ACTIVA YURIS
Volume 1 Nomor 1 Februari 2021
E-ISSN: 2775-6211
DOI: http://doi.org/10.25273/ay.v1i1.8677
Website: http://e-journal.unipma.ac.id/index.php/AY

Liability of Marketplace as Electronic System Provider in Regard to System Failure Occured on Online Transactions

Emmy Febriani Thalib[1], Ni Putu Suci Meinarni[2*]

[1] *STMIK STIKOM Indonesia, Denpasar, Bali, Indonesia*
[2] *STMIK STIKOM Indonesia, Denpasar, Bali, Indonesia*
**Corresponding author: sucimeinarni@stiki-indonesia.ac.id*

Abstract

Digital transaction activities in community activities have increased due to the accelerated adoption of digitalization in Indonesia but it also has potential problems in the future such as many frauds and even crimes that often occur in cyberspace so that they tend to harm consumers or users. The liability of electronic system provider in regard to the system failure occurrence on online transaction uses a normative research method using a statutory approach and an analytical approach to legal concepts. However based on the research The existence of current regulations concerning Electronic Information and Transactions in conjunction with Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions the liability in the case of system failure that causes losses to the other party, is not explicitly stated there does not contain elements of criminal sanctions as a consequence for indemnity for Electronic System Provider, the existing regulation only regulate the administrative sanction. The protection provided in Article 26 of the ITE Law to parties who suffer losses due to the actions or inaction of the electronic system administrators can only be pursued in a civil law.

Keywords: *liability; Electronic System; Provider Sytem; Online Transaction;*

History:
Received: February 13th 2021
Accepted: February 20th 2021
Published: February 26th 2021

Publisher: Universitas PGRI Madiun

Introduction

Even though we know that the internet is an innovation that can support today's daily activities, and provide tremendous efficiency and effectiveness impacts. It cannot be ignored the impacts that exist on social and other aspects arising from the emergence of this technology are also growing. The Covid-19 pandemic prompted the government to begin implementing Large-Scale Social Restrictions (*PSBB*) starting in March 2020. In various areas, many shops and malls have stopped their business activities to prevent the spread of the virus. The pattern of transactions in society has also changed from what previously people carried out conventional shopping activities by meeting each other face to face to shopping and transacting online. Although Covid-19 has greatly reduced physical activity, in other hand it has also made online sales growing up dramatically. Apart from this, developments and increasingly advanced technology with easy access are also major factors in the growth of online transactions.

The phenomenon of Industry 4.0 is also associated with the Industry / Internet of Things, which is the most discussed issue in the industrial business concept in recent years. General Electric (GE) uses the term "Industrial Internet" to refer to the Industrial Internet of

Things, Cisco uses the term "internet of everything ~ while others call it Internet 4.0 and so on (Samudra, n.d.).

Meanwhile, rising together with this phenomenon, there is a new way of digital transaction called Marketplace. Marketplace is an activity to provide a place of business activity in the form of an internet shop in an internet mall as a place for online sellers to sell their products (Sakti, 2014). In Indonesia itself, Marketplace system is very suitable with the society's lifestyle. The marketplace has answered the need of society in this era.

According to a report compiled by the Indonesian Central Statistics Agency (*Biro Pusat Statistik),* online sales during this pandemic have actually jumped sharply when compared to sales in January 2020. In March 2020, online sales jumped 320% of the total online sales at the beginning of the year. The gain was getting sharper, online sales in April 2020 were recorded to have increased 480% from January 2020.(kontan.id, 2020)

The Principal Economist Payment System Policy Department of Bank Indonesia stated that the value of e-commerce transactions has increased because Indonesia has 338.2 million mobile customers, 175.4 million internet users, and 160 million active social media users. Based on data by Bank Indonesia states that e-commerce transactions in August 2020 rose to Rp 140 million compared to last year's 80 million transactions and August 2018, which was 40 million transactions (Tempo, 2020).

In the era of the Covid-19 pandemic, the digitalization trend in Indonesia is growing rapidly through changes in people's behavior. Digital transaction activities in community activities have increased due to the accelerated adoption of digitalization in Indonesia in the era of the Covid-19 pandemic. Even though online transactions make it easy for consumers, this also has potential problems in the future such as many frauds and even crimes that often occur in cyberspace so that they tend to harm consumers or users. Common problems when shopping online include both technical and non-technical aspects, such as: additional costs, product quality, digital payments, security aspects, delivery process, returns of goods. Online fraud is becoming another major hindrance to the development and use of commercial activities on the Internet. The incidence of fraud is reported as being 20 times higher in online trades than in offline trades (Gavish, 2006).

The Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions Law (The ITE Law) is seen as an administrative law. (*UU Informasi Dan Transaksi Elektronik*, 2016) However, even administrative laws carry the threat of criminal sanctions as *ultimum remedium* if there is a violation of the provisions of the law and all efforts to overcome them have been made. The ITE Law exists to accommodate the needs of business people in the world of convergence of information, communication technology or telematics, and the general public to obtain legal certainty in conducting electronic transactions. Article 15 paragraph (1) of The ITE Law has mandated every electronic system operator to maintain its electronic system reliably and safely as well as responsible for the operation of electronic systems as appropriate. Every transaction carries a risk. Risk in electronic transactions can come from humans, nature, or the system itself. The problem is who manages this risk and who is responsible if the risk occurs.

Regulated in Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems (GR 71) and Transactions (*Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions*, 2019), which revokes Government Regulation No. 82 of 2012 on the same subject, it is stated that the electronic system operator is responsible for the operator of the electronic system, unless it can be proven that there is a state of force, error and negligence on the part of the Electronic System user. The use of technology in the marketplace is overshadowed by the potential risk of system failure and / or the risk of electronic crime (cybercrime) committed by irresponsible people. System

failure can be caused due to system damage (such as a server down), and on a large scale it can be caused by natural disasters or such as halting of part or all of the functions of an Electronic System which is essential so that the Electronic System does not function properly. Forcing, errors and negligence on the part of Electronic System users, it may be that the electronic transaction provider / marketplace is not responsible for the indemnity especially if there is a system failure / failure that causes loss to other parties, it is not explicitly stated. This of course raises legal problems including the extent of the responsibility of the electronic system provider / market place in online transactions, especially when there is damage / failure of the system and dispute resolution when there is a legal problem.

Based on the background of these problems, the researcher is interested in conducting research with the problem with the title liability of marketplace as electronic system provider in regard to system failure occurred on online transactions.

Materials and Methods

The legal materials used are primary legal materials in the form of statutory regulations, secondary legal materials in the form of literature related to the problem (Soekanto, 2012). This study also uses descriptive methods in order to provide an overview or shadow of the object to obtain information. All legal materials are collected based on the topic of the problem which has been formulated and analyzed descriptively. In order to complete a scientific research, an appropriate method of approach is needed in accordance with predetermined problems. The approach to the problem chosen in this study is a normative juridical approach. Based on this approach, a positive legal inventory is a preliminary activity to the entire research process. In this research, legal material is needed to study the basic notions contained in the legal system.

Results and Discussion

Refer to Article 1 (4) GR 71, Electronic system operator is any person, state administrator, Business Entity, and society who provides, manages, and / or operates electronic systems individually or jointly to system users. Electronics for his own needs and / or the needs of other parties.

The legal basis for Electronic System Operators includes, among others:

a) Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning ITE;
b) Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions;
c) Regulation of the Minister of Communication and Information Number 36 of 2014 concerning Registration Procedures for Electronic System Operators;

Meanwhile, the meaning of electronic transactions as described in Article 1 number GR 71 is Electronic Transactions are legal acts carried out using computers, computer networks, and / or other electronic media. The operators of this electronic system consist of electronic system operators in the public and private sphere. Meanwhile, operators of electronic systems in the private sphere include operators that are regulated or supervised by ministries or agencies based on the provisions of laws and regulations and operators who have portals, websites or applications in the network via the internet that are used for:

1) Provide, manage, and / or operate the offer and / or trade in goods and / or services;
2) Provide, manage, and / or operate financial transaction services;

3) Delivery of paid digital material or content via the data network by means of downloading via a portal or website, sending via electronic mail, or via other applications to the user's device;
4) Provide, manage and / or operate communication services including but not limited to short messages, voice calls, video calls, electronic mail, and online conversations in the form of digital platforms, networking services and social media;
5) Search engine services, services for providing electronic information in the form of text, sound, images, animation, music, videos, films and games or a combination of part and / or all of them; and / or
6) Processing personal data for operational activities serving the public related to electronic transaction activities.

Based on the provisions of this article, marketplace providers can be categorized as operators of private electronic systems that carry out electronic transactions between sellers and buyers.

In Article 4 GR 71 as long as no separate law is stipulated, every Electronic System Operator is obliged to operate an Electronic System that meets the following minimum requirements:

a) Able to redisplay Electronic Information and / or Electronic Documents in full in accordance with the retention period stipulated by laws and regulations;
b) Able to protect the availability, integrity, authenticity, confidentiality and accessibility of Electronic Information in the operation of such Electronic Systems;
c) Able to operate in accordance with procedures or instructions in the operation of the Electronic System;
d) Equipped with procedures or instructions that are announced in a language, information, or symbols that can be understood by the party concerned with the operation of the Electronic System;
e) Have a continuous mechanism to maintain the novelty, clarity and accountability of procedures or instructions.

Good management and security in the operation of an electronic system are very necessary. In addition to fulfilling user trust, using electronic transactions Electronic systems have the potential to become an important pillar of the economy with the existence of e-commerce (Neama et al, 2016). Neama et al explain about electronic system administrators who must develop and apply the precautionary principle:

> *" Due to such growth, businesses owners should realize that it is vital to improve online services provided to their customers. Currently, many companies are gathering customers' information (eg, name, address, interest, etc.) through registration, online transactions, or cookies in order to achieve such improvement in provided services …Privacy and security concerns are the major barriers from adopting e-commerce services."*

GR 71 states the obligations of Electronic System Provider. As in Article 4, the operation of electronic systems includes aspects of security. Information has strategic-economic value, so it needs to be protected. However, in practice, information leaks can occur, either because the system has a bug that causes it, there is no proper security, a system that has not been properly managed or because of someone's legal action. The information data leakage should not have been caused by the electronic system provider. How to ensure that these leaks are not caused by electronic system provider is something that must be pursued. Explicit or implicit reluctance or refusal to do so must be punished. The roles in the implementation of electronic systems in information and communication technology media can be described as follows: (Samudra, n.d.)

a) Network operators: provide technical facilities for information transmission;

b) Access provider: provides access to the internet to users;
c) Search engines (Search Engines): online tools used to search web pages such as Yahoo!, AltaVista, Google, etc. There are two types of search engines, namely automatic search engines, and search engines that rely on user reviews and web site catalogs.
d) Hosting service provider (Host seNice provider): a party that provides web storage and services or security for individuals, including renting site content, creating site security, and uploading content, such as software, text, graphics, or sound. Hosting services include online information exchange, such as bulletin boards and chat rooms.

Written is usually stated in an agreement signed by the parties concerned. The signature proves that a person binds himself to the clauses set out in the agreement.

In the cyber world, deals and agreement occur electronically. The ITE Law recognizes electronic transactions set forth in electronic contracts that bind the parties (vide Article 18 paragraph (1). The question is when an electronic transaction conducted via the internet occurs. Under Article 20 of the ITE Law, an electronic transaction occurs when the transaction offer sent by the sender is received and approved by the recipient. However, such consent must be made by means of an electronic acceptance statement (for example by sending a confirmation email).

Article 20 of the ITE Law is the conception of the regulation of the civil law legal system adopted by mainland Europe. The party providing the offer (sender) is the party who advertises goods / services via the internet (for example amazon.com). Regarding this matter, in the common law (continental Europe) legal system, there are regulations regarding invitations to trade concerning actors in electronic transactions. However, invitation to trade in the common law legal system regulates the opposite, namely that the party who is considered to be offering an offer is a prospective buyer of goods / services, and the recipient is the party advertising goods / services on the internet (amazon.com). With regard to borderless electronic transactions. Thus, it is necessary to pay attention to the parties who will transact along with the legal system that will be enforced, because it will be related to legal consequences. In this regard, the ITE Law regulates choice of law, namely that the parties have the authority to choose the law that applies to international electronic transactions they make. If the parties do not make a choice of law in international electronic transactions, the applicable law is based on the principles of international civil law (vide Article 18 paragraph (2) and paragraph (3) of the ITE Law).

Article 20 of the ITE Law in relation to parties conducting electronic transaction activities stipulates that the sender or receiver can carry out electronic transactions on their own, through the party damaged by them, or through an electronic agent. In this case the parties responsible for all legal consequences in the implementation of electronic transactions are: (Santoso, 2008)

1) If done alone, all legal consequences in conducting electronic transactions are the responsibility of the transacting parties.
2) If it is done through the granting of power of attorney, all legal consequences in the conduct of electronic transactions shall be the responsibility of the grantor.
3) If done through an electronic agent, all legal consequences in implementing electronic transactions are the responsibility of the electronic agent operator.
4) If done through an electronic agent, all legal consequences in implementing electronic transactions are the responsibility of the electronic agent operator.
5) If the loss of electronic transactions is due to the failure of the operation of the electronic agent due to the actions of a third party directly against the electronic system, all legal consequences are the responsibility of the electronic agent operator.

However, if the loss of electronic transactions is due to the failure of the operation of the electronic agent due to the negligence of the service user, all legal consequences are the responsibility of the service user. This provision does not apply in the event that it can be proven that there is a force, error, and / or negligence on the part of the electronic system user.

Edmond Makarim in his book introduction to Telematics Law states several principles of the responsibility of business actors in law which are differentiated as follows: (Makarim, 2003)

1. The principle of responsibility based on the element of error (fault liability / liability based on fault).
   This principle states that a person can only be held accountable legally if there is an element of wrongdoing. This principle is reflected in the provisions of Articles 1365, 1366 and 1367 of the Civil Code. Article 1365 of the Civil Code requires that there are 4 (four) main elements to be held accountable in an act against the law, namely the existence of an act, an element of guilt, loss suffered, and a causal relationship between error and loss. There are 4 elements of an act categorized as an act against the law. law, namely:
   a. The act is against the rights of others
   b. Contrary to its own legal obligations
   c. Contrary to decency
   d. Contrary to the requirements that must be heeded in the community.
   With regard to this principle, the issue will arise regarding the "legal subject of the offender" (Article 1367 of the Civil Code). In legal doctrine, there is a vicorious liability and corporate liability. Vicorious liablity is responsibility for the mistakes of people who are under the supervision of the employer. If that person is transferred to the control of another party, then the responsibility is also transferred to that other party. Meanwhile, corporate liability emphasizes the responsibility of the institution / corporation to the workers it employs.
2. The Presumption of Liability Principle
   This principle states that the defendant is always held responsible until he can prove his innocence (reverse proof). Article 22 of the Consumer Protection Law confirms that the burden of proof (whether there is an error) lies with the business actor in a criminal case of violating Article 19 paragraph (4), Article 20, and Article 21 of the Consumer Protection Law.
3. The Principle of Presumption not to Always be Responsible
   This principle is the opposite of the second principle and is known only in a very limited scope of transactions which in common sense can be justified. For example, someone who drinks water at a river without boiling it first, if he is sick, he cannot sue the factory located around the river. He should have boiled the water first.
4. The principle of absolute responsibility (strict liability).
   This principle stipulates that an action can be punished on the basis of harmful conduct without questioning whether there is intention or negligence. This principle emphasizes the causal relationship between the responsible subject and the mistakes it makes, by taking into account the existence of force majeure as a factor that can escape from responsibility. Regarding the doctrine of strict liability, one example of its adherents is Britain. Adhering to the principle of "*actus non tacit reum nisi mens sit rea*" this doctrine adheres to the principle of absolute responsibility without having to prove whether or not there is an element of guilt in the perpetrator of a criminal act.
5. Responsibility principle with restrictions

This principle is often used by business actors to limit the burden of responsibility that should be borne by them, which is generally known as the inclusion of an econary clause in the standard agreement they make. Thus, it can be concluded that the forms of responsibility of business actors are contained in Law No. 8 1999. Concerning Consumer Protection are as follows:

a) Contractual liability: Namely, civil liability based on an agreement or contract from a business actor for losses suffered by consumers as a result of consuming goods and / or services produced or utilizing the services it provides.
b) Product liability: It is the direct civil responsibility (strict liability) of business actors for the losses suffered by consumers due to using the products they produce. This accountability is applied in the event that there is no privity of contract between business actors and consumers.
c) Professional liability: In the event that the agreement relationship is a measurable achievement so that it is an outcome agreement, the responsibility of the business actor is based on professional accountabilityuse the civil liability for the agreement / contract (contractual liability) of the business actor as the service provider for the losses experienced by consumers.
d) Criminal liablity: In the relationship between business actors and the state in maintaining public security, the responsibility of business actors is based on criminal liability. Regarding the responsibility of information system operators, Article 28 states that Electronic System Provider are responsible for the security and protection of Electronic System facilities and infrastructure. If there is a failure of an information system which results in the system not running properly, then of course there will be a loss both material and immaterial which most likely will not only be suffered by the organizer directly but also by third parties as users.

As a consequence, there will be a legal liability for claims for compensation due to damage or failure to the system. The existence of a computer-based information system will refer to three important things, namely: (Gerungan, 2013)

a. The existence of the components it uses
b. Continuity of predetermined function activities
c. The integrated nature of all these things.

To see any damage or failure to an information system, also we should look at three points as below:

a. The components (hardware, software, data, procedures and brainware) are not working as expected in the system;
b. The failure of all functional activities (input, process, output, storage, communicate) in the system as determined;
c. The nature of integrity (integration) is not maintained in the system. In this connection, the failure is basically caused by three things that cause malfunction, namely: hardware malfunctioning properly; or non-functioning instruction codes in the software as specified, including (i) programming errors that have a direct impact on the physical process (software produces incorrect information which feeds directly into a physical process), or (ii) program errors that produce information that is not as expected (software produces incorrect information which is relied on by human mind).

To determine these liability, it can be determined based on:

a) Contract / agreement of the parties Liability under the contract will look at the existence of clauses in the contract, such as a contract for the sale or supply of

equipment, a contract for the provision of services, or a license contract for software use.

b) The responsibility based on the provisions in the law which is also known as an act against the law, can be seen at: product responsibility due to defective products (defective product) and liability for negligence that results in damage to property or bodily injury, or negligence that results in financial loss, including consequential losses due to unusable software or losses due to reliance on information produced by an incorrect software.

Conclusion

Currently, the ITE Law and its derivative regulations have become the legal umbrella for the implementation of electronic transaction activities, however, what kind of legal liability and principles of liability are adopted in determining these responsibilities are carried out by the party providing electronic transactions / marketplace in the event of a system failure / failure that causes losses to other parties are not explicitly stated, it can be seen that failure to comply with the obligations as stipulated in the ITE Law, intentionally or negligently, does not contain elements of criminal sanctions as a consequence. The protection provided in Article 26 of the ITE Law to parties who suffer losses due to the actions or inaction of the electronic system administrators can only be pursued in a civil law. GR71 only regulates administrative sanctions. In Article 58 point (3) GR71 it is stated that the responsibility of evidence for intentional or negligent acts committed by parties who are not Indonesian Electronic Certification Providers shall be the responsibility of the person, business entity or agency that has suffered a loss. In the context of implementing an electronic system, Article 15 and Article 16 of the ITE Law, provide a presumed liability principle because it is impossible for the user to prove the errors that occur in the usually high-tech system.

Acknowledgments

We would like to extend our sincere thanks to our institution STMIK STIKOM Indonesia as a home base where we belong. Especially the research department, LPPM (*Lembaga Penelitian dan Pengabdian*) STMIK STIKOM Indonesia for the biggest support in developing our research skill.

References

Regulation

Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions

Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, (2019) (testimony of Republic of Indonesia).

Books

Gavish, B. C. L. T. (2006). *Fraudulent auctions on the Internet*. https://doi.org/https://doi.org/10.1007/s10660-006-6954-0

Gerungan, C. A. (2013). Tanggungjawab penyelenggara sistem informasi jika terjadi kegagalan system. *Jurnal Hukum UNSRAT*, *XXI*(4). https://media.neliti.com/media/publications/885-ID-tanggungjawab-penyelenggara-sistem-informasi-jika-terjadi-kegagalan-sistem.pdf

Kontan.ID. (2020). *BPS catat penjualan online melonjak tajam selama pandemi corona*. 2 Juni 2020. https://nasional.kontan.co.id/news/bps-catat-penjualan-online-melonjak-tajam-selama-pandemi-corona

MAKARIM, E. (2003). *Pengantar Hukum Telematika Suatu Kompilasi Kajian*. Badan Penerbit FHUI.

Neama, Ghadeer, Rana Alaskar, and M. A. (2016). Privacy, Security, Risk, and Trust Concerns in e-Commerce. *Proceedings of the 17th International Conference on Distributed Computing and Networking*. https://doi.org/https://doi.org/10.1145/2833312.2850445

Sakti, N. W. (2014). *Buku Pintar Pajak E-commerce Dari Mendaftar Sampai Membayar Pajak*. Visimedia.

Samudra, A. H. (n.d.). *Liability Korporasi Pengelola Sistem Elektronik & Delik terkait Penyelenggaraan Sistem Elektronik di Era Industri 4.0* (Perspektif). Genta Publishing.

Santoso, A. & D. P. (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*, *5*(4).

Soekanto, S. (2012). *Pengantar Penelitian Hukum*. Universitas Indonesia Press.

Tempo, B. (2020). *Bank Indonesia: Transaksi E-Commerce Agustus 2020 Naik hingga Mencapai 140 Juta*. 21 Oktober 2020. https://bisnis.tempo.co/read/1398066/bank-indonesia-transaksi-e-commerce-agustus-2020-naik-hingga-mencapai-140-juta