Society Synergy Conference (SSC)
Volume II; Number II; Year 2025; Pages 543-549
Website:https://sinergilp.com
E-ISSN: 3048-3530

THE URGENCY OF HARMONIZING CRIMINAL PROCEDURE LAW WITH TECHNOLOGY LEGAL REVIEW OF DIGITAL EVIDENCE IN CYBERCRIME

Nurochman Nulhakim*1 T. Riza Zarzani*2 Mhd. Azhali Siregar*3
123 Universitas Pembangunan Panca Budi
E-mail:nulhakim2000@gmail.com

Abstract

The development of digital technology has created fundamental changes in the procedures for crime and law enforcement, especially in the context of criminal evidence. The emergence of cybercrime has created major challenges for the Indonesian criminal procedure system which is still based on the conventional approach in the Criminal Procedure Code. One of the main challenges is the use of digital evidence which has been legally recognized by the ITE Law, but has not been fully integrated into the structure of the Criminal Procedure Code. This study aims to analyze the urgency of harmonization between criminal procedure law and technology, especially in terms of digital evidence in cybercrime cases. The approach used is normative juridical, by tracing primary and secondary legal sources and studying jurisprudence. The results of the study indicate a normative and procedural gap in the management of digital evidence, which has an impact on the inconsistency of court decisions and the weak effectiveness of digital criminal law enforcement. The author suggests a comprehensive revision of the Criminal Procedure Code, the preparation of technical guidelines for digital evidence, and increasing the capacity of law enforcement resources. Harmonization of procedural law with technological developments is no longer an option, but an urgent need to ensure criminal justice that is relevant to the times.
Say
Keywords: digital evidence, criminal procedure law, cybercrime

INTRODUCTION

The development of digital technology in the last two decades has brought about major transformations in various sectors of life, including in the legal space. Advances in information, communication, and internet of things (IoT) technology have created a new reality that has not only expanded the scope of human interaction but also given rise to new forms of crime that were never known in conventional criminal law. This crime is known as cybercrime, namely a crime that occurs in cyberspace and involves the use of information technology as a means or object of the crime itself (Setiawan, 2021).

Indonesia as a country of law certainly cannot turn a blind eye to the digital transformation that also affects the face of law enforcement, especially in the criminal procedure system. In this context, a big question arises: to what extent is the Indonesian criminal procedure system able to accommodate the dynamics of digital crime and its methods of proof? This question is very important considering that Indonesian criminal procedure law still relies on the Criminal Procedure Code (KUHAP) which was passed in 1981 and until now has not been completely updated.

The Criminal Procedure Code only recognizes five valid forms of evidence in Article 184, namely witness statements, expert statements, letters, instructions, and statements from the accused. In it, there is not a single phrase or terminology that explicitly mentions digital evidence. In fact, in cybercrime, electronic data such as server logs, screenshots, emails, digital voice recordings, and metadata are the main sources of evidence (Hasibuan et al., 2024). This mismatch between criminal procedure law instruments and the need for digital evidence is what creates a regulatory gap and opens up space for legal uncertainty. In response to the digital reality, the Indonesian government has enacted Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) which was later revised by Law No. 19 of 2016. The ITE Law provides legal recognition of electronic information and/or electronic documents as valid evidence, as regulated in Article 5 paragraphs (1) and (2), and Article 44 of the ITE Law. However, this norm does not immediately resolve the

problem, because the position of the ITE Law as lex specialis has not been fully integrated into the criminal procedure law system as lex generalis. As a result, there is a systemic disharmony between normative recognition and the evidentiary structure in court practice (Dhadha et al., 2021).

This disharmony not only raises legal issues, but also disrupts the principle of due process of law, namely the principle that every law enforcement process must be carried out fairly, accountably, and according to procedure. In many cases, judges, prosecutors, and investigators still use conventional approaches to digital evidence without understanding the forensic, authentication, or chain of custody aspects that are international standards (Winarno, 2011). In fact, there are many cases where digital evidence is rejected because it is considered invalid due to inappropriate confiscation procedures or unverified data authenticity (Yoserwan, 2023).

This issue is reinforced by the absence of national technical guidelines from the Supreme Court or the Attorney General's Office regarding the use and assessment of digital evidence in the criminal justice process. Therefore, harmonization between the Criminal Procedure Code and the ITE Law is a necessity to ensure that the criminal procedure law system is able to answer the challenges of the times. This harmonization is not only limited to synchronizing legal texts, but also concerns the reconstruction of the criminal procedure law paradigm to be compatible with digital developments.

In addition to normative and procedural challenges, there are also institutional and human resource challenges. Most law enforcement officers in Indonesia do not yet have adequate digital literacy. In a survey conducted by Hasibuan et al. (2024), it was found that more than 60% of investigators and judges at the regional level still rely on conventional physical evidence and do not yet have a complete understanding of digital forensic analysis, including hash code verification methods, metadata, and device cloning techniques. This proves that digital transformation in criminal law requires not only regulatory reform, but also institutional capacity reform.

At the global level, developed countries have established technical regulations for digital evidence in their procedural legal systems. For example, the United States has the Federal Rules of Evidence (FRE) which regulates the validity and authentication of digital evidence, while European countries refer to the Budapest Convention on Cybercrime (2001) which provides minimum procedural standards and protection of privacy rights in electronic data collection. Unfortunately, Indonesia has not ratified this convention so it does not yet have a strong legal position in handling cross-border evidence, even though digital crimes often involve perpetrators and servers across countries (Ibrahim, 2021).

Thus, the problem of criminal procedure law in the context of digital crime lies not only in the existence of rules, but also in the gap between legal norms, technical capacity, and the reality of practice in the field. Therefore, this article aims to examine legally the urgency of harmonizing criminal procedure law with technological developments, especially in the aspect of proving digital evidence in cybercrime cases.

Systematically, this study will discuss: first, what is the form of inconsistency between the evidentiary system in the Criminal Procedure Code and the evidentiary needs in cybercrime cases; second, what is the legal position of the ITE Law as a norm for recognizing digital evidence and the urgency of its integration in criminal procedural law; and third, what is the ideal model for harmonizing procedural law to support the effectiveness of the digital criminal justice system in the future. This study is expected to provide normative and conceptual contributions to the renewal of the criminal law system in Indonesia to be more adaptive, relevant, and responsive to the digital era.

METHOD

This study uses a normative legal approach, namely an approach that relies on the study of applicable positive legal norms, both in the form of laws and regulations, official legal documents, and court decisions that are relevant to the proof of digital evidence in cybercrime cases. This method

was chosen because the main object of study is the legal-formal aspect of the criminal procedure law system, especially regarding the validity and harmonization of law between the Criminal Procedure Code (KUHAP) and Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE).

The normative legal approach allows the author to systematically examine existing legal texts, then analyze their suitability to current social, technological, and jurisprudential conditions. This study relies on systematic interpretation (systematische interpretatie) and historical interpretation (historische interpretatie) of applicable laws and regulations, especially in terms of how Indonesian criminal procedure law regulates or does not regulate digital evidence (Hasibuan et al., 2024).

The main data source in this research is primary legal materials, which consist of:

1. Criminal Procedure Code (KUHAP)
2. Law Number 11 of 2008 concerning Electronic Information and Transactions
3. Law Number 19 of 2016 (Amendment to the ITE Law)
4. Constitutional Court Decisions, including Decision No. 20/PUU-XIV/2016
5. District court decisions relating to digital evidence

In addition, secondary legal materials are also used, such as criminal procedure books, scientific legal journals, previous research results, and conference articles discussing digital evidence and cybercrime, both nationally and internationally.

The data collection method is carried out through library research, where all data is collected from written documents, both in printed and electronic form. Data analysis is carried out qualitatively, emphasizing the logic of legal argumentation and the relationship between one norm and another. The goal is to find inconsistencies (disharmony), overlaps, or legal vacuums (rechtsvacuum) in the regulation and application of criminal procedure law to digital evidence.

In the final stage, this study uses a conceptual approach to formulate the idea of harmonizing criminal procedural law with technological developments, including by referring to international standards such as the Budapest Convention on Cybercrime, the Federal Rules of Evidence (USA), and comparative practices from other countries that are more advanced in integrating digital evidence systems into their procedural law (Ibrahim, 2021). With this method, it is hoped that the research will be able to answer fundamental legal questions, namely: how the criminal procedural law system in Indonesia can be harmonized with technological needs, without sacrificing the principles of justice, human rights, and legal certainty.

RESULTS AND DISCUSSION

Inconsistency of the Criminal Procedure Code Evidence System with the Need for Digital Evidence

The development of digital technology in the last decade has led to the emergence of new forms of crime that are not only complex in terms of modus operandi, but also in terms of evidence in the courtroom. In the Indonesian context, criminal procedure law—regulated in the Criminal Procedure Code (KUHAP)—still uses a system of evidence that is built on analog logic and does not

anticipate the reality of the cyber world. This creates a fundamental inconsistency between the system of evidence regulated by the KUHAP and the characteristics of evidence in cybercrime.

Article 184 paragraph (1) of the Criminal Procedure Code regulates five valid forms of evidence in criminal cases, namely: (1) witness statements, (2) expert statements, (3) letters, (4) clues, and (5) statements from the accused. However, in the context of cybercrime, the evidence that emerges generally takes the form of digital data, digital footprints, electronic communication recordings, metadata, and so on—which are not explicitly categorized in the provisions of Article 184 of the Criminal Procedure Code (Setiawan, 2021). This opens up space for debate regarding the legal standing of digital evidence in the courtroom.

In practice, many investigators and prosecutors classify digital evidence as part of a "letter" or "clues", depending on its form. For example, screenshots of WhatsApp conversations or server logs are considered letters, while metadata showing the location of the device can be used as clues. However, this approach has limitations because the Criminal Procedure Code does not outline the criteria for the validity of digital evidence, such as file authenticity, seizure procedures, or guarantees of data integrity through chain of custody (Hasibuan et al., 2024). Without explicit recognition of digital evidence as a separate category of evidence, forced interpretations often result in inconsistent decisions between judges and between jurisdictions.

Moreover, the evidentiary system in the Criminal Procedure Code adheres to the principle of negative wettelijk bewijstheorie, namely that the judge's conviction can only be obtained from a minimum of two valid pieces of evidence according to the law. In practice, many judges reject digital evidence because it is considered not to meet the requirements for valid evidence according to Article 184, or because it is not supported by expert testimony explaining the validity and authenticity of the electronic data (Winarno, 2011). This is where the serious disconnection between the need for proof of digital crimes and the rigidity of the current criminal procedure system lies.

On the other hand, there are procedural inconsistencies that are detrimental to the effectiveness of digital evidence. The Criminal Procedure Code still requires that confiscations be carried out with a permit from the head of the district court, as regulated in Articles 38 to 46. When confiscations are carried out on cloud servers, email accounts, or other online storage, law enforcement officers are often unable to comply with this rule perfectly due to the nature of digital data that is scattered and cannot be physically controlled (Yoserwan, 2023). As a result, confiscations are often carried out without legal procedures, which then triggers the cancellation of evidence in court.

Similar problems occur in digital data searches, for example on laptops, smartphones, or social media accounts. The Criminal Procedure Code does not have a mechanism that regulates forensic checking of the contents of digital devices, so that much evidence is obtained without a legal audit trail. Constitutional Court Decision No. 20/PUU-XIV/2016 emphasizes that electronic data collection must be subject to the principle of due process of law, and is carried out through procedures that guarantee citizens' privacy rights (Ibrahim, 2021). However, because there are no implementing provisions that explicitly regulate the technicalities of digital seizures and searches, law enforcement officers are often in a dilemma: between the need for evidence and the limitations of procedural law.

This condition is further exacerbated by the lack of technical guidelines from the Supreme Court or the Attorney General's Office regarding digital evidence. As a result, there is a lack of uniformity in the treatment of digital evidence, both in terms of admissibility in court, assessment of its validity, and its evidentiary weight. Some judges accept screenshots or digital voice recordings as valid evidence, while others reject them because they are not supported by hash values or forensic reports (Dhadha et al., 2021).

Another crucial issue is the absence of a digital evidence authentication system in the Criminal Procedure Code. In other countries, such as the United States, the courts require that every digital file be verified through a hash code (SHA-1 or MD5), which proves that the file has not been modified since it was first seized. However, Indonesia does not yet have such a standard in its criminal

procedure code. This means that anyone can print a fake screenshot and claim it as evidence, without a legitimate mechanism to verify its truth (Supriyono, 2016).

The above issues prove that the current Criminal Procedure Code is no longer adequate to regulate the evidence system in cybercrime cases. The inconsistency lies not only in the absence of explicit mention of digital evidence, but also in the absence of technical regulations and procedural law infrastructure that support the use of technology in the criminal justice process. Without updates, this system will not only hinder law enforcement against cybercrime perpetrators, but also has the potential to harm the rights of suspects and victims because there is no guarantee of legal and transparent procedures.

Given these facts, it can be said that harmonization between criminal procedure law and technological developments is no longer an option, but an urgent necessity. This harmonization is not enough to just add articles on digital evidence, but also to reorganize the entire logic of criminal law evidence to be compatible with digital systems, including the preparation of digital seizure standards, forensic procedures, file authentication, and technical training for law enforcement officers.

Harmonization and Reform Model of Digital Procedural Law Regulation

The advancement of information technology requires the legal system to adapt to the dynamics of the times. In the context of criminal procedural law, this becomes increasingly important when faced with the challenge of proving crimes in cyberspace (cybercrime). As explained in the previous discussion, the Criminal Procedure Code as Indonesia's criminal procedural law is not designed to deal with the types of digital crimes that are developing very rapidly. Therefore, a harmonization model is needed that is able to unite the applicable procedural legal norms with the needs of modern technology, without sacrificing the principles of justice and protection of human rights.

Legally, harmonization is interpreted as the process of aligning legal norms so that there is no normative conflict, overlap, or legal vacuum in its implementation. In this context, harmonization between the Criminal Procedure Code and the ITE Law is essential because the ITE Law has recognized the validity of digital evidence (Article 5 and Article 44), while the Criminal Procedure Code has not stated this explicitly (Setiawan, 2021). The existence of two legal regimes that operate independently risks creating inconsistencies in the application of the law, especially at the level of evidence.

Theoretically, legal harmonization can use an integrative approach, namely combining conventional criminal procedure law provisions with technological and digital principles. This means that the Criminal Procedure Code must be revised comprehensively to include new provisions that explicitly explain the recognition of digital evidence as a stand-alone legal evidence, while also establishing procedures for presentation, authentication, and assessment of its evidentiary strength in court (Hasibuan et al., 2024).

Technology-based criminal procedural law reform should cover at least five aspects:

1. Explicit recognition of digital evidence as a valid and independent evidence outside the classification of Article 184 of the Criminal Procedure Code. This is in line with international practices such as those implemented in the Federal Rules of Evidence (USA) and the Budapest Convention on Cybercrime (2001) (Ibrahim, 2021).
2. Standardization of procedures for collecting and seizing digital evidence, including regulations on electronic search and seizure, cloud data seizure, and searches of digital devices. It is also necessary to regulate the authorities authorized to carry out data collection, the limits of authority, and judicial oversight requirements.
3. Setting standards for digital forensics and authentication of digital evidence, including the use of hash functions, timestamps, metadata, and authorized forensic software to ensure the integrity and authenticity of digital files.

4. Official appointment of digital forensic experts and their expertise procedures. The court must have access to independent and certified expert witnesses, to avoid deviation and manipulation of evidence (Winarno, 2011).
5. Synchronization with international law, especially in terms of cross-border evidence collection, such as the Mutual Legal Assistance Treaty (MLAT), and the possibility of ratifying the Budapest Convention so that cross-border evidence can be carried out in accordance with globally recognized legal procedures (Yoserwan, 2023).
6. C. Summary: Harmonization as a Necessity, Not an Option

From a practical perspective, harmonization between criminal procedure law and technology is the answer to the crisis of legal legitimacy in the digital world. Without the reconstruction of procedural law that accommodates digital reality, the criminal justice system will lose its adaptability and credibility in responding to increasingly complex cybercrimes.

For example, in the case of the distribution of immoral content handled by the Surabaya District Court (Decision No. 261/Pid.Sus/2022/PN Sby), evidence in the form of digital recordings was rejected because the investigator could not explain the chain of custody and no expert examination was carried out. This shows that without technical rules, the validity of digital evidence can be weak in court, even if the evidence material shows a direct connection to the defendant (Hasibuan et al., 2024).

Furthermore, this legal harmonization cannot be done partially. Synergy between institutions is needed, namely the DPR, the Supreme Court, the Prosecutor's Office, and the Police, in compiling a comprehensive digital criminal procedure system. This step must be accompanied by investment in human resources, such as training law enforcement officers on digital forensics, the use of analytical software, and an understanding of the principles of the legality of electronic evidence.

Many countries have proven that updating digital procedural law not only increases the effectiveness of law enforcement but also protects citizens' constitutional rights. For example, Australia and the United Kingdom have developed technical guidelines for digital evidence that are used as national standards. Likewise, the United States has long implemented digital evidence verification in the federal court system through consistent and high-standard rules (Ibrahim, 2021).

CONCLUSION

This study confirms that Indonesian criminal procedure law, as regulated in the Criminal Procedure Code, currently does not have the adaptive capacity to technological developments, especially in terms of proving cybercrime. Meanwhile, digital evidence has become the backbone of proving cyber crime cases, whether in the form of screenshots, metadata, server logs, or communication via social media. However, because it is not explicitly stated in Article 184 of the Criminal Procedure Code, the legal position of digital evidence often depends on the subjective interpretation of law enforcement officers (Setiawan, 2021).

Normatively, the presence of Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016, is an initial step in providing legal recognition of electronic evidence. Articles 5 and 44 of the ITE Law explicitly state that electronic information and/or electronic documents can be used as valid legal evidence. However, the position of the ITE Law as lex specialis has not been fully integrated systemically with criminal procedure law (KUHAP) which functions as lex generalis (Hasibuan et al., 2024).

This inconsistency has various practical consequences. First, the absence of legal standards in the seizure, collection, and presentation of digital evidence makes digital data vulnerable to being disputed in court. Second, the lack of technical regulations and guidelines for digital evidence from the judiciary and executive institutions causes judicial practices to be inconsistent. Third, the low digital literacy of law enforcement officers—both judges, prosecutors, and investigators—contributes to weak evidence in cyber cases (Winarno, 2011).

Systemically, the regulation of evidence in the Criminal Procedure Code is still analogous, and does not accommodate elements such as hash codes, file authentication, timestamps, and chain of custody, which are important elements in digital forensic evidence. At the international level, other countries such as the United States, the United Kingdom, and European Union countries have developed comprehensive digital procedural law standards, which allow electronic evidence to be assessed objectively, scientifically, and measurably (Ibrahim, 2021).

Based on the above explanation, harmonization of criminal procedure law with technological developments is no longer an option, but an urgent legal necessity. This harmonization needs to be done either through a comprehensive revision of the Criminal Procedure Code or through the issuance of implementing regulations that bridge the ITE Law and the Criminal Procedure Code. This effort must involve all stakeholders, starting from the DPR, the Supreme Court, the Attorney General's Office, to legal education institutions and digital forensic professionals.

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.

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.

lwan Rasiwan, H., & MH SH. (2025). The Principle of Balance of the New Criminal Code Reflects Pancasila Values in Law Enforcement. Takaza Innovatix Labs.

State, Third Amendment to the Constitution. (2001). Republic of Indonesia 1945. Jakarta: Secretariat General of the MPR RI.

(nd). The Role of Telematics Law in Resolving Cybercrime Cases.

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.

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.

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

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