Power of Proof Electronic Document Evidence in the Court

Siti Mariyam(✉) and Zabidin

Universitas 17 Agustus 1945 Semarang, Semarang, Indonesia
sitimariyam@untagsmg.ac.id

Abstract. This study aims to examine and analyze the strength of evidence of electronic document evidence in court. This study uses a normative juridical approach, with secondary data sources consisting of primary legal materials in the form of laws and regulations including the ITE Law, Criminal Procedure Code, and secondary legal materials in the form of research results, journals, and supported by tertiary legal materials, while the data collection method using a literature study, and data analysis method using a calibration method. The results obtained: the development of information technology, media, and communication has changed the order of people's lives in all fields, including in the field of legal evidence in court. Since the ITE Law was ratified in 2008, there has been an expansion of the types of evidence in the trial, namely electronic information and/or electronic documents, and the results/printed forms are recognized as legal evidence, this is an expansion of legal evidence in accordance and regulated by law. Events that exist and apply in Indonesia. The electronic document/electronic information is considered valid if it fulfills the requirements, namely that it can be accessed, can be displayed again and its integrity is guaranteed, which means it has not changed its shape from the start of the electronic document being ratified, and the integrity of the electronic document/information can be accounted for so that it can explain a situation, in addition to the specificity for a reliable electronic system operator.

Keywords: Evidence Tools · Electronic Documents · Proof · Court

1 Introduction

The development of the modern era as it is today whose technology is developing very rapidly and is also followed by the development of information technology which can also help simplify and lighten the burden of human work, become a means of education and become a place used to get rupiah coffers in economic activities. Technology is a tool that can facilitate humans in all activities and this cannot be separated from each other, and has become an attachment between humans and technology. As well as being a modern tool, which gave birth to science and technology that greatly helped mankind. In the era of the Industrial Revolution 4.0, the law must be able to respond to the development of information technology, even though the law can hardly keep up with its speed. Prof. Satjipto Rahardjo, S.H., revealed that "the law is for humans, not humans for the law" meaning that if the law is not appropriate, then it is not humans who must be

A. Endah Kusumaningrum et al. (Eds.): ICLEH 2022, ASSEHR 723, pp. 285–297, 2023.
https://doi.org/10.2991/978-2-38476-024-4_31

forced to adapt to the law, but the law must be adapted to the development of demands for human needs.

One of the processes in dealing with civil law is proof, elements of evidence, and rules of evidence. In the court process, the judges' views regarding the evidence prepared were varied, some of which were of the opinion that evidence in the form of electronic documents was considered as legal evidence in addition to conventional evidence in the procedural law; However, there are also those who argue that evidence in the form of electronic documents is a piece of complementary evidence that must be supported by other evidence to increase the conviction of the judge.

The combination of communication technology and information technology gave rise to the internet which is currently the main means of developing information technology. The existence of the internet network means that there are no longer distances or boundaries between countries, in order to increase efficiency in trade transactions using an electronic system, which is often also called e-commerce. E-commerce itself has a general and broad meaning, namely the distribution, purchase, sale, and marketing of goods and services through electronic systems such as the internet or other computer networks. E-commerce may include activities such as: electronic funds transfer, electronic data exchange, automated inventory management systems, and an automated data collection system (http://en.wikipedia.org/wiki/E-commerce). Such a situation shows that the internet provides benefits for the community, because it provides convenience in carrying out various activities, especially those related to the use of information, namely one of the benefits that are most felt by the internet is that this facility functions as a medium without any obstacles for the community. Sending and receiving of information.

Technological developments can increase acts of violation of civil norms, whether it is a violation of contract norms (default) or violations of legal norms or unlawful acts, then regulations should also be improved in accordance with the development of existing technological advances, especially in terms of submitting evidence used as evidence in court. So, related to the law of evidence, it will usually bring up a dilemma position, on the one hand, it is hoped that the law can keep up with the times and technology, on the other hand, there is also a need for legal recognition of various types of digital technology developments to function as evidence in court.

Developments in information technology that issued new rules in Indonesia, in the Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions. In general, the material in the ITE Law is divided into two major parts, namely the regulation of information and electronic transactions and the regulation of prohibited acts. The ITE Law regulates new evidence as an extension of the evidence regulated in the Criminal Procedure Code. Article 5 of the ITE Law reads:

(1) Electronic information and/or electronic documents and/or their printouts are valid legal evidence
(2) Electronic information and/or electronic documents and/or their printed results as referred to in paragraph (1) is an extension of legal evidence in accordance with the applicable procedural law in Indonesia.

Based on the contents of Article 5 of the ITE Law above, there is evidence called electronic information and/or electronic documents that can easily prove criminal acts

regulated in the ITE Law because the new evidence is an extension of the evidence regulated in Article 5 of the ITE Law. 184 KUHAP. As stated in Article 184 of the Criminal Procedure Code, the legal evidence in criminal proceedings is as follows:

(1) Witness Statement
(2) Expert Statement
(3) Letter
(4) Hint
(5) Defendant's Statement

Electronic evidence was first introduced in Article 26A of Law Number 20 of 2001 concerning Amendments to Law Number 31 of 1999 concerning the Eradication of Criminal Acts of Corruption. Then the regulation of electronic evidence is regulated in more detail in Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 or hereinafter referred to as the ITE Law.

In the Association of Chief Police (ACPO), which is contained in the book Good Practice, Guide for Computer Based Electronic Evidence, categorizes several types of electronic evidence, namely: 1. Computers, 2. Network, 3. Video & Closed-Circuit Television (CCTV), 4. Mobile Phones. Meanwhile, in Muhammad Neil El Himam classifying electronic evidence can be sourced from:

1. Computer, which consists of; a. E-mail, b. Digital images, c. Electronic documents, d. Spreadsheets, e. chat logs. f. Illegal software and other intellectual property rights.
2. Hard Disk, which consists of: a. Files, both active, deleted or in the form of fragments, b. File Metadata, c. Slack Files, d. Swap Files, e. System Information, which consists of Registry, Logs, and Configuration Data.
3. Other sources, which consist of: a. Cellular Phone, namely in the form of SMS, Called Number, Incoming Call, Credit/Debit Card Number, E-mail Address, Call Forwarding Number; b. PDAs/Smart Phones, which consist of everything listed in Cell Phones plus contacts, eta, pictures, passwords, documents, etc.
4. Video Games; a. GPS Device containing Routes; b. Digital Camera, contains photos, videos, and other information that may be stored on a memory card (SD, CF, etc.).

Developments in the modernization and digitization of information have helped in many ways, such as in conducting transactions, assisting the world of education, trade, banking, and other benefits that can facilitate activities, both economic and social [1]. The development of this era of globalization using electronic media to make written evidence or letters is increasing, through electronic mail (Electronic Mail). Where in its utilization, people can use the WWW (World Wide Web) domain, for example, Yahoo and Gmail. If it is interpreted more deeply, electronic mail as legal evidence can be seen in Articles 5 and 6 of the ITE Law. In civil procedural law, there is a principle of proof, which is stipulated in Article 163 Herziene Indonesische Reglement (HIR) jo. 283 Rechtsreglement Voor De Buitengewesten (RBg) jo. 1865 The Civil Code (KUHPer) which stipulates that: Whoever claims to have rights to an item, or appoints an event to confirm his rights, or denies the rights of others, then that person must prove it [2].

However, despite the existence of the ITE Law and several other regulations, it cannot be said that Indonesia's procedural law has regulated electronic evidence in its evidence, because the current regulation of electronic evidence is only in the field of material law. Given the nature of procedural law that is binding on parties who use it, including judges, the regulation of electronic evidence in procedural law, both civil procedural law, criminal procedural law, and state administrative procedural law, is very necessary and must be updated in order to achieve legal certainty.

In the world of the internet, the term e-mail is also known, namely, electronic mail or digital mail or electronic post. E-mail is a means of sending letters via the internet. Through regular mail (manually) generally the sender of the letter requires a fee to buy stamps and also takes a longer time for delivery, but through electronic mail, the costs incurred are the costs to pay for an internet connection and the time required for delivery is relatively short and fast (in terms of online). Various activities and activities can be carried out by using internet technology facilities, such as e-mail which often causes legal problems, for example, the case that befell Prita Mulyasari who was charged with Article 27 paragraph 3 of the ITE Law.

In accordance with Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016, in Article 1 number 1 Electronic Information is one or a set of electronic data, including, but not limited to writing, sound, images, maps, designs, photographs, Electronic Data Interchange (EDI), electronic mail, telegram, telecopy, or the like, letters, signs, numbers, codes, access, symbols, or processed perforations that have meaning or can be understood by those who can understand it.

In civil procedural law, the evidentiary system adopted is positive, meaning that proof only looks at the evidence, which is what has been determined in the law. The lawsuit can be granted if it is based on valid evidence. Evidence also has a significant position in the trial process where this evidence becomes a means or tool that can be used to strengthen opinions in a trial in court. Therefore, this evidence should not be left behind if someone wants to conduct and win a case in court, including in a civil case trial. However, in everyday life the explanation that states electronic mail is legal evidence in Article 5 of the ITE Law still often raises many questions and the proof is still often wrongly done by litigants.

2 Research Method

The method used in writing this paper is a normative juridical legal research method, a normative legal research method, or a library law research method is a method used in legal research conducted by examining existing library materials [3]. The legal materials used in this study can be classified into 3 types, namely:

1. Primary legal materials, namely legal and statutory provisions relating to this research;
2. Secondary legal materials, in the form of written literature in the form of books, papers, research reports, newspaper articles, and so on related to the subject matter of this research;

3. Tertiary legal materials are explanatory materials regarding primary and secondary legal materials in the form of dictionaries, encyclopedias, and so on [4].

3 Findings and Discussion

3.1 Position of Electronic Documents as Evidence

Electronic evidence was first regulated in 1997, namely in Law no. 8 of 1997 concerning Company Documents. The law does not explicitly state the word electronic evidence, but article 15 states that data stored on microfilm or other media is considered valid evidence 9. The word electronic was first raised in Law No. 20 of 2001 which is an amendment to Law no. 31 of 1999 concerning the Crime of Corruption. Article 26A states that information stored electronically is evidence of instructions. This is emphasized again in the ITE law in Article 5 which states that electronic information, electronic documents, and their printouts are recognized as legal evidence. Based on these regulations, the definition of electronic evidence is data stored and/or transmitted through an electronic device, network, or communication system. This data is needed to prove a crime that occurred in court, not the physical form of the electronic device. Information technology itself is defined as a technique for collecting, preparing, storing, processing, announcing, analyzing, and/or disseminating information, as stipulated in Article 1 paragraph (3) of the ITE Law.

Proof is an important process in determining whether a person is wrong or not and also whether a case is clear or not, the notion of proof is an act to prove. To prove in this case is to give or show evidence, to do something the truth, to carry out signifies witnessing and convincing. According to Prof. Dr. Eddy O.S. Hiariej in his book "Theory and Law of Evidence" the law of proof as explained is the provisions regarding evidence which include tools, evidence, evidence, as well as how to collect and obtain evidence to the submission of evidence in court as well as the strength of proof and the burden of proof.

Electronic evidence has a weakness in terms of proof because virtual letters/deeds are very vulnerable to be changed, falsified or even made by people who are not actually the parties who are authorized to make them but act as if they are parties who in fact, as often happens in hoax news.

According to Article 1 point 4 of the ITE Law, Electronic Documents are any Electronic Information created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar forms that can be seen, displayed and/or heard through a computer or system. Electronics include but is not limited to writing, sound, pictures, design maps, photographs or the like, letters, signs, numbers, codes, access, symbols or perfocations that have meaning or meaning or can be understood by people who are able to understand them.

Article 5 of the ITE Law explains that electronic evidence is legal evidence in court.

a. Electronic Information and/or Electronic Documents and/or their printouts are valid evidence.
b. Electronic Information and/or Electronic Documents and/or their printed results as referred to in paragraph (1) is an extension of valid evidence in accordance with the procedural law in force in Indonesia.
c. Electronic Information and/or Electronic Documents are declared valid if they use the Electronic System in accordance with the provisions of this law.
d. The provisions regarding Electronic Information and/or Electronic Documents as referred to in paragraph (1) do not apply to: a. Letters which according to the law must be made in written form; and b. The letter and its documents which according to the law must be made in the form of a notarial deed or a deed made by the deed making official.

Prior to the enactment of the ITE Law in force in Indonesia, formally juridical had not used documents or electronic information as evidence in court. Based on the provisions of Article 164 HIR and 284 RBg as well as Article 1866 of the Criminal Code, there are five pieces of evidence in civil cases in Indonesia, namely written evidence, witness evidence, suspect evidence, confession evidence, and oath evidence. Along with the times and technology, electronic evidence, especially electronic documents, is increasingly being used as evidence in civil cases. Not just any electronic information or electronic document can be used as legal evidence. In Article 6 of the ITE Law, electronic information or electronic document is declared valid and can be used as evidence in court if it fulfills the applicable provisions and is regulated in the ITE Law, namely a reliable and secure electronic system, and fulfills the requirements.

The ITE Law does not explain what is meant by the expansion of legal evidence. However, Article 5 paragraph (2) of the ITE Law provides important instructions regarding this expansion, namely that the expansion must be in accordance with the applicable procedural law in Indonesia. Referring to the previous discussion, this expansion implies expanding the scope or scope of the evidence regulated in Article 184 of the Criminal Procedure Code and regulating it as other evidence, namely increasing the amount of evidence provided for in Article 184 of the Criminal Procedure Code. Referring to the provisions regarding evidence regulated in the Criminal Procedure Code, in accordance with the procedural law applicable in Indonesia, the meaning is that there must be a testing tool for electronic evidence so that the evidence can be declared valid in court, the same as for other evidence, namely formal requirements and material requirements.

The use of electronic systems has created a new perspective in addressing the development of technology. In this case, the intended perspective is a paradigm shift from paper-based to electronic-based. Information in electronic based is increasingly recognized for its efficiency, both in terms of making, processing and storing electronic information [5]. An understanding of the differences in the authenticity of conventional and electronic evidence, namely:

No	*Paper Based*	*Electronic Based*
1	General understanding: 1. Written 2. Signed 3. Original (Original)	1. What has been written or saved can be recovered. 2. There is information that finds responsible legal subjects. 3. What is stored and found remains unchanged (its integrity is guaranteed).
2	Stamped is enough	Can be done by e-registry and e-filing
3	1. The physical presence of the party directly appearing with the notary (Article 16 paragraph 1 letter l). 2. Reading of the deed in front of the parties and the parties understand, unless the parties do not ask for it to be read out (Article 16 paragraph 7). 3. The presence and signature of witnesses who are not related by blood or marriage, unless otherwise stipulated by law (Articles 39 and 40). 4. Initials of the parties, witnesses and notaries on each page as an act of approval.	1. Electronic recording (video) + eID tracing 2. Elucidation of Article 16 paragraph 1 letter l explains physical presence 3. 3G mobile facilities have made it possible to prove whether the person is really in a certain area. 4. Time-stamping proves the logical number of deeds?

The interesting thing about the existence of this electronic evidence is that in the use of electronic information technology or the internet, electronic evidence has become a very hot issue. Apart from Indonesia, there are several countries that recognize electronic evidence, namely Singapore, Japan, China, Chile and Australia, which regulate the legal system in which the recognition of electronic data as evidence in court. Article 5 paragraph (1) of the ITE Law, it has provided a legal basis, namely that electronic information capable of producing printed results is an extension of a valid evidence as in accordance with the procedural law in force in Indonesia. The expansion in question is that electronic evidence adds to the evidence that has been previously regulated in the Indonesian criminal procedure law.

The position of electronic document evidence in civil cases can now be said to no longer have to be guided by the type of evidence which has been limitedly determined by the laws and regulations. The pattern and behavior of human life that is increasingly developing, can affect the traffic in civil relations that lasts to this day. The existence of the ITE Law is used as a form of regulation that is recognized as an electronic transaction in the traffic of civil relations, and can be used as a form of evidence in court can have a considerable influence on current legal developments. In criminal procedural law, the strength of all evidence is essentially the same, no one exceeds the other. Evidence in criminal procedural law does not recognize hierarchy. It's just that there are provisions that require the connection between one evidence and another. Therefore, in criminal procedural law, there is complementary evidence.

In the book Dr. Eddy Army "Electronic Evidence in Judicial Practice" explains several types of electronic evidence, the Ministry of Communication and Information (Kemenkominfo) classifies the types of electronic evidence submitted to the Scientific

Working Group on Digital Evidence in 1999, namely: 1. E-mail, E-mail address (electronic mail), 2. Word Processor/Spreadsheet files, 3. Software source code, 4. Image files (jpeg, tips, etc.), 5. Web Browser Booksmark, 6. Cookies, calendar, to-do list.

Evidence from electronic information and electronic documents is very vulnerable to be manipulated. So that the authenticity of electronic information evidence and electronic documents is very important in proof. According to Anugrah, the validity of electronic information evidence and electronic documents is still very much needed for further proof. This evidence is closely related to the originality of electronic information evidence and electronic documents. Considering the assessment of the validity of electronic information evidence and electronic documents is very difficult, because the existence of electronic information evidence and electronic documents should not harm other people. In addition to the problem of originality of electronic information evidence, and electronic document in making a data or document as valid evidence in proving a criminal case is the problem of collecting data that can be used as evidence.

Because in taking evidence is not easy. The second reason is because until now there is no Standard Operating Procedure (SOP) in taking electronic evidence. Whereas considering cases that intersect with cyberspace and electronics have developed. Considering that it is the investigator who is in charge of collecting evidence, it is necessary to immediately SOP from the investigator in relation to the collection of electronic information evidence and electronic documents.

Another thing that needs to be considered in collecting evidence that stores electronic evidence is that there are so many types of tools and media that store information. Given that there are so many types of information storage media and technology, handling also has its own characteristics. In general, digital forensics is divided into 31: a. Computer forensics, namely forensics carried out on computers, laptops, or hard drives and similar storage media. b. Mobile forensics, namely forensics carried out on mobile phones. c. Network forensics, namely forensics carried out on computer networks. d. Audio forensics, which is forensics that is carried out on sound. e. Image forensics, namely forensics is carried out on images. f. Video forensics, namely forensics carried out on video and CCTV.

Based on the ACPO principles mentioned above. The principle of digital forensics is divided into three stages, namely: acquisition, examination and analysis, as well as documents and presentations. Regarding retrieval, considering that it cannot be changed, damaged, or removed if not handled properly, retrieval of information or electronic documents must be carried out by maintaining and protecting their integrity or integrity. In terms of examination and analysis, examination of original electronic evidence generally uses hardware and software specifically made for digital forensics. Examination performs extraction, namely taking all data from the media where the data is stored, including data that has been previously deleted. The examiner also uses a write blocker, which is a tool used to prevent writing to the original data. Examination of the original copy of the electronic evidence, can also make a copy of the copy of the electronic evidence as work material.

3.2 Electronic Document Requirements as Evidence

The requirements specified in the ITE Law are that the conditions for the existence of electronic transactions and/or electronic documents are that both the subject and the system must be certified by [6]:

First, the Reliability Certification Agency, which will carry out administrative functions, which can include: Registration; Physical authentication of business actors; Creation and management of reliability certificates; and Create a list of certificates that have been frozen. As stipulated in Article 10 of the ITE Law.

Second, Electronic Certification Operators, which perform administrative functions, which may include: Registration; Physical authentication of the applicant; Generating and managing public and private keys; Electronic certificate management; and List of certificates that have been frozen. As stipulated in Article 13 and Article 14 of the ITE Law [6].

With the enactment of the ITE Law, new arrangements regarding electronic document evidence are introduced. Based on the provisions of Article 5 paragraph 1 of the ITE Law, it is determined that electronic information and/or electronic documents and/or their printed results are legal evidence. Furthermore, in Article 5 paragraph 2 of the ITE Law, it is determined that electronic information or electronic documents and/or their printed results as referred to in paragraph 1 is an extension of legal evidence and is in accordance with procedural law in force in Indonesia. Thus, that the ITE Law has determined that electronic documents and/or their printouts are valid evidence and are an extension of legal evidence in accordance with procedural law that has been in force in Indonesia, so that they can be used as evidence in court. Furthermore, based on the provisions of Article 5 paragraph 3 of the ITE Law, it is determined that electronic information and/or electronic documents are declared valid if they use an electronic system in accordance with the provisions in the ITE Law [7].

Thus, the use of electronic documents as evidence that is considered valid if using an electronic system is in accordance with the provisions as stipulated in Article 6 of the ITE Law, which stipulates that electronic documents are considered valid as long as the information contained in them can be accessed, displayed, guaranteed its integrity, and can be accounted for, so as to explain a situation. In addition, electronic documents whose position can be equivalent to documents made on paper, as specified in the General Elucidation of the ITE Law. So that electronic documents can be used as evidence of legal instructions according to law.

The validity of the electronic evidence presented at the trial must be maintained, that is, it has fulfilled the requirements and was examined according to the correct procedure. As regulated in Articles 15 and 16 of the ITE Law, electronic systems must:

1. Reliable, safe and responsible.
2. Can display the required Information or Electronic Documents in full.
3. Electronic documents can protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information.
4. Equipped with procedures or instructions and can operate according to the procedures or instructions that have been set.

The power of proof attached to electronic evidence is based on the ITE Law which states that electronic documents are equivalent to documents made on paper. In this case, the idea can be drawn that the power of proving electronic documents in the practice of civil cases is equated with the strength of written evidence (letters). Although so far electronic evidence has been recognized as a valid evidence, the value of the strength of the proof does not yet have a perfect proof value.

According to Munir Fuady [7], there are several criteria or conditions so that evidence in the form of electronic documents can be considered as letter evidence, namely first using the principle of authenticity, meaning that a document or digital letter and the signature are considered original, unless they can prove otherwise. In addition to these principles, Munir Fuady also stated about the integrity of information and the authenticity of documents. In this case, an electronic document or electronic record is considered original if it can provide a guarantee that the document or recording is original, unaltered, complete and at the same time as the time when the manufacturing process was carried out. Furthermore, there is a business notarization, the task of a notary "not only to make authentic deeds but also to register and ratify documents under the hand [8]. Actually, when viewed further, the power of proof of this electronic evidence can use the power of proof of letter evidence and directive evidence. In accordance with the explanation on the validity of electronic evidence above, it is said that electronic evidence is an extension of evidence regulated in the Criminal Procedure Code, namely letter evidence and instructional evidence.

The legal requirement for an electronic document is that it uses an electronic system in accordance with the provisions stipulated in the ITE Law, especially in Article 6 of the ITE Law, namely "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. Thus explaining a situation. In addition, there are also specificities in the implementation of electronic certification and electronic systems as well as electronic transactions.

The Supreme Court's acknowledgment of electronic documents in the judicial system was first known through the Supreme Court Circular Letter (SEMA) Number 14 of 2010 concerning Electronic Documents as Completion of Applications for Cassation and Review. This SEMA aims to improve the efficiency and effectiveness of the case file minutation process as well as support the implementation of transparency and accountability as well as public services at the Supreme Court and the Judicial Body under it. However, this SEMA does not regulate electronic documents as evidence, but electronic documents in the form of decisions or indictments that are included on compact discs, flash disks/sent via email as a complete application for cassation and review.

This SEMA has been amended based on SEMA 1 of 2014 concerning Amendments to SEMA 14 of 2010 concerning Electronic Documents as completeness of the Application for Cassation and Review. This SEMA change was made in relation to the file checking system from a rotating system to an electronically directed shared reading system. In the SEMA points there are additional details of documents that must be submitted by the litigants electronically but once again the importance is not in relation to electronic evidence. Another difference with the old SEMA is the way documents are included through the data communication feature (legal remedies menu) in the Supreme

Court decision directory because the old method through compact disks and sending e-documents has a number of obstacles including unreadable data, missing data storage devices and so on.

In short, the SEMA recognizes that electronic documents are for the completeness of the Application for Cassation and Review, not for trial evidence and the submission of documents by the court of first instance is carried out through the data communication feature and not through flash disk/compact disk devices except in special circumstances. However, the question is how to submit electronic documents as legal evidence in court? This is where there is a void in the procedural law, because the ITE Law and other laws do not regulate the procedure for submitting it in court. If in practice there are those who submit via compact disks or flash disks, according to SEMA 1/2014 it is explained that this causes a number of obstacles, but if sent via e-documents, the delivery procedure has not yet been regulated. The submission procedure is important because it concerns whether the civil procedural law is valid or not and in order to fulfill the element of "guaranteed integrity" in Article 6 of the ITE Law. Guaranteed integrity means that the form has not been changed since the electronic document was ratified.

In the event that the electronic document has been submitted in court according to the procedure accepted by all litigants, then the next question is what if the opposing party wants to see the electronic document that will be submitted as evidence? The provisions of Article 137 of HIR stipulates that "Parties may demand to see their opponent's certificates and vice versa, which letters are submitted to the judge for that purpose". In maintaining the principle of transparency of evidence in court, the provisions of 137 HIR must also be applicable to electronic documents when the opposing party asks to be shown. For this reason, technological devices in the form of laptops or projectors are needed to be able to display/show electronic documents and even this is not regulated.

In addition, electronic documents containing electronic signatures must meet a number of criteria in Article 11 of the UUITE so that they have legal force and legal consequences, namely a. related electronic signature creation data only to the signer, b. the electronic signature creation data at the time of the electronic signing process is only in the power of the signer, c. all changes to the electronic signature that occur after the signing time can be known, d. all changes to the electronic information related to the electronic signature after the signing time can be known, e. there are certain methods used to identify who the signatories are, and f. there are certain ways to show that the signer has given consent to the associated electronic information. The criteria points above also contain aspects of electronic document security as mandated in Article 12 paragraph 1 of the UUITE, including authenticity, integrity, and non-repudiation.

In the context of using electronic documents, what needs to be understood is that the ITE Law prohibits acts as regulated in the provisions of Article 27 to Article 37, which stipulates that if there is an abuse in the use of information technology, especially electronic documents, which is detrimental to other parties, can be sued or prosecuted both civilly and criminally, as specified in Article 38, Article 39, and Article 45 to Article 52 of the ITE Law.

With the inclusion of strict regulations on electronic evidence in the new civil procedure law, it is hoped that judges can examine cases (which use electronic evidence as evidence) to completion and then make a decision, so that legal certainty can be obtained

through the judge's decision in order to provide a sense of justice for the people. Public. Because justice can be achieved on the basis of legal certainty that is applied to certain events or vice versa a legal certainty is achieved on the basis of justice.

4 Conclusion

Based on the explanation of the civil case trial, the evidence in the form of e-mail can be used in the trial. Regarding the legal aspects of the application of e-mail in enforcing the law, with the development of today's technology through communication media known as the internet, it has changed the way of thinking and acting which then has an impact on the law, so there needs to be a clear understanding of evidence in the trial process. After the enactment of the ITE Law, there are additional types of evidence, and the recognition of electronic documents as legal evidence, as stipulated in Article 5 paragraphs 1 and 2 jo.

There is no doubt that Electronic Information and Electronic Documents are legitimate to be used as evidence in court proceedings. However, this electronic document evidence still requires more detailed rules relating to procedures in search and seizure as well as the mechanism for obtaining electronic evidence, as well as other matters that can strengthen the validity of electronic evidence that can have evidentiary value in court.

Although currently there are many laws and regulations in Indonesia that recognize electronic evidence as legal evidence, in fact, the Supreme Court has recognized it since 1988. However, the value of proving electronic data as evidence in court seems to be questionable. In court practice in Indonesia, the use of electronic data as legal evidence is not commonly used. The need for electronic evidence has been expressly regulated in the ITE Law, which provides a legal basis for the legal strength of electronic evidence and the formal and material requirements for electronic evidence to be accepted in court.

Whereas after the enactment of the ITE Law, there were additional types of evidence, and the recognition of electronic documents as legal evidence, as stipulated in Article 5 paragraphs 1 and 2 jo. Article 6 of the ITE Law which stipulates that electronic documents or their printed results are legal evidence and can be used before a trial, as long as the information contained therein can be accessed, displayed, guaranteed for its integrity, and can be accounted for, thus explaining a situation. In addition, electronic documents have the same position as documents made on paper, as specified in the General Elucidation of the ITE Law.

References

1. Johan Wahyudi, 2012, *Dokumen Elektronik Sebagai Alat Bukti Pada Pembuktian Di Pengadilan*, Vol. XVII No.2 May 2012, Jurnal Fakultas Hukum Universitas Airlangga, Surabaya.
2. Bambang Sugeng A.S. dan Sujayadi, 2012, *Pengantar Hukum Acara Perdata Dan Contoh Dokumen Litigasi*, Kencana Prenamedia Group, Jakarta, p. 64.
3. Soerjono Soekanto dan Sri Mamudji, 2009, Penelitian Hukum Normatif Suatu Tinjauan Singkat, Cetakan ke – 11, PT Raja Grafindo Persada, Jakarta , p. 13.
4. Amirudin dan Zainal Asikin, 2008, Pengantar Metode Penelitian Hukum, PT Raja Grafindo Persada, Jakarta, p.30

5. Edmon makarim, 2005, *Pengantar Hukum Telematika Suatu Kompilasi Kajian*, PT. Raja-Grafindo Persada, Jakarta, p. 415.
6. Minanoer Rachman. 2012. *Bahan Seminar Penggunaan Informasi atau Dokumen Elektronik Sebagai Alat Bukti dalam Proses Litigasi*. Surabaya: FH.UNAIR. p. 10.
7. Penjelasan Pasal 5 ayat (3) Uundang Uundang ITE.
8. I Ketut Tjukup, et.al., 2016, *"Kekuatan Hukum Pembuktian Waarrmerken (Akta di Bawah Tangan yang Didaftarkan) Di Notaris"*, Jurnal Ilmiah Prodi Magister Kenotariatan, Fakultas Hukum Universitas Udayana, p. 154.