The Validity of Electronic Evidence as an Expansion of Evidence in the Criminal Justice System

Taun[1], Imanudin Affandi[1], Rahman[2], Muhammad Rusli Arafat[1]

[1] Faculty of Law Singaperbangsa University, Karawang, Indonesia
[3] Faculty of Social Science and Political Science Singaperbangsa University, Karawang, Indonesia
taun@fh.unsika.ac.id

Abstract. The criminal procedural law has not regulated electronic evidence, this is a problem because along with the development of technology many crimes use electronic media, so it has become a legal deadlock for the community, with the promulgation of the Law on Electronic Information and Transactions which regulates electronic evidence has become a legal problem, but there is still a lot of confusion about criteria such as what electronic documents can be categorized as electronic evidence. This research uses a qualitative approach method, data analysis in this study is a case study data analysis that is descriptive analysis, the source of this research data is sourced from primary legal materials, secondary legal materials, tertiary legal materials, field research. Data collection techniques are using literature studies (*library research*,) interviews, studies (review) documents, then The data analysis technique used in this study is qualitative data analysis. if it is related to the substance of this study, namely the Criminal Procedure Code as a general rule that regulates evidence in crime, namely in the form of witness evidence, expert statements, letter butki, instructions and statements of the accused. But then since the promulgation of the ITE Law, the evidence has expanded, namely with the emergence of electronic evidence, the electronic evidence can be said to be valid if obtained from an electronic system with the conditions regulated in the ITE Law, namely electronic documents that can be re-aired if needed in a trial using electronic devices

Keywords: criminal justice, electronic evidence, evidence.

1. Introduction

The development of the internet can be said to be a double-edged sword, on the one hand contributing to the improvement of welfare, progress and at the same time also being an effective means of unlawful acts.[1] Online business practitioners from abroad can take advantage of this condition to create a target market to Indonesia.[2] In addition to the positive impact, that the internet has a negative impact with the emergence of opportunities to commit antisocial acts and criminal behavior.[3] Crime in the field of electronic information and/or electronic transactions today is very concerning and its impact has become global.[4]

Regulation Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) is the first law in Indonesia that specifically regulates cyber crime. Two large content materials regulated in the ITE Law are regarding the regulation of

A. A. Nassihudin et al. (eds.), *Proceedings of the 3rd International Conference on Law, Governance, and Social Justice (ICoLGaS 2023)*, Advances in Social Science, Education and Humanities Research 805,
https://doi.org/10.2991/978-2-38476-164-7_101

electronic transactions and regarding cyber crime.[5] The content contained in the ITE Law is an application of the principles contained in international provisions, namely the United Nations Commission International Trade Law (UNCITRAL) related to EU Directives on Electronic Signature, EU Directives on Electronic Commerce, Convention on Cybercrime, Model Law on Electronic Signature, and Model Law on Electronic Commerce. These arrangements are the content of rules regulated in international and regional instruments that are generally applied in Asia, America and Europe.[6]

Technological developments have encouraged changes in behavior, and one of them is dependence on computers. Whether we realize it or not, with current technology, computer users can store or transmit information in various forms and in very much quality. People do not need long to receive the latest information from relatives thousands of kilometers away. Simply by email or sms then the latest news can be obtained.[6]

A little bit about the conditions that occur in this society can cause various issues in solving criminal acts in the field of information technology. Such conditions create problems in proving information that is processed, stored, or transmitted electronically. Electronic information or documents that are easily changed often raise legal questions regarding the authenticity of the information or document in question. The ease with which a person uses any identity to carry out various types of electronic transactions anywhere can make it difficult for law enforcement officials to determine the identity and location of the real perpetrator.[6]

In this study has novelty when compared to previous research, which is a comparison in the articles of A. A. Mokosolang, R. S. M. Korah., and R. S. Mamengko, "The Legal Power of Electronic Mail as Civil Case Evidence (Based on Law Number 19 of 2016 concerning Electronic Information and Transactions), this study focuses on evidence in the realm of civil law, while in the author in the article explains electronic evidence in the field of punishment. Then in the article N. L. A. K. Isma, "The Power of Proof of Electronic Information Evidence on Electronic Documents and Their Printouts in Proving Criminal Acts," this article explains about electronic evidence in the form of printed results, but the author discusses electronic evidence both printed and those in electronic devices, then the next article I. G. A. A. A. Sedana, Denira Palmanda; Krisnawati, "The Position and Power of Electronic Evidence," explains the power of electronic evidence, while the author expands to the validity of what kind of electronic evidence can be used as evidence at trial.

Questions that still often arise in the general public, including law enforcement officials, are related to legitimate evidence derived from electronic documents, then related to electronic evidence that is the basis for the running of the criminal justice system in Indonesia, and how electronic evidence can be accepted in court as legal evidence will be an important topic in cyber law enforcement in Indonesia, especially with the enactment of the ITE Law.[6]

2. Problems

The problem in this study is the first how to expand evidence in the criminal justice system, the second is how the criteria for electronic documents that can be used as evidence in the criminal justice system.

3. Method

Seeing the problems that include this research requires a deep enough understanding to be able to understand the arrangement of cryber cryme evidence, so this study uses a qualitative approach method. According to John W Cresswell[7] stated that "a qualitative research approach is basically a process of inquiry to understand social problems holistically which is formed by a series of words, describes the view of information in detail, and is arranged in a natural background".

The data analysis used in this study is a case study data analysis that is descriptive analysis. Parsudi Suparlan in Farouk Muahammad and Djaali[8] states that case studies must use anthropology, which requires researchers to live or be among the subjects to be studied in sufficient time so that researchers can live connected or side by side with the object to be studied.

In obtaining data to support the preparation of this study, the following data were used:

a. Primary legal materials

Is a binding document and determined by the competent authority. In this study include:

1) Constitusion of Republik Indonesia 1945;
2) Law Number 18 of 1981 concerning Criminal Procedure Law; and
3) Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions

b. Secondary legal materials

That is, all documents are studies or information related through aspects of civil procedural law, magazines, legal journals, newspapers, and some sources from the internet related to research problems.

c. Tertiary legal materials

All documents that contain concepts and explanations that provide material support for secondary and primary legal materials, such as encyclopedias, dictionaries, and others.

d. Field research is carried out to obtain primary data practically as a secondary data support, by conducting in-depth interviews.

The data collection techniques used in this study are:

a. Library research, this research is carried out through the review of library materials in order to obtain secondary data in the form of books both owned by the researcher himself and from articles, libraries, both obtained from electronic media, print media and state documents, including laws and regulations;

b. Interview, is a method of collecting data by means of communication, namely by personal relationship or contact between the data collector (interviewer) and the source of information. There are three main techniques in the interview process, namely: 1). Structured interviews; 2). Semi-structured interviews; and 3). Unstructured interviews;

c. Document study, document review is a way of collecting data carried out through the review of existing documents so that they can be studied in terms of facts or knowledge to be researched.

4. Discussion

4.1. Expand Evidence In The Criminal Justice System

In general, the difference between electronic information/documents and letters/documents in conventional form lies in their form and nature. In addition, obtainability, availability, and content are other differentiators. Electronic information or documents can be easily obtained as they can be easily created and sent instantly and the recipient of the information or document can receive it more quickly. On the other hand, information contained in paper takes longer to send and obtain – including considerable effort and expense.[9]

In addition, unlike paper which requires a larger physical storage area, electronic information or documents can be stored in a much smaller medium for a considerable amount of time. Parties who need the paper will need a long time to find it, but computers that exist today are equipped with file or data search applications.

Every internet user can use a search engine to obtain the required information equipped with features to find detailed information. The third thing that distinguishes electronic information or documents from paper is that electronic information or documents in their original form often contain more important information that cannot be found when the information or document is printed.[10]

The criminal justice system has several processes and mechanisms in achieving justice, one of which is very important, which is related to the process of proving a case as a determinant of material truth, making light of a case and determining the perpetrators of a criminal act. Therefore, law enforcement in the process of law enforcement both from the level of investigation, investigation, prosecution to the stage of the trial process in court will process and reconstruct criminal principles to find the perpetrators of a criminal event, this can be obtained

from the testimony of witnesses, written evidence contained in documents related to criminal events, expert statements that can provide academic explanations and very expert expertise Needed in determining a criminal act, these legal facts are used as evidence.[6]

Evidence in criminal justice in Indonesia, as stipulated in Article 183 of the Code of Criminal Procedure,[1] adheres to the system of evidence according to the law negatively (negatief wettelijk stelsel), meaning that the guilt of the accused must be proven based on:[11]

a. Evidence tools and methods of proof regulated in law; and
b. The judge's conviction based on the evidence and the manner of proof.

The two elements above are a unity. A person cannot be found guilty based on the judge's conviction alone. The judge's conviction must have a source, and that source is the legal facts (legal events that occur concerning or related to a criminal act and the perpetrator of the crime) contained or given by evidence that has been predetermined in law. Conversely, even if the evidence presented shows that the defendant is guilty, the judge cannot convict him without a conviction based on the evidence presented – the legal facts are fabricated and the witness can forget the legal events that occurred, for example.[12]

The system of evidence according to the law negatively (negatief wettelijk stelsel), has the following meanings:

a. To convict a defendant (accused) a minimum of proof is required, which is established by law;
b. However, the amount of evidence is not enough to determine a criminal act, if the judge does not have confidence in the guilt of the defendant committed, then when the judge does not have confidence in the guilt of the defendant, the judge may not sentence the defendant.[11]

So in that system, what ultimately determines the fate of the accused is the judge's belief. If, even if the evidence is piled up, the judge is unsure of the defendant's guilt, he must acquit him. Therefore, in each decision of the criminal judge, who handed down the sentence, we can read the consideration, "that the judge, based on valid evidence, believes in the guilt of the accused.[11]

Evidence regulated in the Criminal Procedure Code has five forms of evidence, namely first witness evidence, namely people who see, hear or experience a criminal event themselves, second expert testimony, namely people who based on their expertise can explain a criminal event academically or scientifically based on their science, third evidence clues, namely a series of witnesses, evidence or others that lead to information about the occurrence of a criminal event, The four statements of the defendant, namely the defendant as the perpetrator who committed the crime can be in the form of confessions or other information that explains the occurrence of criminal events.[13] All provisions of evidence are explained and regulated in a

gambling manner in the Criminal Procedure Code so that the course of the trial can be based on valid evidence.[6]

The Criminal Procedure Code as a legal basis that regulates evidence has not explained clearly what legal evidence is like, but along with the advancement of information technology also moves hand in hand with the development of types of criminal acts that utilize information technology media so that supporting provisions are needed related to proving criminal acts using information technology media, In some laws and regulations there is no uniformity regarding electronic evidence, but with the promulgation of the Law on Electronic Information and Transactions, the problem can be answered with electronic evidence that adjusts to criminal acts related to information technology.[14]

Provisions related to electronic evidence as stipulated in the ITE Law are regulated in chapter III which explains related to information, documents and electronic signatures in Article 44, then Article 5 paragraph (1) of the ITE Law which expressly explains that electronic information or documents and / printouts are valid legal evidence.[15] Furthermore, Article 5 paragraph (2) of the ITE Law confirms that electronic information and/or electronic documents and/or printouts are extensions of valid evidence in accordance with the applicable procedural law in Indonesia.[15]

The evidence system in Indonesia as previously explained, namely in determining a criminal event and determining the guilt of the defendant, the minimum requirement of proof must be met, namely at least two pieces of evidence that point to the defendant, and based on evidence and the trial process the judge has a belief in the guilt of the defendant, This also applies to the collection and presentation of electronic evidence both in original and printed form, obtained either by confiscation or print, obtained either by confiscation or interception.

The Code of Criminal Procedure has provided clear regulations for forced searches and seizures in general, but not yet on electronic systems. However, the Criminal Procedure Code does not regulate interception or wiretapping, this is regulated in various more specific laws. Therefore, formal and material provisions and requirements regarding electronic evidence must refer to the Criminal Procedure Code, the ITE Law, and other laws that specifically regulate electronic evidence.[6]

What is meant by material requirements are provisions and requirements intended to ensure data integrity, availability, security, authenticity, and accessibility. Electronic information or documents in the process of collection and storage in the process of investigation and prosecution, as well as their submission in court proceedings. In this case, a branch of discipline is needed in the field of computer forensics (computer forensic) or digital forensics (digital forensic), namely a branch of forensic science pertaining to legal evidence found in computers and digital storage media. Cabang This science is important considering:

> *Electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve, and*

examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.[6]

4.2. The Criteria For Electronic Documents That Can Be Used As Evidence In The Criminal Justice System

The provisions for electronic evidence in order to be used as valid evidence must be in accordance with the provisions of Article 5 paragraph (3) of the ITE Law, namely electronic information or documents can be declared valid if using an electronic system or in other words all document files or any form obtained from the electronic system regulated in the ITE Law can be categorized as valid evidence. Furthermore, electronic systems are regulated in articles 15 to 16 of the ITE Law and from these two articles, more detailed requirements can be obtained, namely that electronic systems:[6]

a. The Information System has reliability, has information security, and can be accounted for;

b. The Information System can be shown again both in the form of information and electronic documents as a whole;

c. The information system must be able to provide protection, integrity, availability, confidentiality, and authenticity that can be accessed easily;

d. The information system is accompanied by clear ways of use and instructions and procedures that have been determined and the information system can be run and operate properly in accordance with the procedure.

Then it is also regulated in Article 6 of the ITE Law, the article provides an explanation regarding the requirements for the validity of electronic evidence obtained from electronic information systems, namely with the provision that information or documents obtained from the electronic system can be displayed, accessed, guaranteed to be intact, and can be accounted for so that from these provisions the evidence can make light of a criminal event.[6]

In the ITE Law related to electronic evidence, the Law is not regulated in detail related to the way or method of obtaining the evidence in terms of how to collect, secure, guarantee the integrity and reappearance of the information, this is not regulated in the ITE Law,[16] meaning that the ITE Law provides freedom to any electronic information system in carrying out the method or method of proof as long as the evidence obtained meets the requirements for validity electronic evidence, or in other words, the ITE Law adheres to technology-neutral principles.[17]

Meanwhile, the formal requirements for electronic evidence are regulated in Article 5 paragraph (4) and Article 43 of the ITE Law, namely:

a. Such information or electronic documents are not:

   1) A letter that by law must be made in written form;

   2) The document or letter based on laws and regulations must be made

directly by the authorized official, such as the requirement for a letter made in the form of a notarial deed or land deed making official.

b. A search or seizure of an electronic system must be conducted with the permission of the local Chief Justice;
c. Search or seizure while maintaining the interests of public services;

In the event that the electronic system used has met these requirements, the quality of electronic evidence in its original form (electronic information or electronic documents) and printouts of electronic information or documents are the same. In other words, police, prosecutors, and judges can use both or either of them. However, keep in mind that in certain cases there are times when the use of electronic evidence is more appropriate than the use of printed results of electronic information or documents because the information or electronic documents can provide information that cannot be provided if the electronic information or documents are printed.[6]

Which electronic evidence was used? Is it in its original form or has it been printed? This of course can be seen case by case. One example is in the case of robbery recorded on cctv, the electronic documents recorded by cctv should be presented in their original form. Videos can contain both moving and soundful images. The use of evidence in its original form will make it easier for law enforcement officials to understand the legal facts recorded in the video. Law enforcement officials can also print every move of the perpetrator when carrying out a recorded robbery, but this will certainly require so much paper that it is not effective. [6]

However, in certain cases the use of printed pieces of information or electronic documents makes it easier for law enforcement officials to present them in court. One example is in the crime of extortion sent via SMS or email. In such cases, the use and presentation of printed results from SMS or email obtained from a mobile phone or computer makes it easier for law enforcement officials to assess legal facts. In principle SMS or email is the same as writing, but in electronic form. Therefore, as long as the SMS in the mobile phone in question has been checked for integrity, availability, and authenticity or originality as well as its relevance to the case in question, then the printed SMS is sufficient as evidence.[12] Police or prosecutors do not need to bring, demonstrate and show SMS on the mobile phone in court because it will require more time and costs.[6]

5. Conclusion

Provisions related to electronic evidence as stipulated in the ITE Law are regulated in chapter III which explains related to information, documents and electronic signatures in Article 44, then Article 5 paragraph (1) of the ITE Law which expressly explains that electronic information or documents and / printouts are valid legal evidence. Furthermore, Article 5 paragraph (2) of the ITE Law confirms that electronic

information and/or electronic documents and/or printouts are an extension of valid evidence in accordance with the applicable procedural law in Indonesia.

The provisions for electronic evidence in order to be used as valid evidence must be in accordance with the provisions of Article 5 paragraph (3) of the ITE Law, namely electronic information or documents can be declared valid if using an electronic system or in other words all document files or any form obtained from the electronic system regulated in the ITE Law can be categorized as valid evidence. Furthermore, electronic systems are regulated in articles 15 to 16 of the ITE Law and from these two articles, more detailed requirements can be obtained, namely that electronic systems:

a. The Information System has reliability, has information security, and can be accounted for;
b. The Information System can be shown again both in the form of information and electronic documents as a whole;
c. The information system must be able to provide protection, integrity, availability, confidentiality, and authenticity that can be accessed easily;
d. The information system is accompanied by clear ways of use and instructions and procedures that have been determined and the information system can be run and operate properly in accordance with the procedure.

Then it is also regulated in Article 6 of the ITE Law, the article provides an explanation regarding the requirements for the validity of electronic evidence obtained from electronic information systems, namely with the provision that information or documents obtained from the electronic system can be displayed, accessed, guaranteed to be intact, and can be accounted for so that from these provisions the evidence can make light of a criminal event.

References

[1] A. S. Alkarni and T. Taun, “Upaya Kepolisian Dalam Pencegahan Kejahatan Judi Online (studi Kasus Judi Slot),” vol. 9, no. 4, pp. 55–59, 2023.
[2] R. Apriani, P. S. Putra, T. Taun, and M. R. Arafat, “Sosialisasi Dalam Upaya Menyelamatkan Koperasi Di Karawang Pada Masa Pandemi Covid-19,” *Al-Khidmat*, vol. 5, no. 1, pp. 32–38, 2022, doi: 10.15575/jak.v5i1.13838.
[3] S. Fatimah and T. Taun, “Tinjauan Yuridis Terhadap Pelaku Tindak Pidana Perjudian Online di Indonesia,” *Innov. J. Soc. Sci. Res.*, vol. 3, no. 2, pp. 3224–3231, 2023.
[4] S. Sunarso, *Hukum Informasi dan Transaksi Elektronik*. jakarta: PT.Asdi Mahasatya, 2009.
[5] N. L. A. K. Isma, “Kekuatan Pembuktian Alat Bukti Informasi Elektronik Pada Dokumen Elektronik Serta Hasil Cetaknya Dalam Pembuktian Tindak Pidana,” *J. Penelit. Huk.*, vol. 1, no. 2, pp. 109–116, 2014.
[6] J. Sitompul, *Cyberspace, Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2012.
[7] J. Cresswell, *Research design qualittaive & quantitative Approaches*, Terjemahan. Jakarta: KIK Press, 2002.

[8] F. M. & Djaali, *metode penelitian sosial*, Revisi. jakarta: PTIK Press & Restu Agung, 2005.
[9] S. M. B. P. Affiza, "Upaya Pembuktian dalam Tindak Pidana Pencemaran Nama Baik melalui Sarana Elektronik Menurut Undang-Undang Informasi dan Transaksi Elektronik," *J. Verstek*, vol. 10, no. 8.5.2017, pp. 2003–2005, 2022.
[10] I. G. A. A. Sedana, Denira Palmanda; Krisnawati, "Kedudukan Dan Kekuatan Surat Elektronik," *Progr. Kekhususan Peradil. Fak. Huk. Univ. Udayana*, vol. 7, p. 1, 2018.
[11] R. Subekti, *Hukum Pembuktian*. Jakarta: Pradnya Paramita, 2010.
[12] A. A. Mokosolang, R. S. M. Korah., and R. S. Mamengko, "Kekuatan Hukum Surat Elektronik sebagai Alat Bukti Perkara Perdata (Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik)," vol. 3, no. 04, pp. 215–225, 2023.
[13] K. A. C. T. Dewi, "Kedudukan Alat Bukti Elektronik dalam Hukum Acara Pidana Indonesia," *Kertha Wichara*, vol. 8, no. 7, pp. 1–18, 2019.
[14] F. Sugiarto and D. Siregar, "Pembuktian Hukum Dalam Kejahatan Dunia Maya," vol. 10, pp. 216–223, 2022.
[15] B. Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime)*. Jakarta: Rajawali Pers, 2012.
[16] J. Rizki, P. Permono, M. Tjoanda, and P. Radjawane, "Kekuatan Alat Bukti E-mail Dalam Persidangan Perkara Perdata kebudayaan yang baru , yang dimana hubungan antara manusia pada tataran global saat ini," vol. 2, no. 82, pp. 467–479, 2022.
[17] R. A. A. D. Priyadi and Taun, "Penegakan Hukum terhadap Penipuan Melalui Media Elektronik," *J. Prefer. Huk.*, vol. 1, no. 2, pp. 72–77, 2020, doi: 10.22225/jph.1.2.2345.72-77.