GOOD CORPORATE GOVERNANCE PRINCIPLES ON INTERNET INTERMEDIARY COMPANIES IN PROTECTING THE PRIVACY OF PERSONAL DATA IN INDONESIA

Saskia Kusumawardani[1]; Sinta Dewi Rosadi[2]; Elisatris Gultom[3]
[1,2,3]Faculty of Law, Universitas Padjadjaran
Email: saskiaaribowo@gmail.com, sinta@unpad.ac.id, elisatris@yahoo.com

Article Information

Submitted: February 4, 2020
Accepted: May 2, 2020

Keywords:
good corporate governance; internet intermediary; privacy; personal data protection; liability

Abstract

The implementation of good corporate governance (GCG) is the main foundation of companies that needs to run their business activities for a long period. Along with the development of technology and information, the implementation of GCG is increasingly needed for internet intermediary platform providers in carrying out their business activities. The implementation of GCG principles can also reduce the risk of failure in protecting privacy of personal data on the platform. The related principles are transparency, accountability, and responsibility principle by taking into account a number of laws and regulations such as Law No. 11 of 2008 as amended by Law No. of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE Law), Government Regulation No. 71 of 2019 (GR 71/2019), and Ministry of Communication and Information Regulation No. 20 of 2016. This research will use a normative juridical research method that takes into account the provisions of the legislation and other relevant documents. As a result, the implementation of GCG is not fully implemented in the case of failure in protecting privacy of personal data in internet intermediary company (PT Bukalapak), thus the legal attempt that can be applied to manifest the company's liability refers back to ITE Law, GR 71/2019, and Ministry of Communication and Information Regulation 20/2016 which are compensation and administrative sanctions.

I. Introduction

Company or Business Entity is one of the subject of economic activity that contributes significantly in the development of the country's economic growth. The company has an important role as a producer of goods and services, consumers of production, distributors of goods and services, and development agents (Asih Reta Wening Surya, 2017: 1). The presence of a company is certainly expected to provide prosperity for the wider community and the country's competitive ability globally. Yet various crises befalling these companies, such as conflicts of interest between the majority and minority of shareholders, between shareholders and directors, between directors and employees, as well as the violation potentials of environmental preservation, failure in risk management and company performance, and so forth.

In dealing with those conflicst and problems, indeed a good corporate governance (GCG) is needed. This GCG concept initially developed in the United States and United Kingdom. However, it cannot be denied that today GCG is not only a sole option for businessmen, yet also a vital obligation and necessity to provide accountability for all actions taken by the company. A study compiled by the World Bank shows the weak implementation of GCG is one of the factors that caused the crisis in Asia due to the lack of financial performance report and other corporate obligations (Dwiridotjahjono, Jurnal Parahyangan University Journal, 2009: 102).

In essence, GCG is a system used by Organs (Shareholders, Directors, and Board of Commissioners) to direct and control and oversee the management of organizational resources efficiently, effectively, economically and productively based on the principles of transparency, accountability, responsibility, independence, and equality and fairness which came to be called the principle of TARIF (Syakhroza, 2002: 22). Along with the development of law, science, technology, and information, the GCG principles are implicitly accommodated in the articles in Law Number 40 of 2007 concerning Limited Liability Companies due to the increasingly widespread demands of the community for fast services, legal certainty, and demands for the development of the business world in accordance with the principles of good corporate governance.

The reason companies need to implement GCG practices is because this practice actually has a large impact in increasing the value of the company, optimizing financial performance, reducing the risk that may occur for every decision made by the Organ, and increasing the confidence of stakeholders (Dwiridotjahjono, Jurnal Unpar, 2009: 105). In addition, the need for the implementation of GCG is also very important for internet intermediaries companies along with advances in technology and information. This is because internet intermediaries provide digital platforms such as social media, video streaming, e-commerce, or e-transport that essentially provide services that are fast and easily accessible, making people dependent on using these platforms to carry out their daily activities. Hence, if people need to use the services available on the platform, the company needs to collect and process personal data of each individual.

The collection and processing of personal data is actually a risky thing to do, thus the implementation of GCG is important for companies to reduce any risks that might occur. In essence, the principles of GCG that are closely related to the protection of personal data include the principle of transparency, the principle of accountability, and the principle of responsibility. First, the principle of transparency means that companies must convey clear and definite information to stakeholders (Academic Script, 2006: 5). Based on the General Guidelines for GCG established by the National Governance Policy Committee/Komite Nasional Kebijakan Governance (KNKG), the meaning of the transparency principle is that the company is obliged to submit a privacy policy and if there has been a failure in protecting privacy of personal data on the electronic system. Second, the principle of accountability is every director and employee must carry out their duties and responsibilities by adhering to business ethics and code of conduct, one of which is manifested by maintaining the confidentiality of information in accordance with laws and regulations and company policies. Third, the principle of responsibility can be reflected in the company's compliance with applicable laws and regulations, in

this case by complying with the laws and regulations relating to the protection of personal data, starting from Law Number 19 of 2016 concerning Amendment to Law Number 11 Year 2008 concerning Information and Electronic Transactions (ITE Law), Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions (PP 71/2019), and Ministry of Communication and Information Regulation Number 20 Year 2016 concerning Protection of Personal Data in Electronic Systems (Ministry Regulation 20/2016).

The rise of issues regarding the protection of personal data originated from the increasing number of cell phone and internet users which caused many cases of personal data leakage (data breach), data fraud, or other unlawful actions (Academic Script, 2016: 2). Therefore, every company, especially an electronic system provider company, must comply with statutory provisions concerning the protection of personal data and apply the principles of GCG as a preventive measure for violation of personal data, both external and internal.

In addition to the provisions of the laws and regulations mentioned above, internet intermediary companies also need to take notice of the provision that's commonly used in business practices, namely the General Data Protection Regulation (GDPR) which is the most modern provision for personal data protection in this so called digital era. GDPR aims to encourage companies to continuously compete in developing adequate information management systems and increasing the security of personal data. By issuing a privacy policy that complies with the principles contained in GDPR, companies can get the opportunity to have a lawful yet appropriate privacy protection strategy, because personal data is one of the main assets and keys of the company's most valuable business (Phintraco Group, February 14th 2018).

In Indonesia, a case of failure in personal data protection at an internet intermediary company occurred at PT Bukalapak, a leading e-commerce intermediary company owned by a local citizen. This case was disclosed in March 2019, with a leak of 13,369,666 data users, which was hijacked by a professional hacker from Pakistan with the nickname "Gnosticplayers". The data consists of emails, usernames, real names, shopping details, IP addresses, and passwords which are then traded on the "Dream Market" site on the dark web (Technologue.id, March 8th 2019).

A similar case occurred in Lion Air Group's subsidiary companies, namely Malindo Air and Thai Lion. In this case, Malindo Air acknowledged the personal data breach of passengers such as identity cards and passports that had been misused by irresponsible parties (CNBC, September 18th 2019). Around 30 (thirty) million passenger data were leaked and traded on the dark web (Bisnis.com, September 23th 2019). From the leakage of personal data, this issue did not rule out the possibility of data belonging to Indonesian citizens. Therefore, the Ministry of Communication and Information of the Republic of Indonesia (Kemenkominfo) together with the Lion Air Group company will work this case out.

Both of the cases above represents company's negligence in providing personal data protection. However, this study will focus on how internet intermediary company's which is PT Bukalapak in applying the GCG principles as a preventive measure that can be taken to reduce the risk of privacy invasion in providing personal data protection

for users. This matter certainly needs to be done, because the services available on internet intermediary platforms are already an integral part of one's daily needs. It can be ascertained that the public really needs internet intermediary platform services in order to get easier, more efficient and effective access to carry out daily activities, yet on the other hand, personal data collected by companies carries a high risk of privacy violation, thus the public needs to pay attention to company's privacy policy and give full and conscientious consent.

II. Research Methods

The research method uses normative juridical methods with secondary data i.e. data consisting of legal texts, literature, and pre-existing research documents (Soekanto & Mamudji, 2003:13-14). Literature material used includes relevant legislation and literature in the form of books, journals, and other supporting materials including dictionaries, encyclopedias and other materials that provide instructions about the material used as previous data.

III. Research Result and Discussion

A. Internet Intermediary Company as a Legal Subject

Before entering into the subject matter, it is necessary to understand in advance about the intermediary internet company itself. Literally, "Intermediary" means something that is located between or in the middle, so that "Internet Intermediary" means something that can help the process of transmitting or distributing content, products, or services across a network or server (OECD, 2010: 9). Furthermore, the OECD defines internet intermediaries as follows:

> *"'Internet Intermediaries' bring together or facilitate transactions between third parties on the internet. They give access to host, transmit and index content, products and services originated by third parties on the internet or provide Internet-based services to third parties."*

Third parties as mentioned above is a producer of content, products and services, as well as consumers or users, products and services (OECD, 2010: 9). The classification of internet intermediaries itself comes from various business sectors, as reported in the OECD Report, including (OECD, 2010: 10):

1) Access of internet and service providers (ISPs);
2) Data processing and web hosting providers, domain name registrars;
3) Search engines (Google, Bing, Naver);
4) E-commerce intermediaries Amazon, eBay);
5) Payment system (Visa, Paypal, Mastercard);
6) Participative networking platform (Facebook, Youtube, Instagram, LinkedIn).

Based on the description above, it can be concluded that the object of this research which is PT Bukalapak is qualified as an internet intermediary company

with e-commerce intermediary services that provide e-commerce platforms to connect sellers with buyers on the internet. In addition, based on Ministry of Communication and Information Circular Letter No. 5 of 2016, it is stated that a Platform Provider is a legal subject in ITE Law which is as an Electronic System Provider. In that case, the platform provider is the internet intermediary itself. Normatively, the definition of the Electronic System Provider can be found in Article 1 (4) GR 71/2019. Therefore, PT Bukalapak is an internet intermediary company which is also qualified as a legal subject in the ITE Law namely an Electronic System Provider that provides e-commerce platform as a connecting network between content providers and consumers.

B. The Implementataion of Transparency, Accountability, and Responsibility Principles in Good Corporate Governance on Internet Intermediary Company

PT Bukalapak as an internet intermediary company is one of the contributor of the country's economic growth. To maintain the sustainability of its business in the long term, it is appropriate for PT Bukalapak to implement GCG principles so that the company is able to create a competitive and structured corporate management climate. In addition, the company will continue to face risks in the operation of the company, this matter results in the application of GCG as a prevalent effort to conduct in order to prevent such risk.

In general, the risk that internet intermediary will always face is the risk of failure in protecting privacy of personal data in electronic systems. This certainly must be a concern of companies as their responsibility as an electronic system providers, hence it is appropriate for internet intermediaries to carry out their business activities in accordance with the principles of GCG to control the risk of failure in protecting privacy of personal data. As stated earlier, personal data protection aspect is related to three out of five principles in GCG, namely the principles of transparency, accountability, and responsibility. Referring to the leakage of personal data that occurred at PT Bukalapak as one of the internet intermediary company, the application of the three principles in the GCG will be described as follows:

1) Principle of Transparency

In general, transparency means the company's openness in conveying material and relevant information (KNKG, 2006: 5). Indicators for assessing company transparency are information and policies within the company (Andypratama, Mustamu, Jurnal AGORA, 2013: 3). Based on Article 5 paragraph (1) GDPR principally states that the processing and/or collection of personal data must be legal, fair and transparent. This can be manifested by the way the company submits towards the stakeholders about the purpose of processing and/or collecting personal data openly, about the company's business activities, how the personal data will be used by the company, as well as information related to the failure in protecting privacy of personal data or data breach on the electronic system owned by the company,

especially the user concerned (ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data -protection-regulation-gdpr / principles / lawfulness-fairness-and-transparency / accessed on February 2nd, 2020). Furthermore, the General Guidelines of GCG also outline the main forms of implementation of the transparency principle itself, and those relating to the personal data protection, including:

a) Company has the obligation to fulfill the provision concerning the confidentiality of the company as regulated on the laws and regulations, position secrecy, and individual rights;
b) The policy of the company must be written and proportionally communicated towards all stakeholders.

Personal data is one form of internet intermediary company's most valuable information that must be kept confidential and accurate in order to preserve the interests of consumers. Thus, it is appropriate for the company to convey information to consumers / users regarding the failure in personal data protection which is one of the right to consumer's privacy. This is also a form of good faith as the organizer of the electronic system as stipulated in Article 2 f Ministry of Communication and Information Regulation 20/2016.

The notification mechanism is stipulated in Article 28 c Ministry of Communication and Information Regulation 20/2016 which states that written notice of failure to protect personal data in the electronic system it manages can be made with the following notification provisions:

a. Accompanied by reasons or causes of failure in personal data protection;
b. Can be done electronically if the Owner of the Personal Data has given consent for that which is stated at the time of the acquisition and collection of their Personal Data;
c. It must be ensured that the Owner of Personal Data has received it if the failure contains a potential loss for the person concerned; and
d. Written notification is sent to the Owner of Personal Data no later than 14 (fourteen) days after the failure is known.

PT Bukalapak as an electronic system provider has actually implemented this principle, for the reason that PT Bukalapak has informed users about their Privacy Policy in a clear and proportional manner. This policy can be found and accessed easily in www.bukalapak.com/privacy. In the policy, PT Bukalapak stated that the collection and processing purpose is in order to increase the quality and service provided in Bukalapak's system as regulated in the applicable laws based on user's consent, also to monitor in order to know user's transaction patterns, for administrative and investigation necessity or what is obligated by the laws and regulations, to ensure that the service works fine.

However, PT Bukalapak had been negligence in fulfilling its obligation to inform users regarding the failure in protecting privacy of personal data

as regulated in its Privacy Policy. Referring back to Article 28 c Ministry of Communication and Information Regulation No. 20/2016, actually PT Bukalapak is obliged to send written notification through e-mail no later than 14 (fourteen) days or two weeks after knowing that there was a failure in personal data protection in their system.

In fact, this data breach case that occured in Bukalapak was reported by the media on March 2019, however within 14 (fourteen) days, PT Bukalapak did not submit a written notice of the violation via e-mail. For this reason, it can be said that Bukalapak does not carry out its legal obligation to inform users transparently about the failure in protecting personal data in accordance with the specified time of 14 (fourteen) days.

This failure in protecting privacy of personal data naturally results in the violation of the user's privacy rights, so that it is appropriate for PT Bukalapak to notify this incident to users as a manifestation of its good faith, apart from the possibility that PT Bukalapak's reputation as one of the leading online marketplaces will decrease. This transparency principle also relates to the right of individuals to obtain the information needed related to personal data or "the right to be informed" in GDPR. The reason users must know the existence of personal data is to foster individual trust in the platform and provide useful and necessary information (ICO, Open Government License 3.0).

From the whole explanation, it can be concluded that PT Bukalapak has applied the principle of transparency in GCG, namely by clearly notifying its privacy policies that can be easily accessed by users, as well as providing information about the purpose of processing personal data that it intends to do. However, specifically in the case of personal data leakage, PT Bukalapak did not submit written notice as its legal obligation that is regulated in the provisions of the legislation.

2) Principle of Accountability

This principle contains meaning that a company must be accountable of their work performances transparently and properly. For this reason, the company must be able to be managed properly, measurably, and in accordance with the interests of the company while taking into account the interests of shareholders and other stakeholders. This assessment of accountability principles is seen through work ethics and auditing (Anypratama and Mustamu, AGORA Journal, 2013: 3). The main forms of implementation include each organ and company employees must adhere to business ethics and code of conduct that has been agreed, specifically in terms of keeping company information confidential and taking responsibility for all company actions that cause harm (KNKG, 2006: 6).

Each company must follow the basic accountability principles according to the General Guidelines for GCG. **First**, every company must have values that describe the company's moral attitude in conducting its

business. **Second**, to be able to manifest the moral attitude, the company must have a business ethics formula agreed by the board and employees. **And third**, the values and formulations of the company's business ethics need to be outlined and further elaborated in the code of conduct in order to be understood and applied.

The function of the Code of Conduct and Business Ethics itself is a guide to conflicts of interest, giving and receiving gifts and donations, compliance with regulations, confidentiality of information and reporting on unethical behavior (Kaihatu, Journal of Management and Entrepreneurship, 2006: 7). In the context of implementing an electronic system, a code of conduct is needed by internet intermediaries to prevent unethical behavior, such as the management or employees who want to misuse or disclose the confidentiality of information without rights, for example by leaking users' personal data for personal gain which is commonly known as malicious insider or party in a company that attacks the company's electronic system (Supradono, 2009: 4).

As a form of implementing the principle of accountability in GCG, PT Bukalapak has actually compiled a code of conduct which contains provisions regarding the company's obligation to maintain the confidentiality of information and protect the personal data of its users. This data breach incident experienced by PT Bukalapak is not solely due to the malicious act of an employee (malicious insider), instead based on the Cyberthreat.id site, the Bukalapak site has been hacked by a professional hacker from Pakistan with pseudonym "Gnosticplayers". Based on this fact, the actual violation of privacy is indeed not carried out by an insider acting outside the company's code of conduct, but by a malicious outsider. Therefore, PT Bukalapak has implemented accountability by establishing business ethics and code of conduct that has also been adhered by all of the Company's organs and employees. Even so, the attitude given by one of the members of the board of directors to the company actually does not reflect the implementation of this accountability principle.

One of the members of the board of directors of PT Bukalapak has shown an attitude that underestimated the personal data breach that occured by stating that no important personal data has been obtained. Yet according to the Hacker News website, hackers admit to having stolen 13 (thirteen) million data users that is traded for 1,243 Bitcoin or equivalent to US $ 5,000 (five thousand United States dollars) (Terkini, https://makassar.terkini.id/ceo-bukalapak criticized-assume-trivial-leak-data, accessed on February 2nd, 2019). For this reason, this so called Director do not actually show an accountable attitude and responsibility for data breach cases that occur in accordance with applicable business ethics, whereas in this era of digital economy, protecting personal data is crucial, no matter how small personal data is misused, then it must still be categorized as an invasion of privacy and cannot be seen as a mild matter.

Therefore, it can be concluded that PT Bukalapak has applied the principle of accountability in GCG by compiling a code of conduct for the company in order to avoid malicious insider intending to hijack user's personal data, yet the attitude of one of the directors of PT Bukalapak does not reflect the implementation of this principle by acting as if this incident wasn't a big deal after all.

3) Principle of Responsibility

In essence, responsibility means the company's compliance with laws and regulations by carrying out its responsibilities to the society and the environment in order to achieve business sustainability in the long run as well as to gain recognition as a good corporate citizen (Effendi, 2016: 12). In the aspect of personal data protection, the laws and regulations that need to be considered and implemented by internet intermediary companies include:

a. Law No. 11 Year 2008 Concerning Electronic Information and Transactions (ITE Law 2008) as amended to Law Number 19 Year 2016 concerning Amendments to Law Number 11 Year 2008 concerning Electronic Information and Transactions (ITE Law);
b. Government Regulation No. 71 Year 2019 concerning Operation of Electronic Systems and Transactions (GR 71/2019).
c. Ministry of Communication and Information Technology Regulation No. 20 Year 2016 Concerning Protection of Personal Data in Electronic Systems (Ministry Regulation 20/2016).

In addition to the laws and regulations above, internet intermediary can also refer to the European Union's provision called the General Data Protection Regulation (GDPR) as the most modern and applicable international legal provisions concerning the protection of personal data. The provisions of GDPR that should be complied by the company in implementing personal data protection are regarding personal data protection principles written in Article 5 of GDPR, namely (ICO, 2019):

1) Lawfulness, fairness, and transparency (data processing should be done lawfully, fair, and transparent with the consent of the data subject);
2) Purpose limitation (data processing must be in accordance with company's original purpose);
3) Data minimisation (data processing must be adequate, relevant, and limited to its purpose);
4) Accuracy (data processing should be done accurately and updated if it's necessary);
5) Storage limitation (data storage must have a retention period of time);
6) Integrity and confidentiality (company must have measures to provide security in protecting the personal data which is stored);
7) Accountability principle (company should be responsible in relation

to every action taken against user's personal data and how company comply to other principles).

This responsibility principle is solely intended for companies to comply with statutory regulations (legal compliance). The principles of personal data protection have also been accomodated in Article 14 paragraph (1) GR 71/2019 with the following:

a. Collection of Personal Data is limited and specific, legally valid, fair, with the knowledge and consent of the owner of the Personal Data;
b. Processing of Personal Data is carried out according to its purpose;
c. Processing of Personal Data is done by guaranteeing the rights of the owner of the Personal Data;
d. Processing of Personal Data is done accurately, completely, not misleading, up to date, can be accounted for, and takes into account the purpose of processing Personal Data;
e. Processing of Personal Data is carried out by protecting the security of Personal Data from loss, misuse, unauthorized access and disclosure, as well as alteration or destruction of Personal Data;
f. Processing of Personal Data is done by notifying the purpose of the collection, processing activities, and failure of protection of Personal Data;
g. Processing of Personal Data is destroyed and/or deleted unless it is still in a retention period in accordance with the requirements based on statutory provisions.

Based on the description above, it is common for the principles of personal data protection to become the main foundation for internet intermediaries companies as providers of electronic systems in carrying out their obligations to protect personal data in order to meet the principles of responsibility in GCG. In addition, the obligations of electronic system providers in operating their electronic systems are also stipulated in Article 15 paragraph (1) and (2) ITE Law which reads:

(1) 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.

(2) Electronic System Providers shall be responsible for their Operation of Electronic Systems."

The stated article above does not explicitly describe the company's obligation to protect personal data, but it significantly illustrates the obligation of the electronic system provider to provide a reliable and secure electronic system, which "reliable" means that the electronic system has the ability to suit the needs of its use, while "safe" means that the system is physically and non-physically protected. That way, it can be said that

the electronic system must also have an adequate security system so that electronic information in it, such as personal data can be protected physically and non-physically.

In its application, PT Bukalapak has actually carried out the principles of personal data protection stipulated in Article 14 GR 71/2019, the results of the study below were actually taken based on the Privacy Policy compiled by PT Bukalapak with the following description:

a. First Principle: data collection conducted by PT Bukalapak is only limited to information such as name, e-mail, telephone number, address, gender, and photo ID. This data collection is also carried out with the consent and knowledge of the user.
b. Second Principle: the purpose of PT Bukalapak to process personal data is to improve the quality and service of Bukalapak in accordance with the applicable laws and regulations and based on the agreement of the data owner.
c. Third Principle: Personal Data processing by PT Bukalapak guarantees the rights of data subjects by means of PT Bukalapak is responsible for the Bukalapak System, including the protection and security of confidential personal data, notifying Users in the event of failure in protecting the privay of personal data at least through e-mail users registered with the System Bukalapak and report to law enforcement officials or Supervisory Agencies.
d. Fourth Principle: PT Bukalapak carries out accurate data processing by requesting the authentication and updating of User's personal data periodically, so that User data and information remain accurate, complete, and up to date.
e. Fifth Principle: PT Bukalapak conducts data processing by paying attention to the protection of the security of personal data by maintaining the confidentiality, integrity, and availability of the personal data it manages.
f. Sixth Principle: PT Bukalapak conducts data processing by notifying the initial purpose of data collection, how the processing activities. However, this principle has not been fully accommodated because PT Bukalapak did not notify users in the case of failure in protecting privacy of personal data.
g. Seventh Principle: PT Bukalapak erases the user's personal data in accordance with the provision that the User has the right to submit the deletion by stopping unsubscribe if he does not want to receive such information. For the deletion of personal information, Users can submit it through the OpenHelp feature by attaching a copy of the court's determination, proof of legal identity, and the reason for the removal request.

Thus, PT Bukalapak have fulfilled the principles of personal data protection in carrying out personal data processing. However, it cannot be denied that PT Bukalapak had been negligent in carrying out its legal obligations in the legislation. Looking back on the case of personal data leakage that occurred, a hacker from Pakistan claimed that he managed to break into 13 million Bukalapak accounts, where the data consists of names, usernames, e-mails, passwords, spending details, IP addresses, and others that are sold and enter the dark web market (Tribun News, 2019).

Based on the case above, besides not fulfilling the provisions in Article 15 paragraph (1) of the ITE Law, PT Bukalapak also violated other legal provisions such as Article 3 paragraph (1) GR 71/2019, Article 4 b GR 71/2019, Article 26 GR 71/2019, Article 28 b Ministry of Communication and Information Regulation No. 20 of 2016. Therefore, due to the fact that privacy violations had occured on Bukalapak's platform, it can be said that PT Bukalapak has not fulfilled the provisions of the laws and regulations as well as the principles of protection of personal data as a whole. In relation with the implementaion of responsibility principle in GCG, then it is clear that PT Bukalapak has not fulfilled its obligations as an electronic system provider as stated by the laws and regulations.

Thus, it can be concluded that the principle of responsibility in GCG has been fulfilled by internet intermediaries companies by processing personal data in accordance with the principles of personal data protection. However, its legal obligation as an electronic system provider in the form of providing a reliable and secure electronic system and maintaining the integrity and confidentiality of the user's personal data has not been manifested by PT Bukalapak due to misuse and breach of personal data by an irresponsible third party, therefore this principle has not yet been optimally fulfilled.

C. The Legal Liability of Internet Intermediary Company Regarding The Failure in Protecting Privacy of Personal Data in Indonesia

The legal relation between the electronic system provider and users ultimately create the rights and obligations that underlies a creation of a responsibility (Edmon Makarim, 2005.:368). Taking into account of the rapid development of technology and information, can actually gives birth to a variety of legal issues, everything that's related to the operation of electronic system must be responsible for overcoming damages. Regarding the responsibilities of the electronic system provider can be found in Article 15 ITE Law which regulates:

1) Every electronic system provider must provide a reliable and secure electronic system as well as being responsible towards the operation of the electronic system as it should be.
2) Electronic system provider is responsible towards the operation of their electronic system.

3) The provision as mentioned in paragraph (2) is not applicable in terms of a provable force majeures, errors, and/or negligence of electronic system users.

Which means, behind that responsibility, there must be a legal subject in the operation of the electronic system. This legal subject can be a person, business entity, government, or even the community that provides, manages, and/or operates an electronic system that is capable of being legally responsible for failures that occur in the operation of the electronic system (Article 1 paragraph 4 GR 71/2019). The failure that occurs in the operation of the electronic system can be components that are unable to work (hardware, software, data, procedures, and brainware) in the system as it should, activities that are unable to function (input, process, output, storage, communication) in the system as specified, and convergence that are enable to be maintained in the system (Carlo A. Gerungan, 2013: 48), as well as the failure towards personal data protection.

According to the previous explanation, a legal liability emerges for the reason that there is a legal relation between parties. Liability is the cause of one's freedom concerning their actions related to ethics and morals (Soekidjo Notoatmojo, 2010: 38). Liability in any case must have a basis, which is things that cause the appearance of legal rights for a person to sue another person to give their liability (Titik Triwulan and Shinta Febrian, 2010: 48). The liability in the operation of electronic system and transaction can be found in ITE Law. Every electronic system provider is obliged to provide a realible and secure electronic system also to be liable towards the operation of the electronic system as it should be, however this provision is not applicable in terms of a provable force majeure, failures, and/or negligence of internet users (Agus Santoso and Dyah Pratiwi, 2008: 84).

Edmon Makarim stated that the liability in the operation of electronic system is presumed liability, therefore if there occurs an error or failure in the electronic system, then the one who must prove the error is the electronic system provider for there is an ease of access towards the electronic system that's high-technology, not the user. Thus the appropriate principle to apply is the strict liability principle (Edmon Makarim, 2005: 172). The legal liability of Bukalapak as an internet intermediary company in the case of data breach is also based on the legal relationship between Bukalapak and the users as the data subjects. This legal relationship arises since the data subject declare their consent/agreement towards Bukalapak's privacy policy to conduct the processing of personal data.

In that agreement, besides the user agrees to the terms and conditions that applies in the privacy policy, Bukalapak also guarantees a protection towards every information the users give before using Bukalapak's services, including to maintain confidentiality, wholeness, and availability of personal data that is processed (Bukalapak's Privacy Policy). Ironically, Bukalapak still hasn't fulfilled their obligations as regulated in the laws and regulations

as well as the company's internal policy, which is to provide a secure and reliable system to be used by everyone. In addition, Bukalapak also haven't informed the users regarding the data breach that happened in their system.

One of the liability that can be given by Bukalapak is to measure the impact which user's obtained in the cause of failure in protecting privacy of personal data, whether there is a damage or not, both materially and imaterially. The legal effort that can be conducted by consumers or users if there's damage is to file a lawsuit towards the internet intermediary company as regulated in Article 38 paragraph 1 ITE Law that states:

> "*Any person may institute actions against parties that provide electronic system and/or using information technology to his/her detriment*."

This action (filing the lawsuit) is intended to request compensation for all losses perceived by consumers, including if there is a breach or misused personal data. The lawsuit as stated refers to Act Against The Law in Article 1365 BW with prominent elements i.e (Munir Fuady, 2002: 10-14):

a. There is an action;
b. That action is against the law;
c. There is an error from the perpetrator;
d. There is a loss for victims; and
e. There is a causaliy between the action and the loss.

In the context of Bukalapak's case, the mentioned company did not send any notification to the users concerning the data breach case that occured in the system. Therefore, the first element of Act Against The Law, that is there is an action, by not sending any notification to the users according to the mentioned period of time in Article 28 c Kominfo Regulation 20/2016 has been fulfilled. Furthermore, the action in the first element can be categorized as something against the law if the second element is fulfilled with the following provisions (Rosa Agustina, 2012: 8-9):

a. Against one's subjective right;
b. Against the legal obligation;
c. Against decency;
d. Against appropriateness, accuracy, and prudence

Back to the data breach case, Bukalapak accordingly has fulfilled the second element which is in the "against the legal obligation" category, for the reason which has been deciphered before, Bukalapak has the legal obligation to provide a reliable and secure electronic system to be used (Article 15 (1) ITE Law, Article 3 (1) GR 71/2019, and Article 28 b Kominfo Regulation 20/2016). And then if there is a failure in protecting privacy of personal data in the electronic system, then Bukalapak as the electronic system provider must initiate a written notification to the users no later then 14 days after the data breach occured (Article 28 c Kominfo Regulation 20/2016). Therefore, the second element has been fulfilled.

Furthermore, the third element is error. For the reason that the liability in implementing the electronic system is strict liability, so the Plaintiff, in this case the user of the electronic system, may not required to prove this element in court, because it is very clear that the failure occured in the platform, is because of the company's negligence to obey the legal obligation to provide a reliable and secure electronic system to be used by internet users and the negligence to send notification about the data breach.

The fourth element is indeed the element that needs to be deciphered in writing the lawsuit, because Article 1365 BW regulates the legal obligation of the perpetrator is to give compensation to the victims (Rosa Agustina, 2012: 10). In addition, Moegni Djodjodirjo gave his opinion about the types of compensation, which is compensation in the form of money and compensation in the form of returning to its original state (Moegni Djodjodirjo, 1982: 102). Thomas Clooney also had categorized the types of right that needs to be protected in tort law, one of them is the right to be let alone, for the reason that the loss caused by invasion of privacy does not emerge from a violation of obligation, but can be caused by mocks, fear, or a disturbance of peace in one's life, therefore this right must have a legal protection (Thomas Clooney, 1880: 29).

In casu, the loss that is suffered by users is in the form of imateriil loss that cannot be measured by money, which is the lost of the privacy right itself because their personal data has been robbed and traded freely. Nevertheless, Bukalapak should just inform the users immediately concerning the data breach that has occured so that users can take action themselves to decrease the probability of loss, such as changing their password or temporary disabling their account. Therefore, this element has been fulfilled. The future of privacy protection remains an open question. Justices Scalia and Thomas, for example, are not inclined to protect privacy beyond those cases raising claims based on specific Bill of Rights guarantees. The public, however, wants a Constitution that fills privacy gaps and prevents an overreaching Congress from telling the American people who they must marry, how many children they can have, or when they must go to bed (Tejomurti, K. 2017: 66).

The last element is the causality between the error and loss perceived. In this issue, the failure in providing a reliable and electronic system, as well as informing the users about the data breach experienced in Bukalapak's system has definitely caused loss which is invasion of privacy right of the hijacked and traded personal data by third party. As a result, it is clearly possible if users want to file a lawsuit towards PT Bukalapak in this data breach case, because users has the right to do so in accordance to protect their personal data.

Apart from giving compensation, the legal liability of internet intermediary company in Indonesia in the case of privacy invasion of personal data refers back to Article 100 paragraph (1) dan (2) GR 71/2019

which stipulates that if an electronic system provider does not fulfill the provisions in Article 4, Article 14 paragraph (1), and Article 26 paragraph (1) will be subjected to administrative sanctions which include written warnings, administrative fines, temporary termination, termination of access, or exclusion from the list. The administrative sanctions imposed by the Ministry in accordance with statutory provisions, are carried out in coordination with the instructions from the Ministry of related institution, also the imposition of administrative sanctions will not eliminate the criminal or civil liability.

The application of a deterrent effect can be possible. Given the case of privacy invasion that befell Facebook some time ago, Facebook made amends as a form of its liability by paying fines of US$ 5M (five million US dollars) or around Rp70 T (seventy trillion rupiah) (Wahyu Prihastomo, 2018). The fine was imposed by the FTC as the United States' federal trade commission that guarantees privacy protection of personal data on internet intermediary companies in the United States. Such huge fines were imposed because Facebook was found to be negligent in protecting privacy and user's personal data, which was later leaked and used by irresponsible third parties. Besides being negligent, Facebook was found to take advantage of user's phone number for advertising interests and to misuse the face recognition system on the platform (Kompas, 2018). Not just that, the FTC also requires Facebook to improve and update the latest security systems and privacy mechanisms that are more transparent. One of them is by creating a mechanism to review user's privacy across all products created by Facebook, both the latest software, policies, services, and even systems on the platform. But from the Facebook case above, there is a possibility that Indonesia can apply a deterrent effect in the form of imposing fines for companies that do not carry out their legal obligations to provide personal data protection as a form of legal liability.

In conclusion, if we contextualized with the case of Bukalapak as an internet intermediary compay that provides an e-commerce platform, then for now the legal liability that can be given by Bukalapak is to give compensation to consumers as long as there is a lawsuit for data breach on the electronic system that causes loss, as well as with administrative sanctions that can be imposed by the Government c.q. the Ministry of Communication and Information as stipulated in Article 100 GR 71/2019.

III. Conclusion

1. PT Bukalapak in carrying out its role as an agent of economic activity has implemented the principles of Good Corporate Governance in order to maintain business continuity in the long run, particularly the principles relating to the protection of personal data, namely the principles of transparency, accountability, and responsibility. However, the application was not optimal, because PT Bukalapak still did not transparently notify the data leakage that

occurred, PT Bukalapak also did not comply with its obligations as the provider of the electronic system and the principles of personal data protection as stated in the legislation.

2. The legal liability that can be given by internet intermediary companies for privacy violations in Indonesia currently still refers to the ITE Law, GR 71/2019, and Ministry of Communication and Information Regulation 20/2016, which is to bestow compensation to victims and carry out administrative sanctions as regulated by statutory regulations.

IV. Recommendation

1. The internet intermediaries as electronic system providers have the responsibility of failure in protecting the privacy of user's personal data. Therefore, it is recommended that companies have to implement optimally the principles of GCG, especially the principles of transparency, accountability, and responsibility, such as immediately notifying users concerning personal data breaches that occur through e-mail notifications, being assertive and fast to increase the level of security in the system, and comply with its obligations determined by legislation by taking into account the principles of good personal data protection as stipulated in GR 71/2019 and Ministry Communication and Information Regulation 20/2016.
2. Personal data breach cases in the era of digital economy are now increasing, thus it is recommended that the Government of the Republic of Indonesia and Parlements should discuss the Draft of Personal Data Protection Law which can give a legal protection that guarantees the protection of citizen's privacy right.

BIBLIOGRAPHY:

Books:

Adrian Sutedi. 2011. *Good Corporate Governance*. Jakarta: Sinar Grafika.

Arthur R Miller. 1971. *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor: University of Michigan Press.

Edmon Makarim. 2005. *Pengantar Hukum Telematika*, Jakarta: PT Raja Grafindo Persada.

_____. 2005. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Jakarta: Raja Grafindo Persada.

Iman Sjahputra Tunggal dan Amin Widjaja. 2002. *Membangun Good Corporate Governance*. Jakarta: Harvarindo.

Moegni Djojodirgo. 1982. Perbuatan Melawan Hukum, Jakarta: Pradnya Paramita.

Muh. Arief Effendi. 2009. The Power of Corporate Governance: Teori dan Implementasi, Jakarta: Salemba Empat.

Munir Fuady. 2002. Perbuatan Melawan Hukum: Pendekatan Kontemporer. Bandung: PT Citra Aditya Bakti.

Rosa Agustina. 2012. Hukum Perikatan (Law of Obligations). Denpasar: Pustaka Lasaran.

Sinta Dewi. 2015. Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional. Bandung: Refika Aditama.

Journals:

Agus Santoso dan Dyah Pratiwi. (2008) "Tanggung Jawab Penyelenggara Sistem Elektronik Perbankan dalam Kegiatan Transaksi Elektronik Pasca Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik", Jurnal Legislasi Indonesia Vol. 5 No. 4, December 2008.

Ahmad Syakhroza. (2002). Best Practice Good Corporate Governance dalam Konteks Kondisi Lokal Perbankan Indonesia. Manajemen Usahawan Indonesia No.06, June.

Carlo A Gerungan. (2013). "Tanggung Jawab Penyelenggara Sistem Informasi jika Terjadi Kegagalan Sistem", Jurnal Hukum Vol. XXI No.4, April-June.

Jojok Dwiridotjahjono. (2009). "Penerapan Good Corporate Governance: Manfaat dan Tantangan serta Kesempatan bagi Perusahaan Publik di Indonesia". Jurnal Administrasi Bisnis Vol. 5 No. 2, Bandung, Universitas Parahyangan.

Sinta Dewi. (2018). "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia", Jurnal Hukum Volume 4 No. 1, Universitas Padjadjaran.

Tejomurti, K. (2017). The Personal Electronic Data Security on The Implementation of Solo Smart City According to The Perpective of Privacy Protection Law. *Journal of Law, Policy, and Globalization*, *66*.

Thomas S. Kaihatu. (2006). "Good Corporate Governance dan Penerapannya di Indonesia", Jurnal Ekonomi Manajemen dan Kewirausahaan Vol. 8 No. 1, Fakultas Ekonomi, Universitas Kristen Petra, March.

Website:

"13 Juta Data Pengguna Bukalapak Bocor dan Dijual" https://technologue.id/13-juta-data-pengguna-bukalapak-bocor-dan-dijual/amp/ diakses accessed on June 21st 2020.

"Persiapkan Organisasi Anda untuk Menghadapi GDPR", http://www.phintraco.com/persiapkan-organisasi-anda-untuk-menghadapi-gdpr/ accessed on January 25th 2020.

Asih Reta Wening Surya, "Peran Pelaku Kegiatan Ekonomi", (Surakarta, 2017). https://docplayer.info/58406295-Peran-pelaku-kegiatan-ekonomi.html accessed on January 10th 2020.