Society Synergy Conference (SSC)
Volume II; Number II; Year 2025; Pages 557-564
Website:https://sinergilp.com
E-ISSN: 3048-3530

DILEMMA OF EVIDENCE IN THE CYBER ERA REFORMULATION OF LEGAL STANDING OF DIGITAL EVIDENCE IN THE KUHAP AND ITE LAW

Hasman Hidayah [*1] T. Riza Zarzani [*2] Fitri Rafianti [*3]
[123] Universitas Pembangunan Panca Budi
E-mail:hasman75.h7@gmail.com

Abstract

The digital era has brought significant changes to the evidentiary system in criminal procedure law. The increasing number of cybercrime cases has made digital evidence a major element in evidence in court. However, the Indonesian criminal procedure law system, especially the Criminal Procedure Code, has not explicitly regulated the legal standing of digital evidence. Meanwhile, the ITE Law, which recognizes electronic evidence as valid, does not have binding technical procedures within the framework of criminal procedure law. This imbalance creates a serious legal dilemma that has an impact on justice and legal certainty. This study uses a normative and comparative legal approach to analyze the inconsistencies between the Criminal Procedure Code and the ITE Law and offers a reformulation of the legal standing of digital evidence. The results of the analysis indicate the need to revise the Criminal Procedure Code to include digital evidence as valid evidence, accompanied by technical implementing regulations and strengthening the competence of law enforcement officers. This reformulation is important so that the evidentiary system does not lag behind the times and continues to guarantee the principle of due process of law in the cyber era.

Keywords:digital evidence, reformulation of the Criminal Procedure Code, cybercrime

INTRODUCTION

The emergence of the digital era has fundamentally changed the structure of social interaction and criminal patterns. Cybercrime is now one of the most serious legal challenges, not only because of its transnational and latent nature, but also because of its dependence on electronic evidence (digital evidence) as the main source of evidence. This is where a major dilemma arises in the context of Indonesian criminal procedure law: when digital evidence has not received explicit and integrated regulations in the existing legal system, especially in the Criminal Procedure Code (KUHAP) (Lestari, 2023).

As is known, the evidentiary system in the Criminal Procedure Code still adheres to the classical model that recognizes five pieces of evidence: witness testimony, expert testimony, letters, clues, and defendant testimony. This model was formulated in 1981—long before the internet developed and digital technology became an inherent part of people's lives. In the current context, when most criminal acts involve or leave electronic traces—such as emails, metadata, server activity logs, or online conversations—the existence of digital evidence is inevitable. However, the absence of a special category for digital evidence in the Criminal Procedure Code creates normative ambiguity (Wibowo, 2022).

As a partial response to technological advances, the Indonesian government has issued Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which contains provisions regarding the validity of electronic information and electronic documents as legal evidence (Article 5 paragraph (1)). However, this recognition is only declarative normative, without a clear and operational procedural system within a more general criminal procedure law framework (Wahyuni & Hartini, 2021). As a result, law enforcement officers—investigators, prosecutors, and judges—are in a dilemma in assessing and deciding cases that rely on digital evidence.

This dilemma is not merely theoretical, but real in judicial practice. There are differences in the treatment of digital evidence in jurisprudence, depending on how the data was obtained, how the forensic process was carried out, and the extent to which the judge understands digital forensic techniques. For example, in some cases, screenshots submitted without hash verification are rejected,

while in other cases, digital evidence is accepted only with notary approval, without expert assistance (Ramadhani, 2023).

This condition creates inequality and inconsistency in the practice of criminal evidence, which theoretically undermines the principles of justice and legal certainty. Furthermore, the absence of standard procedures for digital evidence also opens up loopholes for unfair criminalization. Especially in cases of hate speech, digital pornography, or the spread of hoaxes, someone can easily be charged based on digital evidence that is not necessarily authentic, or obtained through illegal means such as hacking (Yuliana, 2021).

In a global context, many countries have updated their evidence systems to adapt to digital realities. The United States, through the Federal Rules of Evidence, strictly regulates the validity and authentication of digital evidence, including testing with hash values and metadata. Meanwhile, the Budapest Convention on Cybercrime (2001) provides an international reference for the process of legally and ethically seizing, storing, and presenting digital evidence. Indonesia itself has not ratified the convention, and does not have similar technical regulations (Surya, 2022).

With this background, this journal aims to answer two main problems:

1. What is the legal standing of digital evidence in the Indonesian criminal evidence system, especially in the context of the lack of synchronization between the Criminal Procedure Code and the ITE Law?
2. How should the reformulation of digital evidence regulations be carried out to ensure procedural justice and legal certainty in the digital era?

This research is very important as part of the big agenda of criminal procedure law reform in Indonesia. If the evidence system is not adapted to accept and manage digital evidence legally, then not only will crimes go unsolved, but there is also the potential for human rights violations against suspects or defendants who are burdened by legally invalid digital evidence.

METHOD

This study uses a normative legal approach, namely a method that examines law as a written norm (das Sollen), with emphasis on the provisions of the Criminal Procedure Code, the ITE Law, and other legal documents related to digital evidence. This approach is intended to examine the normative inconsistency between the conventional evidence system and legal needs in the cyber era based on electronic evidence (Rahayu, 2022).

As part of doctrinal legal research, the main data sources come from secondary legal materials which include:

1. Primary legal materials:
    - KUHAP (Criminal Procedure Code)
    - Law No. 11 of 2008 concerning Electronic Information and Transactions
    - Law No. 19 of 2016 (Amendment to the ITE Law)
    - Constitutional Court and Supreme Court decisions regarding digital evidence
2. Secondary legal materials:
    - Scientific literature (law journals, digital law books, theses/dissertations)
    - Results of studies by State Institutions such as BPHN, Kominfo, and BSSN
    - International policy documents such as the Budapest Convention on Cybercrime

3. Tertiary legal materials:
    - Legal dictionary, digital legal encyclopedia, and technical glossary on digital evidence

The data collection method was carried out through library research by tracing national and international accredited scientific journals, as well as jurisprudence documents from the official website of the Supreme Court. To support the validity of the analysis, a case study approach of jurisprudence from the first instance and cassation courts related to cybercrime cases with digital evidence debates was also used (Prasetyo, 2023).

In terms of analysis techniques, descriptive-analytical and limited comparative methods are used. First, a description is made of the normative provisions of evidence in the Criminal Procedure Code and the ITE Law. Second, a comparative analysis is carried out with foreign legal systems (the United States and the Budapest Convention). Third, a normative evaluation is carried out on the need to update criminal procedure law, especially in the aspects of recognition, authentication, and evidentiary strength of digital evidence (Lutfi, 2021).

To strengthen the theoretical basis, this study uses analytical tools in the form of:

- The Theory of Procedural Justice from John Rawls and Lon L. Fuller
- Theory of Legal Systems by Lawrence M. Friedman
- Responsive Legal Theory of Philippe Nonet and Philip Selznick

With this methodological approach, the research is expected to be able to provide conceptual and recommendatory contributions in formulating the legal standing of digital evidence that is in harmony with the principles of justice and technological development.

RESULTS AND DISCUSSION

Inconsistency of Indonesian Criminal Procedure Law to Digital Evidence

The criminal procedure system in Indonesia is based on the principle of legal formalism which prioritizes five types of evidence as stated in Article 184 of the Criminal Procedure Code: witness statements, expert statements, letters, clues, and defendant statements. This system was born from the continental legal tradition (civil law) which places more emphasis on legal evidence theory—meaning that only certain types of evidence are legally recognized (Fitria, 2020). In this context, digital evidence has never been explicitly recognized as separate evidence, so it can only be included in the category of letters or clues.

In the midst of digital transformation, this position is clearly problematic. Forms of evidence such as screenshots, emails, log files, GPS data, metadata, and digital messages often cannot be categorized as "letters" strictly as defined in the Criminal Procedure Code, because they are not always made by someone, are not addressed to anyone, and are not even printed (Lestari, 2023).

When digital evidence such as recording files or screenshots are presented without expert testimony, judges are often hesitant to accept them because their authenticity and integrity cannot be ascertained. This is where the formalistic evidentiary system becomes a major obstacle in the acceptance of modern evidence (Siregar, 2022).

Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) provides a normative breakthrough. Article 5 paragraph (1) and Article 44 paragraph (1) of the ITE Law state that electronic information and/or electronic documents are valid legal evidence. However, this recognition is not immediately integrated with the Criminal Procedure Code. This means that the

recognition of the legal standing of digital evidence in the ITE Law is normative-sectoral, not systemic (Wahyuni & Hartini, 2021).

Consequently, even though digital evidence is normatively recognized, the court still uses the Criminal Procedure Code as the main procedural basis. As a result, digital evidence is only accepted if it can be constructed as an indication or letter, and that too must be accompanied by expert verification. This fragmentation causes legal uncertainty in the evidence process, especially when there are differences of interpretation between law enforcement officers (Suharto, 2022).

In addition, the Criminal Procedure Code has not yet regulated important principles in digital evidence, such as:

- Data authentication (authenticity)
- Data integrity
- Chain of custody
- Digital forensics

The absence of these principles causes a lot of electronic evidence to be rejected because its authenticity is doubtful, or it cannot be proven where and how the data was obtained (Alamsyah, 2021).

In judicial practice, judges face a major dilemma: whether to pursue material truth by using relevant digital evidence, or to submit to procedural formalities that do not recognize digital evidence as a separate category. Jurisprudence shows inconsistencies: in some cases, screenshots from WhatsApp are accepted if there are witnesses to corroborate them; but in other cases, digital evidence is rejected because it is not accompanied by a digital signature or authentication from a digital forensic expert (Ramadhani, 2023).

It is also not uncommon for digital data to be confiscated without a court order, or for personal data to be collected from electronic devices without valid consent. In this context, the principle of due process of law is violated, and evidence becomes invalid under procedural law. This is contrary to the Constitutional Court Decision No. 20/PUU-XIV/2016 which emphasizes that the confiscation of electronic information must be based on a court order (Yuliana, 2021).

This normative and procedural conflict places digital evidence in a legally ambiguous position. It is unclear whether it is primary, secondary, or complementary evidence. Even in many cases, digital evidence is only used as an aid to strengthen conventional evidence. This is clearly not in line with the characteristics of cybercrime which relies entirely on electronic evidence (Surya, 2022).

Therefore, reformulation of the legal standing of digital evidence is an urgent need. The Criminal Procedure Code must revise Article 184 and add digital evidence as a valid evidence. Not only that, procedural provisions must also be made regarding the collection, confiscation, verification, and presentation of digital evidence forensically. From this description, it can be concluded that the Criminal Procedure Code is no longer compatible with the development of digital technology in terms of evidence. Although the ITE Law has given recognition to digital evidence, this recognition does not have procedural force in the context of criminal procedure law. Without synchronization between substantive and procedural norms, digital evidence will remain in a dilemmatic position and vulnerable to misuse.

Reformulation of Legal Standing of Digital Evidence in the Indonesian Criminal Procedure System

The urgency of reformulating the legal standing of digital evidence in Indonesian criminal procedure law is increasingly unavoidable, considering the escalation of cybercrime that continues to increase along with society's dependence on digital technology. In the modern world, almost all human activities leave digital traces—whether in the form of online communication, electronic transactions, or activities on social media. This reality creates legal consequences that require the evidence system to be not only responsive to changes in the times, but also adaptive to technological developments.

Unfortunately, Indonesia does not yet have an adequate normative and institutional framework to accommodate digital-based evidence in the criminal justice system. The Criminal Procedure Code, which was born in 1981, was not designed to address the challenges of digitalizing evidence, while the ITE Law does not provide adequate procedural details. As a result, digital evidence is often in an ambiguous position: on the one hand, it is normatively recognized as valid evidence, but on the other hand, it is often rejected in court practice because it does not meet formal procedural requirements (Hakim, 2021).

Digital evidence has unique characteristics that distinguish it from conventional forms of evidence. It can be easily manipulated, engineered, copied, or distributed without geographical and time limits. Therefore, the approach to digital evidence requires principles that guarantee authenticity, integrity, and accountability in the handling process. Developed countries have long placed these principles in their procedural legal systems, for example the United States through the Federal Rules of Evidence Rule 902 which stipulates that digital information must be forensically authenticated through hash marks and metadata (Kerr, 2018).

Indonesia needs a reformulation of the legal standing of digital evidence that includes two important aspects: explicit normative recognition in the Criminal Procedure Code, and technical procedural elaboration through implementing regulations. The revision of Article 184 of the Criminal Procedure Code to add digital evidence as a category of valid evidence on par with letters, witnesses, and instructions is very crucial. Without this step, the justice system will continue to be plagued by inconsistencies due to the absence of a solid legal basis in assessing the validity of digital evidence (Rahmat, 2020).

Furthermore, the formulation of implementing regulations must include detailed standard operating procedures (SOPs) regarding the procedures for confiscation, processing, storage, and presentation of digital evidence in court. These procedures must be in line with the principle of chain of custody so that each stage of the process can be legally accounted for. Institutions such as the Police, the Prosecutor's Office, the Supreme Court, and the Ministry of Communication and Information need to work together in compiling a national protocol for digital evidence based on digital forensic principles (Nasution, 2022).

In addition to normative and technical aspects, major challenges also arise from the human resource capacity side. Many judges, prosecutors, and investigators do not yet have adequate competence to assess the validity of digital evidence. In many cases, limited technical understanding is actually an obstacle to proof, not the substance of the data itself. For this reason, reformulation must also include aspects of training and competency certification for law enforcement officers. A multidisciplinary approach—which combines legal knowledge with digital forensic skills—is an absolute necessity in this digital era (Hartanto, 2021).

Comparison with regulations in other countries shows that the success of recognizing digital evidence is highly dependent on the courage of legislators to comprehensively change the paradigm of procedural law. The UK, for example, through the Police and Criminal Evidence Act (PACE) and the Computer Misuse Act, has made digital evidence a key element in criminal evidence. Singapore even has the Electronic Transactions Act and Evidence Act which include detailed provisions on electronic authentication. Indonesia cannot continue to lag behind if it wants to build a fair and modern criminal law system (Wijaya, 2023).

The reformulation must also consider the principle of human rights protection, especially the right to privacy. Many cybercrime cases involve the confiscation of personal devices without permission or a warrant. In this context, the recognition of digital evidence must be accompanied by strict regulations on the limits of investigators' authority. The use of spyware, wiretapping, and confiscation of personal data without a clear legal basis can lead to constitutional violations. Therefore, the legalization of digital evidence must be carried out together with the protection of the rights of the accused (Sasmita, 2021).

Conceptually, a technology-responsive evidentiary system is not enough to simply acknowledge the existence of new evidence, but must also substantially regulate how the evidence

works in the criminal law system. This reformulation is not only a form of adjustment to the dynamics of technology, but also a state commitment to guaranteeing the principles of fair trial and due process of law for all citizens.

With all these arguments, the renewal of the criminal procedure law system is inevitable. When the dominant evidence in a digital case does not yet have a definite legal place, then every law enforcement effort has the potential to lose legitimacy. Reformulating the legal standing of digital evidence is a strategic step to ensure the integrity of justice in the digital era, where facts and data have moved from physical space to cyberspace.

CONCLUSION

Digital transformation has changed the face of human civilization, including in the legal aspect, especially criminal procedure law. Digital evidence is no longer a complement, but rather a major part of proving criminal acts that occur in cyberspace. Unfortunately, the Indonesian criminal procedure law system, which is still tied to the classical and formalistic model, has proven unable to accommodate this development optimally. The Criminal Procedure Code as the main foundation of criminal procedure law in Indonesia does not explicitly regulate the existence and procedures for managing digital evidence. This creates a normative and practical mismatch, which in its implementation often leads to legal uncertainty.

As a partial response to these developments, the ITE Law brings a new norm that recognizes electronic information and electronic documents as valid evidence. However, this recognition is sectoral and declarative, not accompanied by detailed implementing regulations and not systemically integrated with conventional criminal procedure law. As a result, there is a fragmentation of norms between the provisions of evidence in the Criminal Procedure Code and the provisions of evidence in the ITE Law. This not only makes it difficult for law enforcement officers in practice, but also opens up space for debate in the evidence process in court, especially regarding the strength of evidence, formal requirements, and the validity of digital evidence.

The problem becomes more complex when digital evidence must be assessed amidst the lack of technical understanding of law enforcement officers. Many law enforcement officers have not received adequate training in digital forensics, data authentication, and procedures for managing and storing electronic evidence. In such conditions, there is a high risk that important digital evidence will be rejected or misused in the judicial process. This poses a serious threat to the principles of justice and due process of law. Moreover, in some cases, digital evidence is obtained through illegal means, such as unauthorized hacking, illegal wiretapping, and seizure of devices without a valid warrant. If this is allowed to continue, the criminal justice system has the potential to violate human rights protected by the constitution.

Therefore, a comprehensive reformulation step is needed. The legal standing of digital evidence must be strengthened through normative updates to the Criminal Procedure Code, especially in Article 184, to explicitly recognize digital evidence as one of the legitimate and independent evidence. This recognition will provide legal clarity and certainty for all parties involved in the judicial process, including public prosecutors, investigators, legal counsel, and judges.

The reformulation must also be complemented by the preparation of implementing regulations or detailed technical guidelines. These guidelines must regulate operationally everything from the process of obtaining digital evidence, storage, authenticity testing (verification), to the procedure for presenting it in court. Digital forensic principles such as chain of custody, hash verification, and metadata standards must be an integral part of the SOP for electronic evidence. The preparation of these regulations needs to involve strategic institutions such as the Police, the Prosecutor's Office, the Supreme Court, the Ministry of Communication and Information, and the BSSN in order to create synergy in strengthening the national electronic evidence system.

In addition to regulatory and technical aspects, strengthening human resource capacity is an important element. Law enforcement officers must be given special training and certification in the

field of digital forensics. The Supreme Court as the highest institution in the judicial field also needs to organize continuing education for judges regarding digital evidence technology and its legal implications. Thus, the assessment of digital evidence can be carried out objectively, professionally, and accountably.

The reformulation also needs to consider the dimensions of human rights protection, especially the right to privacy and the right to a fair trial. In terms of the collection and seizure of digital data, there must be strict and clear legal limitations. There should be no process of confiscation or analysis of personal data without a court order or a valid legal basis. Law enforcement must continue to uphold the principles of proportionality and legality so as not to cause injustice or abuse of authority by state officials.

In the long term, Indonesia also needs to consider adopting international standards related to digital evidence, such as those contained in the Budapest Convention on Cybercrime. Although Indonesia is not yet a party to the convention, its principles can be used as a reference in the formation of more modern and adaptive national policies. These international standards include not only the recognition of digital evidence, but also cross-border cooperation mechanisms, personal data protection, and responsible digital governance.

With all these conditions and recommendations, it can be concluded that evidence in the cyber era requires a new, comprehensive, and contextual approach to procedural law. The Criminal Procedure Code as the main framework for criminal procedural law must be revised immediately so as not to lag behind the legal and social realities of the digital society. Without significant changes, the criminal evidence system will continue to be in a crisis of legitimacy, justice, and effectiveness.

Therefore, as a final suggestion, the government, lawmakers, and law enforcement agencies should:

1. Immediately revise the Criminal Procedure Code to include digital evidence as valid evidence.
2. Drafting technical implementing regulations that regulate digital evidence mechanisms from upstream to downstream.
3. Conducting training and certification for law enforcement officers in the field of digital forensics.
4. Ensuring the protection of human rights at every stage of the digital evidence process.
5. Adopting international standards and practices as a reference in establishing a modern and adaptive national electronic evidence system.

Through these steps, Indonesia can build a criminal justice system that is fairer, more resilient, and responsive to the times. Digital evidence is not just a technical challenge, but a test of the state's ability to enforce the law in a new era, where justice is no longer only decided in the courtroom, but is also built on logic and a digital system that is transparent, legitimate, and trustworthy.

BIBLIOGRAPHY

Alamsyah, I. (2021). The Urgency of Digital Evidence Authentication in Criminal Evidence. Yustitia Journal, 13(2), 121–134.

Fitria, S. (2020). The Evidence System in the Criminal Procedure Code and its Challenges in the Digital Era. Journal of Law & Development, 50(1), 35–48.

Hakim, R. (2021). Challenges of Digital Evidence in the Era of Industrial Revolution 4.0. Journal of Law & Technology, 5(1), 89–102.

Hartanto, M. (2021). Digital Forensic Training for Judges and Investigators: Necessity or Obligation? Journal of Judicial Law, 6(2), 115–129.

Kerr, O. (2018). Digital Evidence and the New Criminal Procedure. Harvard Law Review, 133(4), 523–567.

Lestari, F. (2023). Electronic Evidence in the Criminal Law System: An Analytical Study of the ITE Law and the Criminal Procedure Code. Indonesian Legislation Journal, 20(1), 77–91.

Lutfi, R. (2021). Chain of Custody in Handling Digital Evidence. Indonesian Journal of Criminology, 12(1), 33–45.

Nasution, F. (2022). SOP for Digital Evidence Management in Law Enforcement. Journal of Legal Reform, 10(2), 213–229.

Prasetyo, D. (2023). Case Study of Cybercrime Jurisprudence and Validity of Digital Evidence. Jurnal Juris, 8(1), 56–72.

Rahmat, A. (2020). The Urgency of Revising the Criminal Procedure Code in Responding to the Challenges of Information Technology. Journal of Actual Legal Science, 14(2), 98–113.

Rahayu, W. (2022). Reform of the Criminal Procedure Law System in Indonesia: A Critical Review. Progressive Law Journal, 17(1), 22–39.

Ramadhani, N. (2023). Inconsistency of Court Decisions in Electronic Evidence Cases. Yustekno Journal, 3(2), 65–80.

Sasmita, A. (2021). Privacy Protection in the Digital Investigation Process. Journal of Constitution and Human Rights, 11(2), 101–117.

Siregar, B. (2022). Judges' Assessment of Digital Evidence in Criminal Cases. Journal of Court Jurisprudence, 9(2), 147–162.

Suharto, M. (2022). The Need for Harmonization of the ITE Law and the Criminal Procedure Code in Criminal Evidence. Journal of Legal Dynamics, 22(2), 199–215.