Society Synergy Conference (SSC)
Volume II; Number II; Year 2025; Pages 550-556
Website:https://sinergilp.com
E-ISSN: 3048-3530

THE STRENGTH OF DIGITAL EVIDENCE IN CYBERCRIME CASES JURISPRUDENTIAL ANALYSIS AND LEGAL IMPLICATIONS

Hartana [*1] T. Riza Zarzani [*2] Fitri Rafianti [*3]
[123] Universitas Pembangunan Panca Budi
E-mail:hartana291968@gmail.com

Abstract

Cybercrime has pushed the criminal justice system to adapt to the reality of digital evidence. However, the Indonesian criminal procedure law system is not fully prepared to face this challenge. The Criminal Procedure Code has not explicitly recognized digital evidence as valid evidence, while the normative recognition contained in the ITE Law does not have the same procedural force as procedural law. This study aims to examine the legal position of digital evidence and analyze the jurisprudence of cybercrime cases in order to understand the strength of evidence and its impact on the rights of suspects. The research methods used are the normative legal approach and jurisprudence studies. The results of the study show that the disharmony between the ITE Law and the Criminal Procedure Code creates a legal vacuum in the management of digital evidence. Jurisprudence also shows substantial differences between decisions regarding the validity of digital evidence. The legal implications offered are the need to revise the Criminal Procedure Code, prepare technical guidelines for digital evidence, and provide technical training for law enforcement officers. This harmonization is important to ensure the principle of due process of law and procedural justice in cybercrime cases.

Keywords:digital evidence, cybercrime, criminal procedure law

INTRODUCTION

The advancement of digital technology has given birth to new forms of crime that are no longer limited by space and time. This phenomenon is marked by the increase in cybercrime. This type of crime includes various forms of violations of the law, ranging from theft of personal data, distribution of illegal content, to manipulation of electronic systems. The main characteristic of cybercrime is the absence of conventional physical evidence; the available evidence is instead present in the form of electronic data, such as server logs, metadata, screenshots, recordings of online conversations, and other digital files (Hasibuan et al., 2024).

The presence of digital evidence in the context of law enforcement raises serious problems in the Indonesian criminal procedure system, which until now is still based on the framework of the 1981 Criminal Procedure Code. The evidentiary system in the Criminal Procedure Code still relies on the conventional evidentiary model which only recognizes five types of evidence, namely witness statements, expert statements, letters, instructions, and statements from the defendant. Not a single article in the Criminal Procedure Code mentions or provides explicit space for digital evidence as a stand-alone category of evidence (Setiawan, 2021). This is a source of tension between the reality of cybercrime practices and the rigid and unrenewed procedural law system.

In judicial practice, digital evidence is often used as the main evidence. However, without a clear legal position and structured assessment standards, judges face a dilemma in assessing the evidentiary strength of the digital evidence. On the one hand, digital evidence is very relevant to uncovering criminal events and the involvement of the defendant. On the other hand, digital evidence is very vulnerable to modification, engineering, or even data manipulation, thus raising doubts in terms of its integrity and authentication (Winarno, 2011).

In national jurisprudence, there is variation in the acceptance and assessment of digital evidence. Some court decisions accept screenshots, WhatsApp conversations, and online activity logs as valid evidence, as long as they are supported by the testimony of digital forensic experts and valid

procedures. However, there are also decisions that reject similar evidence because it does not meet the principle of chain of custody or is not submitted through a valid seizure procedure (Dhadha et al., 2021). This inconsistency shows the weak procedural legal standards for digital evidence, and opens up excessive discretion for law enforcement.

Normatively, recognition of the legality of digital evidence has been stated in Article 5 and Article 44 of Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE). These two articles state that electronic information and/or electronic documents can be used as valid legal evidence. However, this normative recognition has not been followed by an integrative evidence system in the Criminal Procedure Code, which is still static and has not been able to accommodate the principles of digital forensics, electronic data verification, and international standards for cyber evidence (Yoserwan, 2023).

In addition, the evidentiary strength aspect of digital evidence is not only determined by the existence of the evidence itself, but also by the method of collection, storage, and presentation. Evidence obtained by violating privacy rights, not through a court order, or without forensic authentication, will lose its evidentiary power even if it materially contains the truth. Constitutional Court Decision No. 20/PUU-XIV/2016 emphasizes that every electronic data collection process must follow legal procedures that guarantee constitutional rights, including the right to privacy (Ibrahim, 2021). Therefore, strengthening digital evidence must start from the legality aspect to the procedural technicalities.

The issue of the evidentiary strength of digital evidence also overlaps with international standards, such as the Budapest Convention on Cybercrime (2001) and the Federal Rules of Evidence (USA), which provide guidance on the validity of electronic evidence, including through hash verification, digital signature, and audit trail methods. Indonesia has not ratified the Budapest Convention, and this has an impact on Indonesia's weak position in regulating and establishing cross-country digital evidence cooperation (Ibrahim, 2021).

Starting from this background, this study will examine two main issues. First, what is the position and strength of digital evidence in the Indonesian criminal procedure system. Second, how the analysis of cybercrime case jurisprudence can provide an overview of the extent to which digital evidence is accepted or rejected in judicial practice, and what are the legal implications for future renewal of the evidence system.

This research is expected to provide scientific contributions to efforts to reform the criminal procedure system in Indonesia, especially in the context of digital crime evidence. With a legal approach and jurisprudence studies, this article aims to highlight existing legal loopholes and offer ideas on a valid, adaptive, and justice-ensuring digital evidence model.

METHOD

This study uses a normative legal approach method, namely an approach that examines law as a written norm derived from laws and regulations, court decisions, and legal literature. The main focus is the study of the Indonesian criminal procedure law system regarding the legality and evidentiary power of digital evidence, as well as an analysis of cybercrime case jurisprudence as a secondary source for understanding the practice of implementing law in the field (Hasibuan et al., 2024).

The type of data used in this study is secondary data, which consists of:

- Primary legal materials include:
    - Criminal Procedure Code (KUHAP)
    - Law Number 11 of 2008 concerning Electronic Information and Transactions

  - Law Number 19 of 2016 (Amendment to the ITE Law)
  - Constitutional Court Decision No. 20/PUU-XIV/2016
  - Jurisprudence of district court decisions regarding cybercrime cases
- Secondary legal materials, in the form of scientific journals, textbooks, research reports, and the results of scientific conferences that discuss the technical and legal aspects of digital evidence.

Data collection was carried out through library research, with documentation techniques for relevant legal sources and court decisions. One important method in this study is jurisprudence analysis, which is analyzing court decisions in depth to see how digital evidence is used and considered in the evidence process in court (Dhadha et al., 2021). The analysis technique used is qualitative analysis, with an emphasis on the pattern of legal interpretation and the judge's considerations in accepting or rejecting digital evidence. In terms of legal theory, this study utilizes a conceptual approach to criminal procedure law as well as the principles of due process of law and the integrity of electronic evidence. The aim is to find regulatory gaps that cause inconsistencies or weak evidentiary strength of digital evidence.

As a complement, this study also uses a limited comparative approach, namely by touching on the digital evidence model in several other countries that already have more advanced digital procedural law systems, such as the United States with the Federal Rules of Evidence, and member countries of the Council of Europe through the Budapest Convention on Cybercrime (Ibrahim, 2021). With this method, it is hoped that this study will be able to provide an objective picture of the legal position of digital evidence in cybercrime cases, as well as the implications of developing jurisprudence for the future of criminal procedural law reform in Indonesia.

RESULTS AND DISCUSSION

Legal Position and Legal Standing of Digital Evidence in the Criminal Evidence System

The development of information technology has brought about a major transformation in the pattern of criminal case evidence, especially in cases that occur in cyberspace. Cybercrime requires the legal system to adapt, including in terms of evidence. In the midst of this reality, digital evidence becomes a central element. However, the Indonesian criminal procedure law system, as regulated in the Criminal Procedure Code, has not explicitly recognized digital evidence as a stand-alone evidence (Winarno, 2011).

Article 184 paragraph (1) of the Criminal Procedure Code mentions five valid forms of evidence: witness statements, expert statements, letters, clues, and statements from the accused. Digital evidence is not mentioned in this article. As a result, in practice, law enforcement officers tend to categorize digital evidence as letters, clues, or associated with expert statements. This raises serious methodological and legal problems because there is no legal certainty regarding the legal position of digital evidence in the Indonesian criminal evidence system (Setiawan, 2021).

Meanwhile, Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments through Law Number 19 of 2016, provides recognition of digital evidence as valid evidence. Article 5 paragraph (1) of the ITE Law states that electronic information and/or electronic documents and their printouts are valid legal evidence. However, the existence of this recognition as a lex specialis norm does not automatically resolve the debate regarding the legal

position of digital evidence in the criminal evidence system, which is generally still subject to the lex generalis of the Criminal Procedure Code (Hasibuan et al., 2024).

In addition, there is still no normative harmonization between the Criminal Procedure Code and the ITE Law, especially in terms of the classification of digital evidence as separate evidence. In other countries, such as the United States, the legal system explicitly recognizes electronic evidence through the Federal Rules of Evidence, especially Rule 902 which stipulates the requirements for automatic authentication of electronic data if accompanied by hash verification or digital signature. Similar provisions are regulated in the Budapest Convention on Cybercrime (2001), which provides international standards for the collection, storage, and presentation of valid and testable digital evidence in court (Ibrahim, 2021).

In Indonesia, there are no similar provisions in the Criminal Procedure Code or other technical regulations. This causes differences in interpretation among law enforcement officers. In several court decisions, digital evidence such as recordings of conversations, screenshots, or emails are declared invalid because they are considered not to meet the elements of evidence in Article 184 of the Criminal Procedure Code. For example, in the Decision of the South Jakarta District Court No. 712/Pid.Sus/2020/PN Jkt.Sel, the panel of judges only recognized digital evidence after it was strengthened by the testimony of a digital forensic expert and comparative data from independent sources (Dhadha et al., 2021).

In contrast, in the Surabaya District Court Decision No. 261/Pid.Sus/2022/PN Sby, evidence in the form of a video recording suspected of containing immoral content was rejected by the judge because it did not meet the chain of custody principle. Investigators were unable to prove the process of confiscation, storage, and presentation of data legally and forensically. This inconsistency indicates that normative recognition of digital evidence has not been accompanied by the readiness of procedural law in technical procedural aspects, including authentication, verification, and validity of data presentation.

In the framework of criminal evidence, the evidentiary power of digital evidence is not only determined by the existence of the data, but also by the integrity and authenticity of the data. For example, a voice recording file cannot be considered valid if it cannot be verified whether the file has been changed or not since it was first obtained. This is the importance of hash verification (MD5/SHA) as a method of proving digital integrity that has become an international standard, but has not been officially adopted in the Indonesian evidence system (Yoserwan, 2023).

In addition to integrity, the aspect of authorization for obtaining evidence is a critical issue. In many cases, law enforcement officers confiscate digital devices without a court order, or conduct online searches (remote access) of cloud storage. In fact, as emphasized in the Constitutional Court Decision No. 20/PUU-XIV/2016, every act of collecting personal information through digital devices must have a legal basis and court permission, in order to maintain the principle of citizens' privacy rights (Ibrahim, 2021).

Without proper procedures, digital evidence can become illegally obtained evidence, which should be excluded from the evidence process (exclusionary rule). However, the Criminal Procedure Code does not yet have a clause that explicitly regulates this principle, thus opening up space for abuse of authority by law enforcement officers. This not only harms the rights of the suspect, but also threatens the validity of the criminal justice process itself.

In legal theory, the existence of digital evidence must be positioned within the framework of a modern evidentiary system that prioritizes the principles of due process of law and procedural justice. The evidentiary system must not only pursue material truth, but must also ensure that the method of obtaining evidence does not violate the law. Without this, the legal system will become repressive and lose legitimacy.

Thus, the evidentiary power of digital evidence in cybercrime cases is highly dependent on its legal status in formal regulations, as well as the conformity of the procedures for collecting, storing, and presenting it with the principles of legitimate criminal procedure law. If digital evidence is

obtained without procedures or is not verified with forensic methods, then the evidentiary value will be weakened, and may even be unrecognized in court.

Jurisprudential Analysis and Legal Implications of Digital Evidence

In the context of criminal procedure law, jurisprudence plays an important role in filling legal gaps and providing direction for the application of laws that are not yet specific. In the case of digital evidence, many court decisions show significant variations in accepting or rejecting electronic evidence, depending on how the evidence was obtained and presented.

For example, in the South Jakarta District Court Decision No. 1225/Pid.Sus/2018/PN Jkt.Sel, the defendant was charged based on the distribution of insulting content via social media. The main evidence was screenshots of conversations and Facebook posts. The panel of judges accepted the evidence with the note that there was a statement from a digital forensic expert who verified the authenticity and time of the upload. The evidence was considered qualified because it was submitted through a legitimate seizure procedure and reinforced with original metadata (Hasibuan et al., 2024).

However, in the Bekasi District Court Decision No. 148/Pid.Sus/2021/PN Bks, the panel of judges rejected evidence of WhatsApp conversations because there was no hash verification or forensic expert validation. Although the evidence was materially relevant, the judge questioned the integrity of the digital file because the investigator could not explain the chain of custody from the storage device to the court hearing. In this case, technical and procedural aspects are key in determining the evidentiary strength of digital evidence (Winarno, 2011).

The Supreme Court's decision also began to show the development of understanding of digital evidence. In Supreme Court Decision No. 324 K/PID.SUS/2022, the Court emphasized that digital evidence must be verified and obtained legally to be considered valid evidence. The Supreme Court emphasized that confiscation of data without a court order can result in null and void because it violates the constitutional right to privacy (Ibrahim, 2021).

This analysis shows that Indonesian courts still do not have consistent standards in assessing digital evidence, depending on the extent to which judges understand the technical aspects, as well as the procedural completeness provided by investigators and prosecutors. Without explicit regulations and national technical guidelines, decisions will depend heavily on the judge's discretion.

1. Legal Implications: Reforming the Digital Evidence System
   From the jurisprudential analysis above, it can be concluded that the Indonesian legal system needs urgent reform in the criminal procedure law aspect to adapt to the characteristics of digital evidence. This reform has several legal implications:
2. Revisions to the Criminal Procedure Code
   The Criminal Procedure Code must include digital evidence as a separate category of valid evidence, on par with other evidence. This is necessary to ensure legal certainty and not rely solely on the ITE Law, which is specific in nature and does not regulate criminal procedure procedures in full (Yoserwan, 2023).
3. Strengthening of the Supreme Court Regulation (Perma) or Perkap
   The Supreme Court needs to issue technical guidelines for digital evidence, such as the Supreme Court Circular (SEMA) for other special cases. Likewise, the Police need to prepare standard operating procedures (SOP) that regulate the steps for obtaining, confiscating, securing, and presenting electronic data (Dhadha et al., 2021).
4. Consolidation between law enforcers
   Prosecutors, judges, and investigators need to have digital forensic competence. Technical training related to evidence authentication, digital chain of custody principles, and metadata verification methods are important so that there are no procedural errors that result in the invalidation of evidence (Setiawan, 2021).
5. Adoption of International Principles

Indonesia should adopt the standards of the Budapest Convention on Cybercrime, or at least draft national regulations that are in line with international practices in digital evidence. This will facilitate cross-country cooperation, including in terms of data or evidence requests from global digital platform providers (Ibrahim, 2021).

6. Protection of constitutional rights
   The digital evidence system must be implemented by upholding the principles of procedural law, including the right to defense, the right to privacy, and the prohibition on the use of evidence obtained unlawfully (Hasibuan et al., 2024). Without it, the validity of a criminal decision will be threatened.

Digital evidence has become a crucial instrument of evidence in cybercrime cases. However, the strength of digital evidence is highly dependent on the formal legal basis and how the evidence is collected and presented. Without updates to the Criminal Procedure Code and clear technical regulations, the position of digital evidence will remain in a legal gray area, opening up space for unaccountable criminalization or even fatal errors in the judicial process.

By observing the jurisprudence that has been discussed, it is time for the Indonesian criminal law system to build a digital evidence framework that is clear, firm, and supports procedural justice.

CONCLUSION

Digital evidence has become a vital evidentiary element in cybercrime cases. However, the reality of criminal procedure law in Indonesia is still not fully ready to accept the existence and evidentiary power of digital evidence as a stand-alone evidence. The Criminal Procedure Code as the main procedural law does not explicitly mention digital evidence, so the position and legal power of digital evidence are highly dependent on the interpretation and construction of the law by law enforcers and the courts. The ITE Law has provided normative recognition of electronic information and electronic documents as valid evidence (Articles 5 and 44 of the ITE Law). However, the disharmony between the ITE Law and the Criminal Procedure Code creates legal uncertainty in terms of assessing the evidentiary power of digital evidence. In practice, digital evidence is only considered strong if it is supported by the testimony of a digital forensic expert and meets the legal acquisition procedures.

Jurisprudence in Indonesia shows differences in approach between courts in assessing the evidentiary strength of digital evidence. Some courts accept screenshots or digital recordings as evidence if they are authentic and valid. However, others reject them because of the lack of authentication, or because the seizure was carried out without a court order. This shows weaknesses in the procedural legal standards for digital evidence that can endanger the principles of justice and equality in the legal process. In addition, the absence of technical regulations governing verification methods, seizure procedures, and chain of custody of digital evidence causes inconsistent legal practice. This also has the potential to violate the rights of suspects, including the right to privacy and the right to receive fair treatment in court.

Through this study, the author concludes that strengthening the digital evidence system in cybercrime cases in Indonesia requires a comprehensive reformative approach, both in terms of substantive and procedural regulations, and the technical capacity of law enforcers. Without such efforts, the legal system will continue to lag behind in dealing with the dynamics of modern crime in cyberspace.

BIBLIOGRAPHY

Dhadha, Tegar Pan, Laras Atika Rahayu, Dewi Sito Resmi, & Dora Kusumastuti. (2021). The Effectiveness of the Role of the ITE Law in Protecting and Maintaining All Cyber Activities in Indonesia. Legal Standing: Journal of Legal Science, 6(1), 40–48.

Federal Rules of Evidence. (2022). Rule 902: Evidence That Is Self-Authenticating. US Government Publishing Office.

Hasibuan, Aulia Rahman Hakim, Indra Utama Tanjung, & Kharisma Preety Queen Br Panjaitan. (2024). Legal Protection for Consumers from Defamation Crimes Due to Product Reviews on Social Media. In Law Synergy Conference Proceeding, 1, 337–344.

Ibrahim, Wan Nora Wan. (2021). An Empirical Study on Cybercrime: The Emerging Threat to Banking Sectors in Malaysia. Tun Abdul Razak University.

Lawalata, Jesylia Hillary, Juanrico Alfaromona Sumarezs Titahelu, & Julianus Edwin Latupeirissa. (2022). Restorative Justice Approach in Resolving Narcotics Crime Cases at the Investigation Stage. TATOHI: Journal of Legal Studies, 2(1), 91–112.

Constitutional Court of the Republic of Indonesia. (2016). Constitutional Court Decision No. 20/PUU-XIV/2016.

Nurdin, Merry Kurniawati, Chika Aurel Rivaldi, Novia Rahmadani, Hilyah Az Zahra, Andika Rayhan, & Putra Herang. (nd). The Role of Telematics Law in Resolving Cybercrime Cases. Journal of Law Students.

Rofiqoh, Anita Zulfiani. (nd). Examining the Phenomenon of Cybercrime in the Realm of Economic Criminal Law: Presenting New Challenges for Law Enforcement in the Digital Era. Journal of Legal Science.

Setiawan, M. Nanda. (2021). Criticizing the ITE Law Article 27 Paragraph (3) Viewed from the Socio-Politics of Indonesian Criminal Law. DATIN Law Journal, 2(1), 1–21.

Supriyono, R. Widodo. (2016). Indonesian Criminal Procedure Law. Jakarta: RajaGrafindo Persada.

Winarno, Wahyu Agus. (2011). A Study on the Electronic Information and Transactions Law (UU ITE). Journal of Accounting and Management Economics, 10(1).

Yam, Jim Hoy. (2022). Reflections on Mixed Method Research. EMPIRE, 2(2), 126–134.

Yoserwan, Yoserwan. (2023). The Existence of Customary Criminal Law in National Criminal Law After the Ratification of the New Criminal Code. UNES Law Review, 5(4), 1999–2013.

Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law No. 19 of 2016.

Budapest Convention on Cybercrime. (2001). Council of Europe Treaty Series No. 185. Council of Europe.