electronic provider related to storing privacy data both personal and financial data. The definition of Cloud Computing differs from one to another. According to the National Institute of Standards and Technology (NIST), cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimum management effort or the service provider interaction [15]. In comparison, in the Data Protection Review of the European Parliament also can be seen the definition cloud computing as in the NIST [16]. The role of ISP as a provider of cloud computing service leads to liability specifically in term of securing the privacy of data consumers. In the development of storing data in cloud computing, the need for the adequate legal framework is increasingly demanded, particularly to protect data for the purpose specification principle or for the use limitation principle including to protect when personal data reuse or recycling differently from the purpose specification principle. Based on Article 6.1 (b) of the EU Data Protection Directive 95/46/EC, the protection of repurposing data can be identified [17]. In order to protect personal data, it is also relevant using the intellectual property law approach. Trade Secret regime as an example with rationality that personal data is gereally secret, has economic value and security measures (18).

The cloud service contract is used to the underlying legal relationship between ISP and Customer that usually covers the nature of the services related to the volume of data to be transferred to the cloud as well as the leverage of the company. In one hand, cloud-contract can be in the form of a non-negotiated contract (clickwrap agreement) that seemingly in more favor for the cloud service provider. Meanwhile, on the other hand, cloud-contract can be in the form of negotiated agreement where the customer has an opportunity to negotiate and add several provisions that address his or her needs comprehensively [19].

Cloud-contract, both in the form of clickwrap agreement and in the form of negotiated-agreement in the master service agreement, at least contains the obligation to provide adequate security to protect personal data, company financial data and the other asset of intellectual property. Regarding the privacy security of data stored through cloud computing service providers, users or consumers must be smart and thoroughly understand the risks of using cloud computing services by carefully reading and understanding the terms and conditions provided by the provider to avoid the risk of confidentiality and misuse of privacy data [20].

The protection of data privacy stored through cloud computing is not only protected through a contractual legal basis but also through provisions requiring adequate security obligations. The US for example, in regard to its legislation, those obligations can be explored through Section 5 (a) of the FTC Act. This provision can be imposed toward data security breaches on two grounds. First, the liability of online service provider can be emerged on the ground of deceptive trade practice, in this context when an online service provider who provides a privacy policy has a failure to protect personal data of consumer. Second, liability for unfair trade practices when such online service provider does not implement security measures in their cloud computing to prevent unauthorized access for consumer privacy data. The FTC continually focuses to protect privacy and security in virtual reality. The 2018 FTC also cover economic privacy, including when companies fail to secure consumer information, and how to balance the costs and benefits of privacy-protective technologies and practices [21].

The next example is the protection provided in the EU level. In the EU level, under the DPD [22] Reform or the Proposed Amendment Regulation, especially the final Proposal 2017 for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), several major concerns have been regulated to provide better protection upon personal data by empowering more advanced security measures and by imposing sanction and compensation. Based on Article 7 and Article 8 of the Regulation several security measures shall be conducted by service provider in order to protect personal data related to storage and erasure of electronic communication data and protection of information stored and related to end-user's terminal equipment [23]. Furthermore, remedies and right to compensation and liability are clearly stipulated under Article 21 and article 22 of the EU Final Proposal concerning Regulation on Privacy and Electronic Communications. Through those provisions it can be understood that the liability of service provider related to personal data in cloud computing may arise caused by unproperly or lack of security measures provided by the ISP. However, according to Article 14 (1) of the E-Commerce Directive, the service provider has immunity from liability for hosting illegal content, as long as service provider has no actual knowledge of illegal material, or upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information [24].

Related to the data protection, furthermore The General Data Protection Regulation (GDPR**)** adopted by the EU in April 2016, will substitute the Data Protection Directive and will be enforceable starting on 25 May 2018 that fully applicable across the EU. The GDPR is the most comprehensive and progressive piece of data protection legislation in the world, updated to deal with the implications of the digital age. GDPR replaces the Data Protection Directive 95/46/EC [25]. The main protection of personal data can be clearly understood through Article 1 of the General provisions of the GDPR. Even, through this provision also emphasized that personal data protection as a fundamental right. What is personal data, the GDPR regulates under Article 4. (1). Based on Article 4 (1) of GDPR, it can be understood that within the EU level, personal data is any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address. Concerning medical information as personal data is regulated under Article 4 (15) of the GDPR that in general regulates data concerning health is personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. Furthermore, lesson learned can be taken from the current EU regulation is based on Article 3 of the GDPR, it can be understood the territorial scope of personal data protection covering cross border the EU. Article 3 of the GDPR not only applies to organizations located within the EU but it also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location [26].

Regarding breach of personal data protection, such as breach of security cloud computing, unlawful destruction, loss or stolen, data breach could harm personal data owner based on Article 33-34 of the Regulation, the company causing the data breach will have to inform the owner of personal data (and the relevant data protection supervisory authority) shall without undue delay. If the company doesn't do this, it can be fined. Recent attacks, such as WannaCry, Meltdown and Spectre, or the Uber case show how important this new right is [27]. Keeping security of personal data protection is an obligation of the processor under Article 32 of the GDPR. The controller or processor should evaluate the risks inherent in the processing and should ensure appropriate security of personal data, including for preventing unauthorized access [28]. The obligation of the processor in one side create another right of the personal data owner to get an effective judicial remedy as stipulated under Article 79 (1) of the GDPR. In addition, based on Article 82 (1) of the GDPR can be elaborated the right of the data subject or user to get compensation and become a liability of electronic provider. That liability is regulated through Article 82 (2) of the GDPR, specifically when processor has not complied with his obligations as regulated under the GDPR [29].

By comparing to the US level, although many commentators have argued that the regulation concerning the liability of processor is rather limited, such as no regulatory jurisdiction for the banking telecommunication, however remedies for the consumer still can be elaborated through the FTC Act. For example, the FTC charged Google with misrepresenting that it was treating personal information from the EU in accordance with the Safe Harbor Program. In this case, Google is required to establish and maintain a comprehensive privacy program. Furthermore, every two years the company should conduct an independent audit by an independent third party to assess privacy and data protection practices for the next 20 years [30].

Personal data protection in Indonesia has also been one of the hot topics of recent debates, particularly with regard to the Ministry of Communication and Telematic policy in early 2018 which requires every mobile phone user to register a cellular SIM Card with the requirement of the inclusion of the Identity Card Number and Family Card. In the implementation of such registration obligation, there is suspicion on leakage and misuse of personal data, as experienced by an Indosat card customer, Aninda Indraswati. She found out that her NIK and KK was used for registration of more than 50 other cellular numbers [7]. In addition, in early April 2018, the user of Facebook in Indonesia was also shocked by the misuse of user personal data. The vulnerability of security levels and the lack of protection of personal data in Indonesia are questionable. The outstanding problem here in Indonesia is that there are no specific Laws that govern matter on the personal data protection as in the US and the Europe well-established Laws and Regulation. However, personal data protection can be observed in various provisions of Laws and Regulations. The EIT Law Amendment, for example, emphasizes the protection of internet users to gain the right of information access [31]. On the other hand, this protection also can be found in Article 1 number 22 of Law Number 24 of 2013 on the Amendment of Law Number 23 of 2006 on Population Administration Act which stipulates that Personal Data is certain personal data stored, maintained and which truth and confidentiality upon such data is secured. Pursuant to Article 86 Paragraph (1) of the Population Administration Law, Minister shall be responsible for granting the right of access of Personal Data to provincial officers and officers of implementing Agencies. Furthermore, Article 86 Paragraph (1a) of the Population Administration Law provides that the security officers as referred to in Article 86 Paragraph (1) are prohibited to disseminate Personal Data that are inconsistent with their authority. As for the sanction, according to Article 95 A of the Population Administration Law, sanction for any person who disseminates Personal Data as referred to in Article 86 Paragraph (1a) can be in the form of imprisonment for two years and/or a maximum fine of Rp. 25,000,000 (twenty five million rupiah).

The personal data protection, particularly concerning the use of personal data information through electronic media is regulated through article 26 of the EIT Law Amendment. The provision provides that the use of personal data by other parties shall be subject to the consent of the owner of such personal data. Furthermore, it is stipulated that the owner of personal data whose rights are violated and suffered losses, his party may file a lawsuit for losses suffered. In regard to Article 26 Paragraph (2) of EIT Law Amendment, it may be argued that the party suffering losses in connection with the violation of privacy rights may file a lawsuit against the party causing the loss to occur, in this relevant context is attributed to Electronic System Provider. The question is whether the cloud computing service provider is classified as an Electronic System Provider? What about the Law Firm? Whether a Law Firm is also included as the Electronic System Provider? The confusion surfaced among observers of Law Firm in Indonesia as the reflection of the failure of Mossack Fonseca Law Firm to secure the confidentiality of its clients' data in the Panama Papers scandal of April 2016. Teguh Arifiyadi, Head of Sub-Directorate of Investigation and the Implementation of the Security Directorate of the Ministry of Communication and Informatic argues that as long as the legal subject provides, administers and/or operates the Electronic System, thus it constitutes as the Electronic System Provider [32]. Article 1 number 6 of the EIT Law Amendment stipulates that Electronic System Provider is any person, State organizer, business entity, and society that provides, manages and/or operates Electronic System, either individually or collectively, to the users of the Electronic System for the purposes of himself and/or the needs of others. Based on this provision, both law firm and cloud computing service provider that provide, manage and operate Electronic System may be categorized as Electronic System Provider. Therefore, in connection with the provision of Article 26 Paragraph (2) of the EIT Law Amendment, the service provider in cloud computing can be held accountable for any losses suffered by Users due to the disclosure of confidentiality and misuse of personal data of the users.

In addition, the existence of Ministry of Communication and Telematic Regulation No. 20 of 2016 on Protection of Personal Data in Electronic System can be regarded as a regulation that regulates the protection of personal data especially related to Electronic System. Article 3 of this regulation expressly provides that the protection of personal data in electronic systems is carried out in the process of acquisition and collection; processing and analyzing; storage; appearance, announcement, dispatch, dissemination and/or access opening; and e. elimination. In order to implement the process as set forth in article 3 above, thus the provision contained in Article 5 needs to be considered in which the Electronic System Provider must regulate internally and determine security measures in order to prevent failure in the protection of personal data by considering aspects of application of technology, human resource, method, and cost. Preventive measures in order to avoid failures in the protection of personal data which at least must be done by the Electronic Systems Provider are: performing activities that increase awareness of human resources on their environment as well as conducting training on the prevention in avoiding failures of personal data protection in electronic systems. Article 5 of the Ministry Communication and Telematic Regulation appears to be in line with the provisions of the EU Regulation on Privacy and Electronic Communications as well as Article 7

and Article 8 of the Regulation on Privacy and Electronic Communication that emphasize more advanced security measures provided by service provider in order to protect personal data including in cloud computing equipment.

By understanding the protection of personal and privacy data in cloud computing in Indonesia, the US and the EU level, it can be stated that the liability of service providers may arise both on the ground of breach of contract and the breach of the duty of care as required by the laws such as providing and implementing the appropriate security measures to prevent both security attacks and misuse of personal data by irresponsible parties. In regard to provide better protection to the citizens, the EU continually improve the personal data protection, as in the Data Protection Reform which entered into force in 2016 and will be applicable on 25 of May 2018 known as the General Data Protection Regulation (GDPR), this regulation fully applicable across the EU. The cybersecurity issues are crucial ones. Therefore, how to determine who should responsible and how to mitigate the speed of it threaten as well as the appropriate mechanism to reduce it spread in global society it does not a responsibility of States alone but also other stakeholders. Ingolf Pernice reveals that States, Individuals, business, techno academia and public authorities are needed to share a common responsibility. This notion can be as a global cybersecurity governance [33]. By understanding the perfect cybersecurity may cannot be reached, therefore private companies should seek the optimal solution for their cybersecurity investment based on a company-by-company basis [34]. Even from the computer technic, the measures to protect data may still relevant employing the data hiding technique hides secret information within a multimedia file [35].

4. CONCLUSION

Based on contract principles and the Law Number 11 of 2008 on Electronic Information and Transaction, it can be understood that all clausula agreed on the contracts shall bind on parties as well as the obligations agreed in electronic transactions contain the expressions of the freedom of contract that shall be conducted in good faith, such obligations including the obligations of the Electronic System Provider for maintaining the security of the users' personal data stored in the Cloud Service Provider that it manages. The ISP as an intermediary company should be held liable for its failure in performing internet service properly on the contractual legal basis. Furthermore, the liabilities of the Electronic System Provider in Indonesia are explicitly regulated under Articles 15 and 16 of the Electronic Information Technology Law that basically govern that any Electronic System Provider must provide electronic systems in reliable and secure manner and shall be responsible for the proper operation of the Electronic Systems, as well as Electronic System Providers shall be responsible for their Provision of Electronic Systems. Meanwhile, related to the notion of force majeure, Electronic Provider can relieve from its liability, or in other words, the Article 15 shall not apply where it is verifiable that there are occur compelling circumstances, fault, and/or negligence on the part of the Electronic System users. When there is unforeseen event occurred, for which the parties are not responsible, beyond the debtor's fault as well as beyond the fault of the parties. The circumstances of *Force Majeure* that can divert the liabilities of the parties are as follow 1. natural disaster, such as: floods, earthquakes, fires and hurricanes; 2. State of war; 3. Riot; and/or 4. government policies in the financial or monetary and economic fields that directly affect the implementation of the work.

The role of ISP as a provider of cloud computing service leads to liability specifically in term of securing the privacy of data from consumers stored in cloud computing. The Electronic provider has an obligation to provide adequate security to protect personal data and the other asset of intellectual property which stored through cloud computing service providers. In the form of contractual basis users as a consumer also has an obligation to understand the risks of using cloud computing services to avoid the risk of confidentiality and misuse of private data. However, the electronic provider still should be held liable for the security attacks of cloud computing service committed by the third party as well as government policies causing the disclosure of confidentiality and misuse of personal data that lead to losses or damages to the users. In the US level, through Section 5 (a) of the FTC Act, the liability of electronic online provider related to personal data security breaches can be imposed on the grounds of deceptive trade practice and liability for unfair trade practices. Meanwhile, in the EU level, the obligation and responsibility of online provider or electronic provider to provide security measures in order to prevent failure in the protection of personal data have continually improved from the Data Protection Directive (DPD) to the General Data Protection Regulation (GDPR). In comparison to Indonesia, the protection of personal data related to electronic media including the liability of electronic provider for any losses suffered of user caused by disclosure of confidentiality as well misuse of personal data event failure has been regulated through Article 26 of Law No. 19 of 2016 concerning the Electronic International Technology Law (Amendment). Through Article 5 of the Ministry of Communication and Telematic Regulation No. 20 of 2016 on Protection of Personal Data in Electronic System, in order to prevent failure in the protection of personal data, the Electronic System

Provider must regulate internally and determine security measures by considering aspects of application of technology, human resource, method and cost. Lesson learned can be taken from the US and the EU for better protection of personal data as well as to anticipate the advanced electronic information and technology, the Big Data's regulation and clear territorial scope of protection become necessary to consider in line with providing sufficient security measure to prevent breach and misuse of personal data.

ACKNOWLEDGEMENTS

We would like to deliver our gratitude to the Dean of the Faculty of Law of Udayana University who has provided us with an opportunity to participate in the journal writing workshops as well as the Association of Law Journal throughout Indonesia which open our insights in writing international journal articles. Also thank to Putu Aras Samsithawrati for her dedication as a proof reader.

REFERENCES

[1] Cook WJ., "Why Internet service providers should be copyright guardians," 1996.
[2] Vamialis A., "Online service providers and liability for data security breaches," *J Internet Law*, vol. 16, no.11, pp. 23-33, 2013.
[3] Štitilis D, Pakutinskas P, Malinauskaitė I. "EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis," *Secur J.*, vol. 30, no. 4, pp. 1151-68, 2017.
[4] Altmayer O. "The Tipping Point–Reevaluating the ASNEF-EQUIFAX Separation of Competition of Data Privacy Law in the Wake of the 2017 Equifax Data Breach," *Northwest J Int Law Bus*, vol. 39, no. 1, pp. 37, 2018.
[5] Abdulrauf LA, Fombad CM., "Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms," *Liverp Law Rev.*,vol. 38, no. 2, 105-34, 2017.
[6] Kurnia T., "Facebook Data Leaks Become a Momentum for Understanding Privacy (in Bahasa)," *Tekno Liputan6.com*, [Online]. Available from: https://www.liputan6.com/tekno/read/3422019/kebocoran-data-facebook-jadi-momentum-untuk-memahami-privasi, [cited 2018 Apr 28].
[7] Hidayat R., "The importance of being initiated by the Personal Data Protection Act (In Bahasa)," [Online]. Available from: https://www.hukumonline.com/berita/baca/lt5aa121e363f75/pentingnya-digagas-uu-perlindungan-data-pribadi, [cited 2018 Mar 10].
[8] Rustad ML, Koenig TH., "Harmonizing internet law: lessons from Europe," *J Internet Law*, vol. 9, no. 11, pp. 3-11, 2006.
[9] Reed C., "Internet law: text and materials, " Cambridge University Press; 2004.
[10] Makarim E., "Legal responsibility of providers of electronic systems (in Bahasa)," Rajawali Pers, 2010.
[11] Zhao Y., "Internet service providers and their liability," *Law Technol.*, vol. 34, no. 1, pp. 1, 2001.
[12] Berenstein GL, Campbell CE., "Electronic contracting: The current state of the law and best practices," *Intellect Prop Technol Law J.*, vol. 14, no. 9, pp. 1, 2002.
[13] Hayes CM, Kesan JP, Bashir MN., "Cloud Services, Contract Terms, and Legal Rights," *J Internet L.*, vol. 6, pp. 3, 2013.
[14] Tysver DA., "ISP Liability (BitLaw)," [Online]. Available from: https://www.bitlaw.com/internet/isp.html, [cited 2018 Jan 30].
[15] Rghioui A, Oumnad A., "Internet of Things: Surveys for Measuring Human Activities from Everywhere," *Int J Electr Comput Eng.*, vol. 7, no. 5, 2017.
[16] Štitilis D, Malinauskaitė I., "Evaluation of legal data protection requirements in cloud services in the context of contractual relations with end-users," *Soc Technol.*, vol. 3, no. 2, pp. 390–414, 2013.
[17] Custers B, Uršič H., "Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection," *Int Data Priv Law.* vol. 6, no. 1, pp. 4–15, 2016.
[18] Malgieri G., "'Ownership'of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?," *Journal of Internet Law*, vol. 20, no.5, Nov 2016.
[19] Gilbert F., "Cloud service contracts may be fluffy: selected legal issues to consider before taking off," *J Internet Law*, vol. 14, no. 6, pp. 17–30, 2010.
[20] Dewi S., "The Concept of Legal Protection for Privacy and Personal Data Associated with the Use of Cloud Computing in Indonesia (in Bahasa)," *DEMO 2 J.*, (94), 2016.
[21] Henderson JG., "FTC Releases Agenda for PrivacyCon 2018," *Federal Trade Commission*, [Online]. Available from: https://www.ftc.gov/news-events/press-releases/2018/02/ftc-releases-agenda-privacycon-2018, [cited 2018 Mar 3].
[22] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," [Online]. OPOCE; Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3Aen%3AHTML, [cited 2019 Mar 12].
[23] "Regulation Of The European Parliament And Of The Council: concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)," *European Commission*, [Online], Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN, [cited 2018 Mar 8].

[24] Sartor G., "Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?," *Int data Priv law*. vol. 3, no. 1, pp. 3–12, 2012.
[25] "GDPR FAQs," *EUGDPR*, [Online]. Available from: https://eugdpr.org/the-regulation/gdpr-faqs/. [cited 2018 Apr 27].
[26] De Hert P., Czerniawski M., "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context," *Int Data Priv Law.*, vol. 6, no. 3, pp. 230–43, 2016.
[27] "EU Data Protection Reform: better data protection rights for European citizens," [Online], Available from https: //ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-citizens_en.pdf, [cited 2018 May 9].
[28] European Commission, "Questions and Answers – General Data Protection Regulation," [Online], Available from: http://europa.eu/rapid/press-release_MEMO-18-387_en.htm, [cited 2018 May 9].
[29] "Art. 82 GDPR – Right to compensation and liability," *General Data Protection Regulation (GDPR)*, [Online], Available from: https://gdpr-info.eu/art-82-gdpr/, [cited 2018 May 9].
[30] Colonna L., "Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?," *Int Data Priv Law*, vol. 4, no. 3, pp. 203–21, 2014.
[31] Yusa IG, Bunga D, Stiawan D., "The Authority of Government in Clearing Hatefull and Hostilities Electronic Information Based on Tribe, Relegion, Race and Intergroup," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 6, pp. 3735, 2017.
[32] Edwin Elnizar N., "Mossack Fonseca Bangkrut, 3 Lessons from the Failure of a Famous Law Firm Protect the Confidentiality of Personal Data," [Online], Available from: https://www.hukumonline.com/berita/baca/lt5aacd1293437c/mossack-fonseca-bangkrut--3-pelajaran-dari-gagalnya-firma-hukum-ternama-lindungi-kerahasiaan-data-pribadi, [cited 2018 Mar 18].
[33] Pernice I., "Global cybersecurity governance: A constitutionalist analysis," *global-Constitutionalism*, vol. 7, no. 1, pp. 112–41, 2018.
[34] Teplinsky MJ., "Fiddling on the Roof: Recent Developments in Cybersecurity," *Am U Bus L Rev.*, vol. 2, pp. 225, 2012.
[35] Ntahobari M, Ahmad T., "Protecting Data by Improving Quality of Stego Image based on Enhanced Reduced Difference Expansion," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 4, pp. 2468, 2018.