Law Synergy Conference (LSC)
Volume I; Number I; Month 6, Year 2024; Pages 321-328
Website:https://sinergilp.com
E-ISSN: 3048-3530

Legal Certainty of the Use of Electronic Evidence in Criminal Law Enforcement in Indonesia Review of the ITE Law and the Criminal Procedure Code

Ronny Yoesfianda[1], Henry Aspan[2]
ronnyaceh1@gmail.com henryaspan@dosen.pancabudi.ac.id
Universitas Pembangunan Panca Budi

Abstract

This study discusses the legal certainty of the use of electronic evidence in criminal law enforcement in Indonesia, focusing on Law No. 19 of 2016 concerning Electronic Information and Transactions (UU ITE) and the Criminal Procedure Code (KUHAP). In the increasingly developing digital era, electronic evidence such as digital messages and online transactions has become very important, but the main challenges faced are the unclear regulations regarding the authenticity of electronic evidence and the unpreparedness of law enforcement officers in processing it. The ITE Law recognizes electronic evidence, but there are no detailed regulations in the Criminal Procedure Code governing how this evidence is collected, authenticated, and used in court. This study uses a normative juridical method, with a statutory regulatory approach and case analysis to examine the harmonization between the ITE Law and the Criminal Procedure Code, as well as the challenges faced by law enforcement officers in implementing electronic evidence. The results of the study show that the absence of explicit rules on electronic evidence in the Criminal Procedure Code creates legal uncertainty. In addition, the limited understanding of law enforcement officers regarding technology and digital forensics results in the less than optimal use of electronic evidence in criminal cases.
This study recommends a revision of the Criminal Procedure Code to include clearer provisions on electronic evidence, as well as increasing human resource capacity through digital forensics training. With these steps, it is hoped that the use of electronic evidence can be applied legally and effectively in the Indonesian criminal justice system.

Keywords:*Electronic Evidence, Legal Certainty, Criminal Law Enforcement.*

INTRODUCTION

The rapid development of information technology in the last two decades has had a significant impact on various aspects of life, including in the legal field. In the context of criminal law enforcement, the emergence of digital technology has changed the way evidence is collected, stored, and presented to court. Electronic evidence, such as emails, text messages, digital transactions, and CCTV recordings, are now an inseparable element in investigations and legal processes. However, although electronic evidence is increasingly recognized, its application in criminal law in Indonesia still faces various challenges, especially related to legal certainty.

As a legal basis governing information technology, Law No. 19 of 2016 concerning Electronic Information and Transactions (UU ITE) legitimizes the use of electronic evidence. Article 5 of the ITE Law emphasizes that electronic information and/or electronic documents and their printouts are valid legal evidence, as are other evidence regulated in the Criminal Procedure Code (KUHAP) (Abdurrahman, 2018). However, this law still raises various questions related to the validity, legality, and recognition of electronic evidence in criminal law processes, especially in practical application in court.

The first problem that arises is the unclear regulation regarding the authenticity of electronic evidence. Authenticity is an important criterion in determining whether evidence is valid or not before the law. Electronic evidence, such as digital footprints and electronic communications, is vulnerable to manipulation. On the one hand, the ITE Law provides a legal basis for the acceptance of electronic evidence, but on the other hand, there are no detailed and firm regulations regarding how this evidence must be collected, processed, and authenticated before it can be accepted in court. The current Criminal Procedure Code does not explicitly regulate electronic evidence as part of the category of valid evidence, thus creating legal loopholes in its use. This often causes confusion in court practice when judges have to decide whether the submitted electronic evidence is valid or not (Dewi, 2019).

The second significant problem is the unpreparedness of law enforcement officers in dealing with electronic evidence. Often, the limited understanding of technology by law enforcement officers is a major obstacle in the application of electronic evidence. Investigators, prosecutors, and judges often lack adequate knowledge and skills to evaluate the validity and relevance of the electronic evidence submitted. In many cases, electronic evidence is not considered equivalent to physical evidence due to technical problems in confirming the validity of the evidence. The absence of a clear mechanism on how to verify and test electronic evidence creates a legal vacuum that is detrimental to the parties involved in the judicial process (Rahardjo, 2020).

In addition to these two main problems, legal certainty in the use of electronic evidence in Indonesia is becoming increasingly important considering the increase in cybercrime and illegal activities based on digital technology. Crimes such as identity theft, online fraud, and hacking, which often leave digital traces as the only evidence, require law enforcement to be able to use electronic evidence effectively in criminal law proceedings. In this context, the ITE Law attempts to fill the gaps in the Criminal Procedure Code by recognizing electronic evidence. However, the integration between the ITE Law and the Criminal Procedure Code is not strong enough to provide a comprehensive legal basis for its use. Courts often face challenges in assessing the validity of electronic evidence due to differences in standards applied in the field (Suryani, 2021).

The problem of the authenticity of electronic evidence that has not been clearly regulated in the Criminal Procedure Code also causes problems in the evidentiary process. Article 184 of the Criminal Procedure Code mentions five valid forms of evidence, namely witness statements, expert statements, letters, instructions, and statements from the defendant. However, electronic evidence is not explicitly mentioned in this article, so electronic evidence is often only seen as a form of additional evidence or supporting evidence. In practice, many courts have not fully recognized the strength of electronic evidence due to the legal vacuum in the Criminal Procedure Code, which should be the main reference in enforcing criminal law (Hasibuan, 2017). This vacuum weakens the position of electronic evidence in the legal process, even though its role is very crucial in resolving modern cases, especially those related to cybercrime.

Although recognized in the ITE Law, the lack of technical and procedural guidelines in managing electronic evidence is also one of the reasons why this evidence is often not recognized in court. To overcome this, there needs to be more detailed regulations regarding how electronic evidence is collected, processed, and presented in court. Digital forensic standards, for example, need to be implemented so that the authenticity and validity of electronic evidence can be ensured. Digital forensics is a discipline that focuses on collecting, examining, analyzing, and reporting digital

evidence that is relevant for legal purposes (Adams, 2020). Without clear standards, electronic evidence will always be in a weak position in the evidence process in court.

In this context, a revision to the Criminal Procedure Code is needed so that electronic evidence can be accommodated clearly and comprehensively as one of the valid evidence. This revision is expected to integrate the ITE Law with the Criminal Procedure Code, so that better legal certainty is created in handling electronic evidence. The courts, as the spearhead in law enforcement, also need to be given broader authority in evaluating electronic evidence, both in terms of authenticity and validity. Law enforcement officers must also be given adequate training in digital forensics, so that they can understand and use electronic evidence more effectively in the law enforcement process (Widiastuti, 2022).

Ultimately, the legal certainty of the use of electronic evidence in criminal law enforcement in Indonesia is highly dependent on the harmonization of the ITE Law and the Criminal Procedure Code. Clearer and more assertive regulations regarding the procedures for the use of electronic evidence, as well as increasing the capacity of law enforcement officers, will ensure that electronic evidence can be used legally and effectively in the criminal justice process. Without adequate legal certainty, the use of electronic evidence will remain a crucial problem that hinders law enforcement in Indonesia, especially in dealing with digital technology-based crimes.

METHOD

The research method used in this study is the normative legal method with a statutory regulatory approach and case analysis. This normative legal research aims to examine the legal certainty of the use of electronic evidence in criminal law enforcement in Indonesia by reviewing the provisions stipulated in Law No. 19 of 2016 concerning Electronic Information and Transactions (UU ITE) and the Criminal Procedure Code (KUHAP). Data collection techniques are carried out through literature studies by analyzing primary legal materials in the form of laws, government regulations, and court decisions related to electronic evidence. In addition, secondary legal materials such as law journals, textbooks, and academic articles are also used to enrich the analysis. The statutory regulatory approach is used to examine the harmonization between the ITE Law and the KUHAP in regulating electronic evidence, while case analysis is carried out to understand how judicial practices apply electronic evidence in criminal courts. Data analysis is carried out descriptively qualitatively by interpreting and elaborating applicable legal regulations and their practical applications in the field.

RESULTS AND DISCUSSION

Regulatory Ambiguity Regarding the Authenticity of Electronic Evidence in Criminal Law Enforcement

The use of electronic evidence in criminal law enforcement in Indonesia has been regulated through Law No. 19 of 2016 concerning Electronic Information and Transactions (UU ITE), in which Article 5 states that electronic information and electronic documents along with their printouts are recognized as valid evidence. However, the application of this electronic evidence in the field still faces many challenges, especially related to the authenticity of electronic evidence. In a legal context, authenticity refers to the ability to prove that electronic evidence is truly original and has not changed

since it was first collected until it was submitted to court (Adams, 2020). This is where the main problem lies, namely the absence of comprehensive and clear regulations in the Criminal Procedure Code (KUHAP) that can guarantee the authenticity of electronic evidence, even though the recognition of the validity of such evidence has been regulated in the ITE Law.

As evidence that is increasingly used in criminal cases, electronic evidence plays a crucial role in proving technology-based crimes, such as cybercrime, identity theft, and online fraud. However, the main challenge in using electronic evidence is its validity and authenticity. Electronic evidence can be easily manipulated or modified by interested parties, and without strict regulations regarding the process of collecting, storing, and validating this evidence, there is a legal vacuum that makes the position of electronic evidence weak in criminal law processes. One example that often arises is in cybercrime cases, where digital evidence such as electronic conversation recordings, online transaction traces, or activity logs are often the only evidence that can reveal a crime. Without clear standards regarding the digital forensic procedures that must be applied, the validity of this evidence is easily questioned (Hasibuan, 2017).

While the ITE Law legitimizes the use of electronic evidence, existing regulations are not specific enough in providing guidance on the management and authentication of this evidence. In criminal law proceedings, evidence must meet several requirements in order to be accepted in court, one of which is authenticity (Rahardjo, 2020). Unfortunately, the Criminal Procedure Code which was passed in 1981 does not provide explicit recognition of electronic evidence. This results in uncertainty in the legal recognition of electronic evidence, because the Criminal Procedure Code only recognizes five valid forms of evidence, namely witness statements, expert statements, letters, instructions, and statements from the defendant (Dewi, 2019). The absence of clear regulations regarding electronic evidence in the Criminal Procedure Code means that this evidence is often considered additional evidence or secondary evidence, which does not have the same evidentiary power as physical evidence.

This situation creates a gap in the Indonesian justice system, as many cases requiring electronic evidence cannot be resolved properly without digital forensics standardization. For example, in cybercrime cases, digital evidence such as activity logs or email conversations are often the main evidence. However, without strict standards on how such evidence should be collected and processed, there is often concern that such evidence could be manipulated before being presented in court (Suryani, 2021). In some cases, courts have decided not to accept electronic evidence due to the lack of clear authentication procedures, which makes the evidence's authenticity questionable. This shows that the authenticity verification process is a very important issue, especially when dealing with electronic evidence.

The absence of clear regulations regarding the authenticity of electronic evidence also leads to diverse interpretations among judges. In judicial practice, judges have considerable discretion in determining whether evidence is valid or not. However, when dealing with electronic evidence, many judges do not yet have a deep understanding of digital forensics and how to test the authenticity of electronic evidence (Widiastuti, 2022). This results in inconsistencies in court decisions, where in one case, electronic evidence may be accepted, while in another case, similar evidence may be rejected. This uncertainty raises questions about legal certainty which should be one of the main pillars of the Indonesian legal system.

The problem of authenticity of electronic evidence is further exacerbated by the lack of coordination between various law enforcement agencies in handling electronic evidence. For example, in cybercrime investigations, electronic evidence is often obtained through cooperation

between the police, cybercrime investigators, and third parties such as internet service providers or digital platforms. However, the lack of uniform standard operating procedures (SOPs) in collecting evidence often results in the evidence being invalid in the eyes of the law. Investigators who are not trained in digital forensics may make mistakes in collecting evidence, resulting in the loss of authenticity of the evidence (Adams, 2020). In cases like this, even evidence that should be decisive in a criminal case can be useless due to technical errors in its management.

In this context, the need for clear and detailed regulations regarding the authenticity of electronic evidence is urgent. The Criminal Procedure Code needs to be updated to accommodate developments in information technology, including in terms of accepting electronic evidence as one of the valid evidence. The revision of the Criminal Procedure Code must include procedures for collecting, storing, and validating electronic evidence, as well as providing clear guidance for law enforcement in assessing the authenticity and validity of such evidence. In addition, the ITE Law also needs to be equipped with more technical implementing regulations related to digital forensic standards and management of electronic evidence, so that there is no longer any doubt regarding the validity of this evidence in court (Dewi, 2019).

One solution that can be proposed is to implement stricter and more comprehensive digital forensic standards throughout all stages of law enforcement, from investigation to court proceedings. Digital forensic standards should include clear technical guidelines on how to collect, analyze, and store electronic evidence, as well as how to prove its authenticity in court. For example, in developed countries such as the United States and the United Kingdom, digital forensics has become an important part of the evidence process, where every piece of electronic evidence must go through a series of strict verification processes before it can be accepted in court (Hasibuan, 2017). The implementation of these standards in Indonesia will help increase legal certainty regarding the use of electronic evidence and reduce the potential for manipulation or doubt regarding its validity.

Unpreparedness of Law Enforcement Officers in Handling Electronic Evidence

After discussing the issue of authenticity of electronic evidence, the second crucial problem in the application of electronic evidence in Indonesia is the unpreparedness of law enforcement officers, especially in processing, verifying, and using electronic evidence in criminal law enforcement. Although regulations have been in place through Law No. 19 of 2016 concerning Electronic Information and Transactions (UU ITE) which recognizes the legitimacy of electronic evidence, the biggest challenge actually comes from the capacity of human resources, including investigators, prosecutors, and judges, who do not understand technology and digital forensics (Rahardjo, 2020).

In the law enforcement process, electronic evidence differs from physical evidence in several fundamental aspects. Electronic evidence requires technical analysis and in-depth knowledge of information technology in order to be processed and evaluated properly. In this case, law enforcement officers not only function as law enforcers but must also have expertise in digital forensics, a discipline that requires an understanding of how electronic evidence is collected, stored, and maintained its authenticity (Dewi, 2019). Unfortunately, not all law enforcement officers in Indonesia have this capability, so that often electronic evidence that should be able to strengthen the case cannot be used effectively due to a lack of technical knowledge and skills.

One aspect that is often overlooked in the handling of electronic evidence by law enforcement officers is the integrity of the chain of evidence. In many cases where electronic evidence is used, the evidence must go through several stages of processing, from collection at the scene, analysis by forensic experts, to presentation in court. Each of these stages must be carefully managed to ensure

that the evidence is not damaged or manipulated (Suryani, 2021). However, without a good understanding of the digital chain of evidence, many law enforcement officers fail to maintain the integrity of the evidence. This often occurs when investigators do not follow strict operational standards in collecting electronic evidence, or when they do not use the right technology to protect the authenticity of the evidence during the investigation. For example, electronic evidence collected through personal devices or servers is often accessed without proper authorization or without secure forensic methods, which ultimately casts doubt on the validity of the evidence in court (Adams, 2020).

Furthermore, the inability of law enforcement officers to conduct digital forensics independently is one of the main obstacles in the use of electronic evidence. In many cases, digital forensics often requires expertise from third parties, such as technology companies or private institutions that have more in-depth resources and knowledge of digital evidence. This causes a heavy dependence on third parties in the process of collecting and analyzing evidence, which raises potential conflicts of interest and privacy issues (Hasibuan, 2017). In some cases, electronic evidence collected by third parties can raise questions about neutrality and security, which ultimately affects the validity of the evidence in the judicial process.

In addition to technical issues, the unpreparedness of law enforcement officers is also reflected in the lack of in-depth legal understanding of electronic evidence. Although the ITE Law has regulated the validity of electronic evidence, the interpretation of this law in practice is often still ambiguous. Many judges do not fully understand the legal framework for electronic evidence and digital forensics, resulting in inconsistencies in the application of the law in court (Rahardjo, 2020). For example, there are cases where judges reject electronic evidence due to a lack of understanding of how the evidence is collected and verified. This shows that the problem lies not only in the collection of evidence, but also in the different legal interpretations regarding the validity of electronic evidence.

In some cases, the rejection of electronic evidence is not because the evidence is irrelevant or invalid, but because the judge is unsure of the technical procedures used in collecting the evidence (Dewi, 2019). This problem indicates the need to increase the capacity of human resources in the field of law enforcement, especially in terms of technology and digital forensics. Continuous training and education are needed so that judges, prosecutors, and investigators can understand the development of information technology and its implications for criminal law. Without a good understanding of digital forensic technology and standards, the use of electronic evidence in legal proceedings will remain a major challenge.

In addition, courts in Indonesia still face difficulties in managing electronic evidence involving cross-border information. In the era of globalization and digitalization, many cybercrimes involve electronic evidence that is outside Indonesia's jurisdiction, such as servers located abroad or communications involving international perpetrators (Suryani, 2021). In this case, law enforcement officers must cooperate with international institutions or foreign technology companies to access and verify electronic evidence. However, this process often takes a long time and is full of international legal obstacles, which ultimately hinders the resolution of criminal cases.

This is where the urgency of international cooperation in handling electronic evidence lies. Many developed countries already have more advanced systems in terms of managing and authenticating electronic evidence, and have international legal protocols that allow cross-border cooperation in the collection and analysis of electronic evidence (Adams, 2020). Indonesia needs to strengthen this international framework through bilateral or multilateral agreements, so that it can accelerate the process of collecting electronic evidence that is outside national jurisdiction. Without strong

international cooperation, much important electronic evidence cannot be used in court due to limited access to data in other countries.

As a solution to this problem, several strategic steps are needed. First, the government and law enforcement agencies need to develop a special curriculum on digital forensics in legal education institutions and law enforcement training. This will ensure that all law enforcement officers have basic knowledge on the collection, verification, and presentation of electronic evidence. Second, the government needs to increase investment in technological infrastructure that supports digital forensics, such as forensic laboratories equipped with sophisticated devices and technology to process electronic evidence. Third, it is necessary to revise the Criminal Procedure Code which explicitly regulates the use of electronic evidence in criminal proceedings, as well as setting clear standards on the authenticity and chain of digital evidence (Hasibuan, 2017).

With these steps, it is hoped that there will be better legal certainty in the use of electronic evidence in Indonesia. Law enforcement officers who are trained in technology and digital forensics will be able to handle electronic evidence more effectively, while clear legal standards will ensure that electronic evidence can be used legally and fairly in the criminal justice process. This is not only important for dealing with cybercrime, but also to ensure that justice is maintained in this increasingly complex digital era.

CONCLUSION

This study highlights two main problems in the use of electronic evidence in Indonesia, namely the unclear regulations regarding the authenticity of electronic evidence and the unpreparedness of law enforcement officers in handling electronic evidence. Although the ITE Law has recognized electronic evidence as a valid means of evidence, regulations regarding the authentication process and management of this evidence are still not regulated in detail in the Criminal Procedure Code, creating a legal vacuum that causes uncertainty. In addition, law enforcement officers are still less prepared to process electronic evidence due to the lack of digital forensic knowledge, so that much electronic evidence cannot be used effectively in court. Therefore, a revision of the Criminal Procedure Code is needed to integrate regulations regarding electronic evidence and increase the capacity of law enforcement through training and development of digital forensic infrastructure. These steps are expected to create legal certainty and better justice in law enforcement in the digital era.

BIBLIOGRAPHY

Abdurrahman, M. (2018). Electronic Evidence in the Perspective of Criminal Law in Indonesia. Jakarta: Rajawali Press.

Adams, J. (2020). Forensic Digital Investigations: Techniques and Tools. New York: Oxford University Press.

Dewi, S. (2019). Validity of Electronic Evidence in Criminal Law. Bandung: Alfabeta.

Hafied, A. (2018). Digital Forensics and the Challenges of Evidence in Court. Jakarta: PT Gramedia Pustaka Utama.

Hasibuan, A. (2017). Recognition of Electronic Evidence in the Criminal Procedure Code. Medan: University of North Sumatra Press.

Ibrahim, J. (2020). Introduction to Telematics Law: Legal Aspects in Information Technology. Surabaya: Airlangga University Press.

Nugraha, Y. (2019). Cyber Law: A Review of National and International Law. Bandung: Refika Aditama.

Rahardjo, S. (2020). Challenges of Law Enforcement in the Digital Era. Yogyakarta: Pustaka Pelajar.

Rahayu, T. (2021). Integration of Digital Forensics in Criminal Law Enforcement in Indonesia. Yogyakarta: Gadjah Mada University Press.

Suryani, R. (2021). Integration of the ITE Law and the Criminal Procedure Code in Criminal Law Enforcement. Surabaya: Airlangga University Press.

Susanto, M. (2022). The Position of Electronic Evidence in Criminal Law Processes in Indonesia. Bandung: Pustaka Ilmu.

Widiastuti, D. (2022). The Role of Digital Forensics in Criminal Law Enforcement. Malang: Universitas Brawijaya Press.