

Challenges Of Electronic Evidence In Law Enforcement In The Era Of Digital Technology

Guna Harta
Universitas Nusa putra
gseramby@gmail.com

ABSTRACT

Evidence in court plays an important role in a case. This is the basis for judges in viewing a legal event. Criminal acts in the modern era, a sophisticated electronic technology has become a new tool for perpetrators of criminal acts, where these perpetrators take advantage of the complexity and speed of technology. This requires law enforcement officers to rely on electronic evidence (digital evidence) in uncovering a crime. However, the existence of electronic-based evidence in Indonesian criminal procedure law faces fundamental legal challenges, such as in terms of legal construction, authenticity standards, and its application in court. This study aims to analyze the effectiveness of electronic evidence. The definition of evidence in Law 1 of 2024, concerning Amendments to Law Number 11 of 2008 concerning electronic information and transactions (ITE Law). This study uses Normative Jurisprudence with a conceptual legislative approach. The research findings indicate that although electronic evidence has been explicitly recognized as valid evidence, its practical implementation still faces challenges, including doubts among judges regarding its authenticity, technical complexity requiring specialized expertise, and inconsistent presentation standards in court. Further harmonization, socialization, and increased capacity of law enforcement in handling electronic evidence are needed to ensure the effectiveness of money laundering eradication efforts.

Keywords: Validity of electronic evidence, money laundering crimes, TPPU Law, ITE Law

INTRODUCTION

Electronic evidence as a whole plays a very important role in handling a case, in the era of modernization of technological advances, there is a significant legal challenge (Tanoto, E., Tandy, J., & Banke, R., 2024) namely in the form of how the validity of electronic evidence is where the criminal procedure law system in Indonesia itself is still based on Law number 8 of 1981 concerning criminal procedure law (KUHAP), where the Criminal Procedure Code only regulates conventional evidence mentioned in the provisions of Article 184 of the Criminal Procedure Code, namely witness statements, expert statements, letters, instructions, and statements from the defendant. The types of electronic evidence consist of digital information and digital documents (Waruwu, P., R., R., Supreme Court of the Republic of Indonesia, 2018).

The provisions of the procedural law do not mention electronic evidence as a stand-alone form of evidence. Electronic evidence is recognized as independent only in Article 181 of Qanun No. 7 of 2013 concerning Jinayat Procedural Law related to the procedural law of Jinayat cases in Aceh (Ma'arif, S., HukumOnline, 2024). Electronic documents do not yet have regulations on procedures for their submission in court, procedures for showing them to the opposing party, and regulations are currently being drafted regarding the standardization of electronic certification service providers (Waruwu, 2018).

Article 1 number 1 of the ITE Law explains that digital information is one or a set of digital information, which includes, but is not limited to, writing, sound, images, maps, designs, photos, electronic data interchange (EDI), email, telegram, telex, copies of text or similar, letters, signs, numbers, codes, access, symbols or perforations that have been processed that have meaning or can be understood by people who can understand them.

The existence of electronic evidence is forced into the category of "letters" or "instructions," which raises evidentiary issues (Ma'arif, S., 2024). Law Number 1 of 2024 concerning Information and Electronic Transactions (UU ITE) provides a more comprehensive legal basis for electronic information and documents as evidence.

The system of evidence in civil cases that has been in effect in Indonesia binds judges to valid evidence based on civil procedural law (Ma'arif, S., 2024). Evidence includes letters, witnesses, allegations, confessions and oaths. The conditions required by electronic evidence are, namely, authenticity, data integrity, and accountability. These conditions are absolute requirements for electronic evidence so that it can be presented at trial.

METHODS

This study uses normative legal research. This research analyzes how the intensity of legal rules with applicable legal norms in analyzing commands and prohibitions based on applicable legal principles. The legal materials used include primary and secondary legal materials. To describe the findings of the research obtained.

DISCUSSION

Construction Of Proof

The evidentiary system plays a crucial role in investigating crimes related to information and electronic transactions (Tanoto, E., Tandy, J., & Banke, R., 2024). Through evidentiary

systems, we attempt to gather explanations using evidence and materials. This aims to ensure the judge is confident in whether the defendant's alleged wrongdoing is true.

Because if the evidence does not meet the absolute requirements of evidence to prove the defendant's guilt, the defendant is acquitted of all charges against him. However, if the defendant is proven guilty through the evidence, the defendant must be subject to the applicable sanctions.

The regulation of electronic evidence in the context of criminal law in Indonesia has experienced significant progress along with the development of information technology. The position of electronic evidence is primarily regulated by Law Number 11 of 2008, entitled "Information and Electronic Transactions" (UU ITE), which was later amended through the ITE Law. This is the first law in Indonesia to specifically regulate cases related to cybercrime and electronic transactions, including aspects of evidence.

Proving crimes in electronic information and transactions using electronic evidence in accordance with Article 5 paragraph 1 of the ITE Law paragraph (1) basically explains that electronic information and documents are valid evidence. Information in electronic form and/or electronic documents are considered valid if they use an electronic system that is recognized as valid in accordance with the rules stipulated in this Law.

In practice, the provisions regarding electronic information and/or electronic documents, as described above, often face conflict. Letters are legally required to be in writing; and letters and all related documents are legally required to be in the form of a deed drawn up by a notary or a deed prepared by a deed maker. According to what is explained in Article 5 of the ITE Law that has been mentioned, the author concludes that there is an expansion that the types of evidence in proving crimes related to electronic information and transactions include electronic data, electronic documents, and copies thereof.

Electronic data, electronic documents, and copies made from these documents are developments in the category of evidence that is legally recognized based on the legal regulations in force in Indonesia, namely Law Number 8 of 1981 concerning the Criminal Procedure Code (KUHAP).

Evidence that is legally recognized based on Article 184 of the Criminal Procedure Code, consists of: Witness statements, Expert statements, Documents, Clues, Defendant's statements. Evidence is very important because according to Article 183 of the Criminal Procedure Code, the judge **may not impose a penalty** except if with at least two valid pieces of evidence he is convinced that a crime actually occurred and the defendant is guilty of

committing it (Law Number 8 of 1981). The judge must be convinced that a crime actually occurred and that the defendant is the person who committed the act.

Proof in criminal cases involving electronic information and transactions as a basis for charges from the public prosecutor needs to follow valid evidence as stipulated in Article 5 of the ITE Law and Article 184 of the Criminal Procedure Code. The evidence must truly reflect the facts, meaning it must not be fabricated. According to Article 187 of the Criminal Procedure Code, what is meant by a Letter as explained in Article 184 paragraph (1) letter c is a document and other letter in an official format made by a public official who has power or made in front of them which contains information regarding events or situations that they have noticed, observed, or experienced directly, accompanied by a clear and definite explanation regarding the information.

A letter written by an expert containing their expert opinion on a matter or situation officially requested. Other letters are valid only if they are related to the contents of other evidence. Concerning indicative evidence, indicative evidence is actions, situations, or conditions that are closely related to each other and to the crime itself, indicating that a crime has occurred and who committed it.

An article in the CAUSA (Journal of Law & Citizenship) journal explains that electronic evidence ("electronic documents") is sometimes treated as "clues" because the Criminal Procedure Code does not explicitly mention electronic evidence, and that clues are obtained from witness statements, letters, and statements from the accused (CAUSA, 2024). Even if an accused person admits their actions, there must still be other evidence that demonstrates the truth, because what is sought is the actual truth. Therefore, judges must be mature in assessing each piece of evidence presented. Generally, the category of electronic evidence consists of information in electronic form and digital documents.

Article 1 number 1 of the ITE Law explains that electronic information includes one or more data in electronic form, including but not limited to text, sound, images, maps, designs, photos, electronic data exchange, electronic mail, and telegrams, telex, copies of text or similar things, characters, markers, numbers, codes, access, symbols or holes that have been processed that have meaning or can be understood by individuals who can understand them.

Evidence, known in Latin as *corpus delicti*, refers to "objects related to a crime, namely objects used to carry out a criminal act and are very important as evidence during the criminal trial process." The view regarding the ability of electronic evidence to be used as

evidence in the process of examining general crimes based on the Criminal Procedure Code was conveyed by T. Nasrullah, a lecturer in criminal procedure law at the University of Indonesia (UI), which was reported with the following statement. Technology has touched various fields. Almost all aspects of human life have been influenced by technology, including the legal field.

Recently, a phenomenon has emerged that has become an innovation in the legal world: the use of text messages (short message service—SMS) as evidence in court proceedings. The thesis research "The Evidential Strength of Short Message Service as Electronic Evidence" in gambling cases shows that SMS can be used as evidence in criminal trials (Karina, R. E, 2014).

Overall, the research shows that electronic evidence functions as an extension of written and indicative evidence as stipulated in Article 184 of the Criminal Procedure Code. Although the Criminal Procedure Code does not directly mention electronic evidence as *lex generalis*, in order to achieve substantial truth, indicative electronic evidence can still be accepted as valid evidence in the criminal justice process.

Article 5 of the ITE Law clearly states that electronic information and documents, including printouts, constitute valid legal evidence. The existence of digital evidence is officially recognized in Indonesia's positive legal system. However, its implementation in criminal procedure practice still faces various procedural obstacles, primarily due to the lack of detailed regulations regarding the submission and verification of electronic evidence in normative and procedural challenge trials.

This obstacle is primarily caused by the incomplete integration of provisions regarding digital evidence into the applicable criminal procedure system, namely the Criminal Procedure Code. The procedures for submitting and presenting electronic documents in court can be addressed through developing court practices, but to provide legal certainty, they need to be regulated in the Civil Procedure Code or formulated in a Supreme Court Regulation (Waruwu, 2018).

This research also emphasizes that in the context of enforcing criminal law, the basis for assessing whether someone is guilty or not of a criminal act is very dependent on the system of evidence applied.

One of the advantages of an effective evidentiary system is the judge's ability to objectively evaluate the defendant's guilt, without being influenced by subjective factors such as emotion or personal conscience. The Criminal Procedure Code's evidentiary system

"combines objective and subjective elements in determining the defendant's guilt." If the judge is unsure, even if the evidence is valid, he or she cannot impose a sentence (SOCIAL SCIENCES, 2014).

This is crucial to ensure that the decisions taken are truly based on legal facts and valid evidence, including digital evidence which now plays an important role in the process of proving cyber cases and valid evidence, including digital evidence which now plays an important role in the process of proving cyber cases. Cybercrime cases show that digital evidence, such as communication gadgets (cell phones), social media profiles, and various other electronic data, play a role as a tool to prove cases in court.

However, detecting cybercriminals is often challenging due to their anonymity, unclear jurisdictional issues between countries, and the perpetrators' ability to disguise their identities through public networks such as internet cafes. This highlights the importance of international and regional collaboration in investigating cybercrime.

The provisions regarding criminal sanctions contained in the ITE Law are considered quite rigid because they generally only cover primary penalties such as imprisonment and fines. This draft does not reflect an approach that prioritizes the effectiveness of punishment, the character of the individuals involved, and the objectives of punishment, such as resocialization and prevention (Arief, B. N, 2013). This raises questions about whether imprisonment and fines are truly capable of creating a deterrent effect or instead create social stigma for cybercriminals.

Therefore, it is very important to consider the implementation of alternative punishments, such as community service, digital rehabilitation, or educational sanctions, which are considered more contextually appropriate and more humane in dealing with cybercriminals.

CONCLUSION

The provisions in the ITE Law Article 5 paragraph (1) explain electronic information and documents as valid evidence. Although it has expressly recognized electronic evidence as valid evidence, it clearly states that electronic information and documents, as well as their printouts, are valid legal evidence. However, on the other hand, it does not specifically mention it in Law Number 8 of 1981 Criminal Procedure Code (KUHAP), explaining that the evidence that is legally recognized based on Article 184 of the KUHAP, consists of: Witness statements, Expert statements, Documents, Clues, Defendant's statements.

Article 187 of the Criminal Procedure Code, what is meant by a letter as explained in Article 184 paragraph (1) letter c, is a document and other letter in an official format made by a public official who has legal force or which is made in front of them.

REFERENCES

- Arief, BN (2013). Criminal policy. Kencana.
- CAUSA. (2024). The position of electronic document evidence and electronic information in proving criminal acts. *CAUSA: Journal of Law and Citizenship*, 5(1).
- SOCIAL SCIENCES. (2014). CCTV as evidence in criminal investigations (Book 1). Sespim Lemdiklat Polri.
https://sestim.lemdiklat.polri.go.id/sestim-app/public/assets/file/1712130108_BAYUP_CCTVALATBUKTI_BUKU1.pdf
- Karina, RE (2014). The evidentiary power of Short Message Service as electronic evidence in the case of illegal lottery gambling (Thesis). Sebelas Maret University, Surakarta.
- Ma'arif, S., HukumOnline. (2024). The problem of electronic evidence in court (Part One). Retrieved from <https://www.hukumonline.com/berita/a/masalah-alat-bukti-elektronik-di-sidang-pengadilan-bagian-pertama-lt669889c6098b9/>
- Republic of Indonesia. (1981). Law Number 8 of 1981 concerning Criminal Procedure Law.
- Tanoto, E., Tandy, J., & Banke, R. (2024). The Power of Electronic Evidence in the Proof Process in Criminal Justice. *SYARIAH: Journal of Legal Studies*, 2 (1), 90–96.
<https://doi.org/10.62017/syariah.v2i1.2352>
- Waruwu, P., R., R., Supreme Court of the Republic of Indonesia. (2018). The existence of electronic documents in civil trials. Accessed from <https://www.mahkamahagung.go.id/id/artikel/3048/eksistendokumen-elektronik-di-persidanganperdata>