

“COMPARATIVE STUDY ON ONLINE INTERMEDIARY SERVICE PROVIDER IN INDONESIA AND EUROPEAN UNION”

Steven Leonardi¹, Abdul Gani Abdullah², Amad Sudiro³

¹Doctoral Program in Law, Faculty of Law, Tarumanagara University, Jakarta, Indonesia ²Professor at Faculty of Law, Tarumanagara University, Jakarta, Indonesia ³Professor at Faculty of Law, Tarumanagara University, Jakarta, Indonesia email: leonardisteven791@gmail.com

ABSTRACT:

By giving exemption of liability of online intermediary services for Indonesia, it is also expected to create one comprehensive and codified regulation applied only for the general internet regime, or possibly only for online intermediary services. The current overlapping creates multiple impositions of rules. Online intermediary services providers are meant to only provide a platform or media for users to use the platform. This research aims to compare the online intermediary service provide between Indonesia and European Union. This a normative legal research using secondary data. The analysis was conducted using a qualitative approach. Results and discussion found that the E.U. E-Commerce Directive 2000/31 could be a reference for the Indonesian government to improve its regulations regarding e-commerce, especially in the online intermediary services provider. However, to adopt the E-Commerce Directive 2000/31 especially articles 12 to 14, where the exemption of liability is regulated, it needs some adjustment to be suitable for the Indonesian legal system and culture.

Keywords:

Exemption of liability, E-Commerce Directive, Online intermediary Service Provider, Comparative Study

Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

INTRODUCTION

Online services have become a new trend in Indonesia in recent years. There are several forms of online services, i.e., business to business (B2B), business to consumer (B2C), and consumer to consumer (C2C). The online intermediary service provider provides services for people to advertise their goods and services (VanHoose, 2013). In Indonesia, the increasing number of online intermediary services provider has been followed by an increase in the number of cases. Due to the internet characteristics, such as a high degree of anonymity, incomplete legal constraints, and lower entry and exit barriers, it is more challenging to handle fraud in the online intermediary services provider (Dong et al., 2012). The current regulations on commercial electronic activities in Indonesia are:

- a. Law No. 11 of 2008 on Information and Electronic Transaction;
- b. Government Regulation No. 82 of 2012 on Operation of Electronic System and Transaction;

- c. Law No. 7 of 2014 on Trades; and
- d. Government Regulation No. 80 of 2019 on Trades via Electronic System (GR 80/2019).

The recent addition of the Indonesian Government Regulation No. 80 of 2019 on Trades via Electronic System has incorporated a particular exemption of liability for online intermediary services. However, it is still inadequate to accommodate the interest of the stakeholders.

Meanwhile, in the European Union, a regulatory framework for intermediary service providers is based on section four articles 12 to 15 of Directive 2000/31/E.C. of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (E-commerce Directive). This Directive is implemented in the laws of the Member States. The E-commerce Directive has been proven to effectively regulate the exemption from intermediary service provider liability, like online intermediary services provider, due to its rapid development through case law. Therefore, it can be a reason for Indonesia to compare and adopt

the principle of exemption from intermediary service provider liability for online intermediary services providers in the interest of legal development.

THEORETICAL CONCEPT

The European Commission believed that the diverse approach that was set up by the various national regimes is not suitable to establish a flourishing online market place. The same method should be applied in all Member States to protect all citizens. Therefore, the E-Commerce directive 2000/31 was introduced to harmonize the Member States' legal regime (Schellekens, 2011). By enacting this Directive, online intermediary services providers are expected to have the same obligations in all Member States. This Directive creates incentives for online business development by establishing several protections for Providers of online intermediary services. The Directive focuses on services instead of the crime or infringement (Edwards and Waelde, 2005). By complying with several services, an online intermediary services providers will be exempted from being liable (Bistrochi, 2003). Those special liability regimes are described as follows:

2.1 Mere Conduit

There are two types of "Mere Conduit" services under Article 12 of the E-Commerce Directive, which is "transmission in a communication network of information provided by a recipient of the service" and "provision of access to a communication network." There are several requirements to be protected under this provision. The first requirement is that the service providers must be passively involved by not initiating data transmission. The second requirement is that the service provider cannot decide to whom the information is sent. Lastly, the service provider is not allowed to interfere with the information by selecting or modifying it. An exception for manipulation is allowed for technical nature in the transmission. It does not alter the integrity of the information contained in the transmission. Hence,

the provider has neither knowledge of nor control over the information which is transmitted or stored.

Article 12 (2) gives the scope of transmission and access that are intended in paragraph 1. The information transmitted in a network that goes from computer to computer is stored for a temporal time. The duration of the temporary storage functionality should only be as long as is necessary for the transmission. A computer system must automatically perform this functionality during the transmission process. Despite these previous requirements, a court or administration authority can ask for an injunction requiring the service provider to terminate or prevent an infringement.

Aside from all these protections for "Mere Conduit" services, the Directive still contains several ambiguities. First, it is regarding the scope of a communication network. Due to the lack of a communication network definition, many parties, such as operators of chat networks, instant messaging networks, or peer-to-peer networks, may argue that they provide access to a communication network. It may not be the aim of this provision (E.U., n.d.). Second, it is unclear to what extent the Intermediary Service Providers have to remain passive and not select or modify the information. The growth of the number of internet users is directly proportionate with the number of inappropriate or unlawful users. Intermediary Service Providers may need to react to a certain extent when their users disseminate illegal or improper information. The previously mentioned exemption of manipulation does not have a clear borderline of which information is unlawful or inappropriate. It is unclear which data needs to be selected or modified to ensure that the intermediary service provider can still be protected under article 12 (E.U., n.d.).

2.2 Caching

"Caching" services are provided to increase efficiency by providing temporary and automatic data storage by making copies of materials stored remote servers into a local server. In this manner, the user's data delivery will be received faster because it will travel less (Baistrochi, 2003). In caching cases, five conditions need to be fulfilled to be exempted from being liable. First, the provider must not alter or change the information. Second, the provider must comply with the conditions on the access of information given from the source. Third, the provider must regularly update the information to ensure that the material stored corresponds to the original server's latest update. Fourth, the provider is not allowed to interfere with applications that measure the use of information, such as visitor counting. Fifth, the provider has to remove the information as soon as he knows that its initial source is removed. No longer accessible, blocked, or competent authority has ordered such removal or disablement. However, even if the "caching" providers comply with the requirements mentioned above, there is still room for an injunction. A court or administration authority is still permitted to ask for an injunction requiring the service provider to terminate or prevent an infringement. Article 13 is supposed to protect traditional "proxy-servers," especially by conditions (c) and (d) of Article 13, which require the provider to comply with updating rules and hit counting rules "widely recognized and used by industry" (E.U., n.d.). However, it may also cover other technology, which was not initially envisaged by the legislator.

2.3 Hosting

Article 14 establishes a limitation of liability for "hosting" providers. "Hosting" service is a form of service where the provider offers space for data on the internet to the user. There are two requirements for "hosting" service providers to comply with under this exemption regime. First, the provider must not have actual knowledge of illegal activity or information and, as regards

claims for damages, must not be aware of the facts or circumstances from which the illegal activity or information is apparent. This paragraph contains two essential elements: the type of illegal content and the type of knowledge required to be exempted from specific liability.

Concerning the type of illegal content, there are two types of unlawful content mentioned in this paragraph. The first illegal content mentioned is an unlawful activity. Illegal activity refers to the user's activity on the website, which may be illegal, e.g., exchanging information about committing certain crimes. The second illegal content mentioned is unlawful information. Illegal information refers to the user's material, which may be unlawful, e.g., child pornography or copyright-infringing material.

The type of knowledge refers to the actual and constructive knowledge. If the Intermediary Service Provider has actual knowledge, it can be held liable for both civil and criminal liability. On the other hand, if the Intermediary Service Provider has constructive knowledge, it can only be held responsible for civil liability. However, the Internet Service Provider can be exempted from being held liable even if it has either actual or constructive knowledge when they immediately remove or disable access to the infringing information. Moreover, there are two exclusions concerned with paragraph 1. First, it does not apply if the service recipient is acting under the authority or the provider's control. Second, it does not affect a court or administration authority's ability to order an injunction to terminate or prevent an infringement to the Internet Service Provider. It also does not affect the Member State's authority to create a procedure for removing or disabling access to information.

As in the previous regime, there are several ambiguities in a "hosting" regime. One of the ambiguities is in the phrase "consist of" in paragraph 1. Nowadays, the difference between

hosting providers who are not involved in creating the content from content providers interested in making the content is becoming vaguer (E.U., n.d.). Cloud computing services and other Web 2.0 services are also providing storage systems as a part of their full service. The criterion does not have a solid framework to what extent a service should relate to hosting service to fall under the hosting regime. Various interpretations come to deal with the situation.

The next ambiguity is in the phrase "under control" in paragraph 2. This ambiguity is because of the service providers' level of control to alter the information to prevent lawsuits, such as misleading information or defamation comment. An administrator monitors some websites to maintain the accuracy of specific data. But it does not give the service providers the ability to prevent such information from being posted first hand. The element of illegal information can also be multi-interpreted; it depends on what law governs the website. The most critical ambiguity comes from the required level of knowledge or awareness. The E-Commerce Directive does not give the limitation or prerequisite level on "actual knowledge" or "awareness." In the end, the courts have the power to determine the prerequisite level needed.

2.4 No general obligation to monitor

Unlike the previous articles, article 15 does not give Intermediary Service Providers the criteria to be exempted under a specific liability regime. Article 15 (1) states that Intermediary Service Providers who provide services, as mentioned in Articles 12, 13, and 14, do not have a general obligation to monitor the information they transmit or store. They also do not have to seek facts or circumstances indicating illegal activity.

Article 15 (2) specifies that the Member States necessitates a specific obligation for the service providers to receive or obtain certain illegal activity information. Intermediary Service

Providers need to inform the authorities if there are indications of unlawful activities or illicit information provided by users as soon as the provider becomes aware of it. Member States still may oblige Intermediary Service Providers to disclose the user's identity with storage agreements.

Furthermore, the reason behind no general obligation to monitor is that Intermediary Service Providers cannot possibly monitor all the content passing on their network and guarantee the freedom of communication and expression (Coudert and Werkers, 2008). An obligation to monitor may breach the user's fundamental rights. However, Article 15 paragraphs 2 of E-Commerce Directive 2000/31 still gives room for the Member States to provide an obligation for Intermediary Service Providers to inform the authorities of alleged illegal activities undertaken or information provided by the recipient of services. Intermediary Service Providers may also be asked by the authority to provide information that enables identifying the users.

2.5 Notice and takedown procedure

As mentioned above, the Directive sets a duty for hosting providers to immediately remove or disable access to the illegal information as soon as they have actual knowledge or are aware of facts or circumstances. However, the Directive does not define the required knowledge and awareness, a precise time limit to be considered "expeditiously," or removal procedure.

Notice and takedown procedures are usually applied to the content related to intellectual property infringement, defamation, terrorism, illegal online gambling, child abuse, misleading advertisement, incitement to hatred or violence based on race, origin, religion, gender, sexual orientation, etc. (Wang, 2012). The typical procedure that is usually adopted requires several steps. First, the hosting providers wait for the notification about the existence of illegal information. After the notice is received, the

providers will temporarily take down the material and send a message to the information owner. This notification to the owner is for confirmation. If the owner does not respond to this notification, the information stays down. On the other hand, if the owner responds to the message, the result may vary depending on the reaction.

In terms of the requirement to be considered "sufficiently precise or adequately substantiated," notice should be allowed to be submitted by electronic means and contain details of the sender without disclosing the sender's details to other parties without informed consent, except to the criminal investigation authorities. It should also specify the precise location and details of the alleged illegal content, such as a URL, item number, and the description of the alleged unlawful nature of the content. Such notification must be accepted by the hosting service providers regardless of whether they can provide proof or evidence that the content provider could not be contacted. There is no reaction after such notification from the content provider.

On the element of the takedown process, it has to be done expeditiously. The hosting service providers will take down the alleged content and send a notification to the content owner about their action. However, there is not any explicit limitation about how fast the takedown has to be done. Considering the Proposal of General Data Protection Regulation 2012, it is ideal to be done within 24 hours. Also, in order to provide transparent information about the process, the hosting service providers need to confirm receipt to the notice parties when they received the notice sent, along with the content provider about the alleged content. A counter-notice system needs to be provided to create a balance for the content provider to plea against the allegation.

The time it takes to take down the alleged content on the notice and takedown process varies. It depends on the content. Several contents

considered to be illegal widely usually are taken down faster, outweighing the nature of the material or the legal framework for removal. It shows that where complainants are highly motivated and hence persistent, content is promptly removed. Meanwhile, in the context where the incentives are weak, or third parties become involved with far less of an incentive to act, then removal is slow or almost non-existent (Moore and Clayton, 2008). These conditions suggest that notice and takedown procedures do not create relief on the burden of the right holders' obligation because it still requires active monitoring by the right holders.

2.6 Passive and neutral

The service providers have to act as intermediaries. They must maintain a passive role to benefit from the liability exemption, but the level and form of passiveness differ depending on the types of services. Being neutral means that the host provider's service is independent of the contents of the hosted or carried information and does not involve any direct interest of the provider regarding the specific contents of the carried or hosted information (Leistner, 2014). "Mere conduit" providers have the strictest passiveness. They cannot initiate the transmission, interfere with the information, or select the recipient. Meanwhile, "caching" providers are allowed to filter the data or the recipient, even though they may not allow changing the local copy of the data. Lastly, "hosting" providers are still allowed to select and modify the data stored and are also allowed to choose the recipient of the data (E.U., n.d.).

Article 15 paragraph 2 GR 80/2019 states that "Online Intermediary Services Provider can be exempted from the obligation to have a business license if (1) is not a party that receives a direct beneficiary from the transaction; or (2) not directly involved in the contractual relationships of the parties conducting Online Intermediary

Services."Article 22 GR 80/2019 regulates as follows:

- (1) If there is illegal electronic information contained in the Online Intermediary Services, the domestic Online Intermediary Services and/or overseas parties and Intermediary Facility Providers are responsible for the impact or legal consequences due to the existence of the illegal electronic information content.
- (2) The provisions referred to in paragraph (1) do not apply if the domestic Online Intermediary Services and/or abroad concerned act quickly to delete the electronic links and/or content of illegal electronic information after gaining knowledge or awareness.
- (3) The provisions referred to in paragraph (1) are exempted for Intermediary Facility Providers who:
 - a. in the context of work as a party that is only continuing to search for information (re conduit), namely:
 1. not initiating a transmission;
 2. not selecting the acceptance; and
 3. does not make any modifications to the information transmitted.
 - b. in the context of work as a party that only temporarily stores information temporarily to streamline communication (caching), namely merely:
 1. not make any modification to the information;
 2. comply with the terms and conditions to access the information;
 3. comply with regulations on updating information following provisions that are widely recognized and used by industry;
 4. does not interfere with the use of technology against the law, widely recognized and used by industry to obtain data to use the information; and
 5. act quickly to delete or deactivate access to information stored after gaining actual knowledge, that information at the initial source of the transmission has been removed from the

network, or access to it has been deactivated; or the court or the authorities have ordered deletion or deactivation.

c. in the context of work as the party providing space for hosting, loading, or storing information (hosting), namely:

1. does not have actual knowledge of action or information that is against the law, and if there is a claim or claim for damage or loss, the relevant provider is not aware of or is aware of the fact that an action or information is illegal; or
2. after the provider concerned knows or is aware that an action or information is unlawful, the Intermediary Facility Provider acts quickly to delete or deactivate access to the information.

d. in the context of work as a provider, search engine, and information searcher and network (searching engine).

- (4) Intermediary Facility Providers providing interactive computer services are not responsible and cannot be sued or sued for their actions in limiting or eliminating access to content if:

- a. the act is a voluntary action carried out on a good faith basis to restrict access to or availability of material that the user or provider considers to be within the scope of illegal electronic information content, without having to do a legal test of its protection; or
- b. the action was taken to restrict public access, not activate, or make it unavailable to be accessible by the content provider of the information on its analysis or other parties.

RESEARCH METHODOLOGY

The research methodology in this research is normative legal research. The legal norms that become the main focus in this research are the E.U. rules on exemption of responsibility for online intermediary service providers and what they adopt in Indonesian law. This research is descriptive, evaluative, and analytical, expressing legislation relating to the research object's legal theories. This research focuses on the principle of limitation of responsibilities in the E-Commerce

Directive and how the principle of limitation of responsibility can be adopted into the Indonesian legal system.

RESULT AND ANALYSIS

The current legislations are overlapping and create a limitation on the development of internet society. Different legislations require different licenses from internet service providers. Those requirements create obstacles to the establishment of online services. They also induce reluctance among business owners to establish their business. Nonetheless, it will hamper internet society's development, including the service provider's variety of services. By giving exemption of liability of online intermediary services for Indonesia, it is also expected to create one comprehensive and codified regulation applied only for the general internet regime, or possibly only for online intermediary services. The current overlapping creates multiple impositions of rules. Online intermediary services providers are meant to only provide a platform or media for users to use the platform. The content is not given by the online intermediary services provider but by its users. The multiple sources of content make it unreasonable to ask an online intermediary services provider to sensor all postings.

Adopting laws causes problems at all levels of government and society. Several factors may be the cause. Those are differences in culture and trust, society, technology, law, crime, etc. (Widjaja, 2021). These problems may also happen regarding adopting an exemption of liability for online intermediary services provider in Indonesia. One of the most feasible issues is to create a balance between online intermediary services provider rights and user's rights. Many other law fields may be affected if the online intermediary services provider has fewer obligations, such as consumer protection. Consumer Protection Law is created in consideration that consumers are in the least favorable position. Consumers are very well

protected in the current Indonesian Law, to the detriment of service providers. The existing e-commerce legislation has an unclear level of negligence, fault, and forces major, which can be problematic in determining the extent to which an online intermediary services provider can be held liable. It does not make any sense for online intermediary services provider providers to monitor and check all the information given by their users.

Another problem arises concerning the legal structure in Indonesia. The online world is a very dynamic and developing place, including online intermediary services provider. Unfortunately, Indonesian regulations tend to be very rigid and not up-to-date. Furthermore, Indonesia's legal structure also creates the problem in making comprehensive legislation (Widjaja, 2017). The characteristic of Indonesian legislation that it contains more than one field of law in a single piece of legislation, but is scattered over several pieces of legislation dealing with similar issues, creates overlap. Therefore, coordination with other existing legislation needs to become a serious concern in future legislative initiatives to prevent multiple overlaps on the online intermediary services provider in running or establishing their services. However, that solution given in the current legislation in Indonesia is not in favor of developing E-Commerce. Nowadays, Indonesian online intermediary services providers are under a burden to monitor all the traffic on their site without a guarantee not to be held liable. As a developing country, Indonesian e-commerce legislations are still underdeveloped. Several aspects need further improvement to create a good regulation. With the proliferation of online intermediary services provider in Indonesia and seeing many cases relating to online intermediary services provider transactions, improving the legislation becomes essential.

The E.U. E-Commerce Directive 2000/31 could be a reference for the Indonesian government to

improve its regulations regarding e-commerce, especially in online intermediary services provider. Since this Directive has been proven to be effective in regulating the e-commerce market in the European Union, there are valuable lessons from the Directives that Indonesia could adopt to strengthen its e-commerce regulation. However, to assume the E-Commerce Directive 2000/31, especially Articles 12 to 14, where the exemption of liability is regulated, it needs some adjustment to be suitable for the Indonesian legal system and culture. The adjustment is to make the adopted version better than the original; to avoid the problems that have already arisen in the European Union. In conclusion, it is beneficial for the Indonesian government to adopt the exemption from intermediary service provider liability for online intermediary services providers under Articles 12 to 14 of the E-Commerce Directive 2000/31 with some adjustments. As explained in previous Chapters, e-commerce plays a large role in the present Indonesian society and economic development. Nowadays, many Indonesians favor shopping through the online intermediary services provider for several reasons, including that it is more practical because they do not have to go anywhere; that it is more comfortable as it offers more variety. Unfortunately, they are still having many legal protection problems if an unfortunate event happens in the transaction process. Therefore, the current legislation makes online intermediary services providers responsible for everything on their website.

Some recommendations can be proposed for the Indonesian legislator to improve e-commerce regulation regardingan exemption from intermediary service provider liability for an online intermediary services provider. It will balance the protection for online intermediary services providers and their users and further develop and flourish online intermediary services providers in Indonesia. The exemption from intermediary service provider liability for online intermediary services provider should be

implemented in the form of a new Government Regulation. The new Government Regulation's role will be implementing Indonesian Law Number 11 of 2008 on Electronic Information and Transaction, following Article 7 of Indonesian Law Number 12 of 2011 on Formulation Legislation. To prevent contradiction and overlap with the existing legislation, it must have a provision clearly stating that all other legislation does not apply if the subject matter has been regulated in this new Government Regulation.

Furthermore, some adjustments need to be implemented to the new Government Regulation to align with the E-commerce Directive 2000/31. Those adjustments have to be following the guidance outlined in the Indonesian Law Number 12 of 2011 on Formulation Legislation. First, the new Government Regulation has to be limited to online intermediary services provider and must include an online intermediary services provider. The limitation can be specified in the title of the new Government Regulation. Besides, the definition of online intermediary services provider is defined in the General Provision section.

Secondly, the provisions' formulation has to be under the guidelines outlined in the Indonesian Law Number 12 of 2011 on Formulation Legislation, including provisions that form a positive manner, usage of capital letters, etc. Therefore, it must have provisions about the obligation of an online intermediary services provider. One of the significant differences of the responsibility is on the monitoring. Online intermediary services provider in Indonesia should be obliged to collect sufficient information regarding their users for others to identify the counterparty in their transaction. It also has to guarantee that an online marketplace will not be held liable as an accomplice or negligent if they can provide sufficient information to identify their users.

Finally, it has to have a provision that functions as a clear guideline of notice and takedown

procedure. Notice and takedown procedure will function as a procedural guideline and a source of knowledge required to take down infringing material. By having a definite knowledge source, online intermediary services providers are no longer needed to monitor their website to find any infringement actively.

CONCLUSION AND RECOMMENDATION

Based on the above analysis, the new Government Regulation's should be amended as follows. The following recommendation is made under guidelines as stipulated in Appendix I of Indonesian Law Number 12 of 2011 on Formulation Legislation. The new Government Regulation should have the definition of online intermediary services provider on the General Provisions section. The definition of online intermediary services provider on the new Government Regulation should be read as follows:

"Online intermediary services provider are a form of Electronic System run by an Electronic System Organizer that performs intermediary services by providing a platform for their users to trade among themselves."

The new Government Regulation has to regulate online intermediary services provider' obligation and prohibition. The formulation of obligation should be:

"In performing their services, Online intermediary services provider are obliged to

1. Collect sufficient information regarding its users for others to be able to identify the counterparty in their transaction. The information collected is published on the platform and accessible to other users.

2. Provide for the operation of a Notice and Take Down system."

Furthermore, the formulation of prohibition should be:

"In performing their services, Online intermediary services provider are prohibited from:

1. Initiate the transmission to users. Online intermediary services provider are not restricted

from performing the promotional activity as permitted by Indonesian Law

2. Selecting or modifying the information provided by users at some reasonable extent permitted by Indonesian Law. Selections or modifications of information from users are implemented as a form of co-operation between Online intermediary services provider and their users to monitor the platform together."

The Notice and Take Down in the obligation section will need an explicit process provision. The provision of the Notice and Take Down should be:

"Online intermediary services providers have to provide a system for their users to be able to report alleged illegal Electronic Information and/or Electronic Documents. After receiving a report from their users about alleged illegal Electronic Information and/or Documents, Online intermediary services providers have to take down the alleged illegal Electronic Information and/or Electronic Documents while asking for clarification from users who provide the Electronic Information/or Electronic Documents within 24 hours. The users who give the Electronic Information and/or Electronic Documents have 24 hours after being asked by the Online intermediary services provider to clarify the Electronic Information and/or Electronic Documents.

1. In such cases where the users who provided the Electronic Information and/or Electronic Documents give a justified clarification, the Electronic Information and/or Electronic Documents will be reinstated online.

2. In such cases where the users who provide the Electronic Information and/or Electronic Documents do not give any form of clarification that has been asked by the Online intermediary services provider, the Electronic Information and/or Electronic Documents are taken down permanently.

3. In cases where it is necessary, depending on the Electronic Information and/or Electronic Documents, the Online intermediary services

provider may have to notify the relevant authorities about the Electronic Information and/or Electronic Documents."

In the end, a transitional provision is needed as a link to other legislation. The transitional provision should be:

"As long as this Government Regulation has not governed it, all other legislation that may govern any elements related to Online intermediary services provider remains valid and unaffected."

As for further recommendations, the new Government Regulation can set a specific privacy and data protection legislation only for online intermediary services providers as Indonesia does not have general privacy and data protection legislative framework. Besides, online intermediary services providers must be obliged to provide an internal dispute resolution mechanism. Even though the Indonesian government allows dispute settlement inside or outside of court, they are rare in practice since it consumes a lot of time and money. The online marketplace should provide an internal dispute resolution mechanism to solve users' problems in a cost and time-efficient manner.

REFERENCES

- [1] Baistrochi, Pablo. (2003). "Liability of Intermediary Service Providers." *the E.U. Directive on Electronic Commerce*, 19 Santa Clara Computer & High Tech. L.J. 111 (2003). Available at <http://digitalcommons.law.scu.edu/chtlj/vol119/iss1/3>
- [2] Coudert, Fanny, and Evi Werkers. (2008). "In The Aftermath of the Promuscae Case: How to Strike the Balance?" *International Journal of Law and Information Technology*, 18(1); 50-71.
- [3] Dong, Fei, Sol M. Shatz, Haiping Xu, and Dibyen Majumdar. (2012). "Price Comparison: A Reliable Approach To Identifying Shill Bidding In Online Auctions?" *Electronic Commerce Research and Application*. 11;171-179.
- [4] E.U. (n.d.). "Study on the Legal Analysis of a Single Market for the Internet Society; New Rules for a New Age.- Liability of Online Intermediaries."
- [5] Edwards, Lilian, and Charlotte Waelde. (2005). "Online Intermediaries and Liability for Copyright Infringement." keynote paper at WIPO Workshop on Online Intermediaries and Liability for Copyright, Geneva, April 2005 p.23
- [6] Leistner, Matthias. (2014). "Structural aspects of secondary (provider) liability in Europe." *Journal of Intellectual Property Law & Practice*, 9(1);75-90
- [7] Moore, Tyler, and Richard Clayton. (2008). "The Impact of Incentives on Notice and Takedown." Seventh Workshop on the Economics of Information Security (WEIS 2008), June 25–28 2008.
- [8] Schellekens, Maurice. (2011). "Liability of Internet Intermediaries: A Slippery Slope?" *SCRIPTed*, 8(2);154-174
- [9] VanHoose, David D. (2013). *E-Commerce Economics*. South-western: College Pub,
- [10] Wang, Faye Fangfei. (2012). "Response to Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries." *Intellectual Property forum*, 91;93-98.
- [11] Widjaja G, and Sijabat HH. (2021). Rules-Raised Ethical Issues During The Covid-19 Pandemic In Indonesia. *SRP*, 12(1): 623-632. [doi:10.31838/srp.2021.1.90](https://doi.org/10.31838/srp.2021.1.90).
- [12] Widjaja, Gunawan. (2017). "The Importance of Comprehensive Trusts Law in Indonesia." *International Journal of Applied Business and Economic Research*, 19);149-155.