LEGAL CONSEQUENCES OF ELECTRONIC AGREEMENTS VIEWED FROM ARTICLE 1866 OF THE CIVIL LAW

Gusti Putu Krisna Murti AV[1*], Dewa Gede Pradnyana Yustiawan[2]
[1,2]Faculty of Law, Universitas Udayana
E-mail: [1)] krisnamurtiav1@gmail.com, [2)] Pradnyana_yustiawan@unud.ac.id

Abstract

Legal issues with regard to authenticity, authenticity, and proof arise frequently because no laws exist to control the private information of users of electronic agreements. The aim of this research is to determine whether or not there are issues with the legal binding force of agreements established via electronic means. This study employs a normative qualitative approach, based on the analysis of secondary data and bolstered by original data collected in the field. The findings prove that digital investigative tools can be used to verify the legitimacy, veracity, and integrity of electronic contracts. A person's permission is required before any of their personally identifiable information (PHI) can be used in any way, shape, or form via technological media. The evidentiary weight of an electronic or digitally signed deal is the same as that of a handwritten one. As progress is made toward open proof, the judicial system can make use of the system. Given the prevalence of online media in modern business dealings, it follows that any evidence acquired from any source, provided it is true, is admissible so long as it does not violate public order.

Keywords: *Electronic Agreement, Legal Consequences, Authenticity*

1. INTRODUCTION

The rapid growth of internet use, the impact of advances in electronic technology, and the actions of the global community in carrying out agreements and other tasks are examples of how humans are increasingly conducting their daily lives online. It is as if there are no barriers for humans to establish legally binding relationships across vast distances and time. In this regard, the rule of law must step in to ensure that all participants in electronic transactions are afforded equal protection under the law regardless of the nature of the transaction.

The agreement is mandatory for the parties and must be implemented in good faith if it fulfills the legal requirements of the agreement. The requirements of Article 1320 of the Civil Code must be met before making a contract. In order for judges to have confidence in the evidence presented at trial, it is important for both parties to present evidence of real events. This is an example of proof.

Concerns about which laws and jurisdictions apply to the conduct of electronic agreements arise when the parties to the agreement are located in different places. Many people still think that contracts or agreements signed online are not legally binding because they exist on the internet or cyberspace. When an electronic agreement is created, it demonstrates that its participants don't just imagine themselves somewhere in cyberspace (Sitorus, 2015).

Tokopedia, Shopee, and Bukalapak are just a few of the many online applications that act as intermediaries for electronic commerce, although sellers and buyers are free to transact with each other directly. Of course, in electronic transactions this cannot be separated from data which is also provided digitally because it is used to facilitate

transactions. Because if the data is known by other parties, then the transaction will not be in accordance with what is desired by the parties in the transaction, it is only natural that electronic transaction intermediary application providers want to maintain the security of the data that has been given to them. Bukalapak, an application supplier for electronic transaction intermediaries, suffered a data breach that affected 91 million of its users (Simamora et al., 2022). In this case, both the plaintiff and the defendant must rely on electronic evidence.

The author will analyze the relevant parts of the Civil Code, especially Article 1320 regarding the legal requirements for agreements, Law no. 19 of 2016 concerning Information and Electronic Transactions, and finally Article 163 HIR together with Article 1866 concerning types of proof of the Civil Code.

Based on the background described above, this research was conducted with the aim of finding out how the problems of authenticity, authenticity and integrity of electronic agreements and the validity of an agreement made electronically.

2. RESEARCH METHODS

This research uses a socio-legal approach, which examines law from the community's point of view. The aim of this research is to illuminate the challenges inherent in legal compliance. The purpose of this descriptive research is to document the current state of a particular variable or subject, in this case the symptoms and conditions being experienced by the participants. This study details the protocols and procedures for determining the legality of electronic transactions based on Article 1866 and the ITE Law.

This socio-legal study relies on secondary data supplemented by original data collected in the field. Most of the information was collected through in-depth interviews with government officials at the Ministry of Communication and Informatics and the Tangerang District Court.

3. RESULTS AND DISCUSSION

3.1. Problems with originality, Authenticity and Integrity of Electronic Agreements

The difficulty in proving the authenticity of an electronic agreement stems from issues such as the following: how to prove that the parties have provided electronic agreement with an electronic signature? Law No. 19 of 2016 concerning Information and Electronic Transactions is the only substantive legislation that currently regulates electronic evidence (Dotulong, 2014).

Problems with electronic evidentiary law relating to electronic signatures on paper remain in Indonesian civil procedural law (Saruji & Martana, 2015). According to Arif Budi Cahyono, a judge at the Tangerang District Court, in an online national seminar regarding electronic agreements, he said that "with digital forensics. Digital forensics is a method used to identify, collect, analyze and test digital evidence for a legal case.

Furthermore, Arif Budi Cahyono, a judge at the Tangerang District Court, when asked several questions, added that, “There is no legal regulation relating to e-commerce. Currently using the default 'terms of agreement' on the e-Commerce page. As soon as we click 'I accept', it means that we have automatically submitted ourselves and are bound to the agreements and regulations of the e-Commerce that we use”.

Arif Budi Cahyono further explained that: “According to the Supreme Court,

electronic evidence is classified as evidence if it is linked to Article 184 of the Criminal Procedure Code. What needs to be considered is if the electronic evidence is denied by the opponent. So that's why we use digital forensics to find out the authenticity of the evidence. For example, photos can be changed and edited. This is where the role of digital forensics is to test its authenticity to ensure that the photo was taken from what source and is original without editing. An example is the Antasari case where there is evidence that he texted the perpetrator, even though according to an ITB expert it was not sent from his cell phone". Providers can be defined as companies or business entities that provide services to users. Providers can sometimes also be referred to as companies that usually serve as website creation, arrange their placement in the cyber world (including maintenance and provision of Internet access) as well as help in terms of promotion so that the website is visited by Internet users (Romindo et al., 2019).

According to Ruby Zukri Alamsyah, a forensic expert, revealed that "Residents can report the provider to the police if it is proven that there are non-law enforcement civilians who intentionally leak personal data without the owner's permission, the provider is subject to a warning or sanction from the Indonesian Telecommunication Regulatory Agency".

Josua Sitompul as The Ministry of Communication and Information Technology (KOMINFO) Legal and Cooperation Coordinator in his answers to our Research and Research questions stated that "Electronics is easy to change, add, or subtract. Therefore, the acceptance of electronic information as legal evidence (admissibility) is determined by the certainty that the authenticity of the information is maintained and its availability. The meaning of authentic is not that electronic information is made by an authorized official. There are at least two things that must be considered in determining the authenticity of electronic information or documents. First, electronic information is called authentic if the source of the electronic information comes from a person or party that has the right or authority to issue the intended electronic information or document. Second, the content or content is the content intended by the source".

As stated in Article 26 paragraph (1) of the Information and Electronic Transactions Law which states that: "Unless otherwise provided by laws and regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. Therefore, if personal data is violated, such as in the case of leaking of personal data, the party who feels their rights have been violated can file a lawsuit".

Electronic information or documents and/or printouts are recognized as valid evidence according to Article 5 paragraph 1 of the ITE Law. The definition of "Electronic Knowledge" is contained in the ITE Law Article 1 Point 1. On the other hand, the definition of electronic documents used in the Criminal Code is regulated in Article 1 Number 4. Although they can be distinguished, electronic and paper information cannot be separated. The difference between electronic information and electronic documents can be summed up as follows: electronic information is data, while electronic documents are data in a certain structure. Electronic Information, for example, refers to words, writing, letters and numbers contained in files with extensions .doc, .pdf, .mp3 and .jpg. .doc, pdf, mp3, and jpeg are file types for electronic documents.

The procedural law in force in Indonesia recognizes electronic information and/or electronic documents and/or printouts as additional valid evidence. This is stated in Article 5 paragraph (2) of the ITE Law. This arrangement is a first for the ITE Law, and

it helps bridge the gap between traditional rules and principles for presenting evidence (which require tangible objects) and technological advances.

In order to expand the scope of evidence that can be accepted in the Criminal Procedure Code, it is necessary to expand the scope of evidence regulated in Article 186 of the Civil Code, in particular the expansion of documentary evidence. In this context, truncation refers to hard copies of data or files that were originally stored digitally. The term "electronic evidence" is used to describe a growing body of evidence that can be presented in court, in this case information or letters stored or transmitted by electronic means.

3.2. The Legitimacy of Agreements Through Electronic Viewed from Article 1866 of the Civil Code

As a result of having agreed on the terms of the agreement, now each party is legally obliged to carry out the rights and obligations (also called achievements) set forth in the agreement (Sa'adah, 2020). The consequences imposed by law on the parties to the agreement are the result of the legal actions they took to realize their rights and fulfill their obligations under the agreement (Sari, 2017).

According to Subekti in Kumalasari & Ningsih (2018) that "An agreement isan event where a person promises to another or where two people promise each other to do something". Based on Article 1313 of the Civil Code, it states that "Consent is an act in which one or more people bind themselves to one or more other people". According to Article 1320 of the Civil Code, for an agreement to be valid, four conditions must be met. This includes consent on their own terms, free and informed consent, no coercion or undue influence, and no fraud.

According to Bambang & Joni (2013), "There are 4 (four) explanatory theories when an agreement can be considered as having been reached: Pronunciation Theory; Delivery Theory; Theory of Knowledge and Theory of Acceptance". The ability to make an agreement means that the parties who will make an agreement must be legally competent, if there are parties who are not legally competent, the agreement can be canceled. Based on Article 1330 it states that "Incompetent to make an agreement are: First, immature people, meaning that immature people are prohibited from making agreements, the law stipulates that what includes immature people is those who have not reached the age of 21 years; Second; those who are placed under guardianship, meaning that people who are still placed under guardianship cannot make an agreement, if they make an agreement then the guardian will represent them; and thirdly, women, in matters stipulated by law, and in general all people to whom the law has prohibited making certain agreements, meaning that women are included as people who are not competent at law, but after the marriage law is born, this rule does not apply. As long as they are an adult and there are no other problems, married women are considered fully competent legal subjects under the law. What this means is that the agreement should define clear, achievable goals that can be used by both parties, rather than something that is just a pipe dream or a tentative plan. When an agreement is said to be for valid reasons, it means that it is not against the principles of law, morality, or public order.

Article 8 paragraph (1), "United Convention on the Use of Electronic Communication in International Contracts recognizes the validity of electronic agreements, which can be legally enforced".

Josua Sitompul stated that "The validity of printed results from electronic

information depends on the validity of the electronic information and documents. If the electronic information or document is valid, then the printout is also valid". In order for data or paper stored in electronic format to be legally binding, the following conditions must be met:

1) Article 5 paragraph (4) of the ITE Law which confirms that "according to the law, letters must be made in written form or letters and documents which according to law must be made in the form of a notary deed or a deed drawn up by an official making the deed. In this case, the electronic form of the letter or document cannot be used as valid legal evidence. The formal requirements set out in the Civil Code, are a private deed or other letter that is recognized by interested parties".
2) Article 6 of the ITE Law, "Electronic Information and/or Electronic Documents are considered valid as long as the information contained therein can be accessed, displayed, guaranteed for its integrity, and can be accounted for so as to explain a situation".
3) Article 7 of the ITE Law, "every person who declares rights, strengthens existing rights, or rejects the rights of other people based on the existence of Electronic Information and/or Electronic Documents must ensure that the Electronic Information and/or Electronic Documents in it originate from an Electronic System that meet the requirements based on the Laws and Regulations".

Furthermore, Josua Sitompul said that "regarding electronic signatures, the ITE Law and PP 71/2019 regulate the existence of non-certified electronic signatures (for example in the form of scans), and certified signatures. Certified signature using a trusted third party. Both types of signatures have legal force and legal consequences as long as the provisions of Article 11 of the ITE Law are met".

Telecommunications Law Number 36 of 1999 concerning Telecommunications in Article 2 states that "telecommunication is organized based on the principles of benefit, fairness and equity, legal certainty, security, partnership, ethics, and self-confidence". Article 3 states that "telecommunication is organized with the aim of supporting national unity and integrity, increasing the welfare and prosperity of the people in a fair and equitable manner, supporting economic life and government activities, and enhancing relations between nations".

According to Mualifah (2020) that "Proof contains logical, conventional and juridical meanings". In a logical sense, is to provide absolute certainty. In the conventional sense it means certainty only not absolute certainty. In a juridical sense, it is proof that provides the truth that applies only to the parties to the case.

Yahya (2005) said that "what is meant by the general principle of proof is the basis for the application of evidence. All parties, including judges, must adhere to the standards outlined by the said principle. Indeed, in addition to that, there are more specific principles that apply to each type of evidence, so that it must be used as a benchmark in the application of a system of evidence. However, what is discussed in general principles is a provision that applies to the evidentiary system in general".

According to Arif Budiman, the Tangerang District Court judge, when interviewed, explained Article 5 paragraph (1) of the Electronic Information and Transaction Law, stating that: "Electronic Information and/or Electronic Documents and/or their printouts are valid legal evidence". Furthermore, judges' acceptance of electronic evidence broadens the scope of what can be considered evidence.

According to Article 164 HIR and Article 1866 of the Civil Code, our country's

civil procedural law recognizes the following pieces of evidence: (1) written; (2) witnesses; (3) presumption; (4) recognition; and (5) oath.

According to Yusandy (2019) that "the evidentiary system adopted to date is as follows: Closed and Limited System. The parties are not free to submit the type or form of evidence in the process of settling a case. Developments Towards Open Evidence In evidentiary law it is no longer determined a certain type or means of evidence, but from any means of evidence the truth must be accepted as long as it does not conflict with public order."

4. CONCLUSION

In conclusion, there is a slight refusal to update or delete data in electronic form. Therefore, the availability and guarantee of maintaining the authenticity of information determines whether or not the information can be used as legal evidence (admissibility). This term does not imply that any particular piece of electronic data has been created by a sanctioned authority figure. To verify the legitimacy of digital files, two factors are required. For starters, we can say that an electronic information is genuine if it comes from a source that has the right or legal power to publish certain parts of the electronic documentation. Second, the information presented is what the original author had in mind. Those involved, including courts, must be able to easily access the electronic information required for evidentiary purposes. Each party making a statement in a civil law dispute must bear the burden of proof. The ITE Law which applies to every material or document made electronically recognizes the legal force of electronic agreements. When a case goes to court, the court will be able to apply an evolving evidentiary system that supports open evidence.

A recommendation to the legislature of the Personal Data Protection Act is necessary for personal information security to ensure that all parties involved in electronic interactions are protected. The burden of upholding legal certainty lies with the judiciary, especially regarding evidence that is not regulated in Article 1866 of the Civil Code.

REFERENCES

Bambang, R. J., & Joni, R. (2013). Hukum ketenagakerjaan. *Bandung: Pustaka Setia*.

Dotulong, T. (2014). Keberadaan Alat Bukti Elektronik Dalam Penyelesaian Sengketa Perdata. *Lex Privatum*, *2*(3).

Kumalasari, D., & Ningsih, D. W. (2018). *Syarat Sahnya Perjanjian tentang Cakap Bertindak dalam Hukum menurut Pasal 1320 Ayat (2) KUH Perdata*.

Mualifah, M. (2020). Penyuluhan Hukum Tentang Peranan Alat-alat Bukti dalam Penyelesaian Perkara Perdata. *Jurnal Abdi Insani*, *7*(3), 268–271.

Romindo, R., Muttaqin, M., Saputra, D. H., Purba, D. W., Iswahyudi, M., Banjarnahor, A. R., Kusuma, A. H. P., Effendy, F., Sulaiman, O. K., & Simarmata, J. (2019). *E-Commerce: Implementasi, Strategi dan Inovasinya*. Yayasan Kita Menulis.

Sa'adah, N. (2020). Akibat Hukum Pembuktian Perjanjian Tidak Tertulis (Analisis Putusan Nomor: 373/Pdt. G/2016/PN Mdn). *Pamulang Law Review*, *1*(2), 137–150.

Sari, N. R. (2017). Komparasi Syarat Sah Nya Perjanjian Menurut Kitab Undang-Undang Hukum Perdata Dan Hukum Islam. *Jurnal Repertorium*, *4*(2).

Saruji, P. V., & Martana, N. A. (2015). Kekuatan Hukum Pembuktian Tandatangan Pada

Dokumen Elektronik Sebagai Alat Bukti Dalam Hukum Acara Perdata. *Kertha Semaya: Journal Ilmu Hukum*, *4*(2).

Simamora, A. M., Fahmi, F., & Triana, Y. (2022). Akibat Hukum Perjanjian Melalui Elektronik Ditinjau dari Pasal 1866 Kitab Undang-Undang Hukum Perdata: Legal Consequences of Agreements Through Electronic Judging From Article 1866 of the Civil Code. *DOKTRINA: JOURNAL OF LAW*, *5*(2), 108–217.

Sitorus, D. A. (2015). *Perjanjian Jual Beli Melalui Internet (E-Commerce) Ditinjau Dari Aspek Hukum Perdata*. Universitas Atma Jaya Yogyakarta.

Yahya, H. M. (2005). Hukum Acara Perdata. *Jakarta: Sinar Grafika*.

Yusandy, T. (2019). Kedudukan dan Kekuatan Pembuktian Alat Bukti Elektronik dalam Hukum Acara Perdata Indonesia. *Jurnal Serambi Akademica*, *7*(5), 645–656.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).