Reconstruction of Electronic Evidence in Cyber Fraud Criminal Offenses in Indonesia

M. Ihsan, Mhd. Azhali Siregar, T. Riza Zarzani

Abstract

The rapid advancement of digital technology has fundamentally transformed the pattern of criminal activity in Indonesia, particularly in the form of cyber fraud. Electronic transactions, digital communication systems, and internet-based financial activities have introduced new challenges to criminal law enforcement, especially concerning the validity and evidentiary weight of electronic evidence. This study aims to analyze the weaknesses of the current electronic evidence system in cyber fraud cases and to formulate a legal reconstruction model capable of strengthening the evidentiary mechanism within Indonesia's criminal justice system. This study employs a normative legal research method utilizing statutory, conceptual, and case approaches. The legal materials consist of legislative regulations, court decisions, academic journals, and legal doctrines pertaining to electronic evidence and cybercrime. The findings indicate that the existing evidentiary framework remains fragmented, overlapping, and insufficiently adaptive to technological developments. In practice, investigators, prosecutors, and judges frequently encounter difficulties in establishing the authenticity, integrity, and admissibility of electronic evidence. This study further reveals that limited digital forensic capacity and the absence of comprehensive procedural standards contribute to legal uncertainty in the adjudication of cyber fraud cases. Accordingly, legal reconstruction is necessary through the harmonization of procedural law, the strengthening of digital forensic institutions, the standardization of electronic evidence verification, and the modernization of criminal procedure law in a manner responsive to technological progress. Such reconstruction is expected to bring about a more effective, equitable, and legally certain criminal justice system in the handling of cyber fraud offenses in Indonesia.

Keywords: Electronic Evidence, Cyber Fraud, Digital Forensics, Criminal Law, Cybercrime.

M. Ihsan[1]
[1]Magister of Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: ihsanpolda12@gmail.com

Mhd. Azhali Siregar[2], T. Riza Zarzani[3]
[2,3]Magister of Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: azhalisiregar@dosen.pancabudi.ac.id[2], rizazarzani@dosen.pancabudi.ac.id[3]
3rd International Conference Epicentrum of Economic Global Framework (ICEEGLOF)
Theme: Cross-Sector and Cross-Disciplinary Strategies for Achieving the SDGS
https://proceeding.pancabudi.ac.id/index.php/ICEEGLOF

Introduction

Over the past two decades, developments in information technology have significantly transformed nearly all aspects of social life, including patterns of economic interaction, communication, and financial transactions. The rapid expansion of digitalization has yielded positive outcomes by improving efficiency across various societal activities. Nevertheless, these developments have also given rise to increasingly complex and transnational forms of crime. One of the most rapidly evolving forms of criminal offense is cyber fraud (*cyber fraud*), referring to fraudulent acts committed through electronic systems. This phenomenon demonstrates that technological advancement is not always accompanied by sufficient legal preparedness to anticipate the evolving dynamics of digital crime [1].

Cyber fraud has evolved through various modus operandi, including *phishing*, *social engineering*, digital investment fraud, manipulation of electronic transactions, digital identity theft, and unauthorized access to accounts through technological engineering [2]. The characteristics of this criminal offense differ fundamentally from conventional crime, as it is perpetrated through electronic systems, involves digital data both as an object and as an instrument of crime, and requires an evidentiary approach distinct from traditional criminal proof mechanisms. In practice, proving cyber fraud cases does not rely solely on conventional evidence as regulated under the Criminal Procedure Code (KUHAP), but also necessitates the validation of electronic evidence, which is dynamic in nature, susceptible to manipulation, and vulnerable to alteration.

According to reports published by the National Cyber and Crypto Agency (BSSN), Indonesia has experienced a significant increase in various cyber threats in recent years, including *phishing* attacks and digital fraud targeting both the public and financial institutions [3]. Furthermore, data published by the Financial Services Authority (OJK) indicates that digital banking crimes and electronic transaction fraud continue to rise in tandem with the rapid growth of digital financial services in Indonesia [4]. These facts reflect a substantial gap between technological development and the effectiveness of law enforcement mechanisms, particularly with regard to electronic evidence systems.

From a normative standpoint, recognition of electronic evidence has been accommodated through Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016. Article 5 paragraph (1) of the ITE Law explicitly stipulates that electronic information, electronic documents, and their printed outputs constitute valid legal evidence [5]. This provision expands the evidentiary system in Indonesian criminal procedural law, which previously recognized only five categories of evidence as stipulated in Article 184 of the KUHAP. Nevertheless, these regulations have not yet fully addressed the complexity of the evidentiary process in cyber fraud cases.

The primary challenge lies in the absence of comprehensive procedural standards governing the collection, examination, storage, and verification of electronic evidence. In law enforcement practice, divergent interpretations frequently arise regarding the validity of digital evidence, the application of *chain of custody*, electronic data authentication, and the capacity of digital forensic laboratories to verify the authenticity of evidence [6]. This situation creates legal uncertainty and has the potential to impede the evidentiary process in criminal proceedings.

Numerous cyber fraud cases have revealed evidentiary obstacles stemming from the compromised integrity of electronic evidence. In several instances, judges have determined that the digital evidence submitted failed to meet adequate authentication standards or was not supported by comprehensive digital forensic examination [7]. This situation indicates that the normative recognition of electronic evidence has not been accompanied by corresponding institutional and procedural readiness in law enforcement practice.

From a theoretical perspective, the law of evidence plays a pivotal role in realizing substantive justice. Evidence is not merely understood as a formal mechanism for establishing the guilt of the accused, but also as an instrument for the protection of human rights to ensure

that judicial proceedings are conducted objectively, accountably, and fairly [8]. Therefore, the use of electronic evidence in cyber fraud cases necessitates legal reconstruction capable of reconciling technological developments with the principles of *due process of law*.

Prior studies have generally focused on the recognition of electronic evidence within the criminal law system or the effectiveness of the ITE Law in combating cybercrime. However, relatively few studies have specifically examined the reconstruction of electronic evidence systems in cyber fraud cases through an integrative approach that combines normative, digital forensic, and criminal procedure reform dimensions. This study seeks to fill this academic gap by emphasizing the urgency of reforming the electronic evidence legal framework in Indonesia.

Indonesia's criminal law system must fundamentally develop in an adaptive manner in response to social dynamics and technological advancement. According to Mhd. Azhali Siregar, the development of Indonesian criminal law cannot be separated from the necessity of building a legal system that is responsive to social transformation and global challenges [9]. This perspective is particularly relevant in the context of cyber fraud, which is characterized by its transnational nature and heavy reliance on complex technological systems.

Furthermore, the human rights perspective must be positioned as a foundational principle in the reform of electronic evidence mechanisms. The use of digital evidence must continue to uphold the principles of legality, privacy protection, and the guarantee of a *fair trial*) in order to prevent the abuse of authority in law enforcement practice [10]. In this context, the reconstruction of electronic evidence is not solely concerned with the effectiveness of criminal law enforcement, but also encompasses the protection of citizens' constitutional rights.

Based on the foregoing discussion, this study focuses on two primary legal issues. First, what are the weaknesses of the electronic evidence system in the handling of cyber fraud criminal offenses in Indonesia? Second, how should the ideal legal reconstruction of electronic evidence be formulated in the handling of cyber fraud criminal offenses in Indonesia?

Research Methodology

This study employs a normative legal research method utilizing a statutory approach (*statutory approach*), a conceptual approach (*conceptual approach*), and a case approach (*case approach*) [11]. The normative legal research method was selected because this study focuses on the analysis of legal norms governing electronic evidence in cyber fraud criminal offenses, as well as the legal reconstruction required to strengthen the evidentiary system in Indonesia [12].

The statutory approach involves examining various legislative regulations pertaining to electronic evidence, including the Criminal Procedure Code (KUHAP), Law Number 11 of 2008 on Electronic Information and Transactions as amended by Law Number 19 of 2016, Law Number 1 of 2024 on the Second Amendment to the Electronic Information and Transactions Law, and various technical regulations relating to digital forensics and cybersecurity [13].

The conceptual approach is employed to analyze legal concepts pertaining to electronic evidence, digital forensics, cyber fraud, and the evidentiary system within criminal law. This approach is conducted through an examination of legal doctrine, expert opinions, and legal theories relevant to the subject of research. Meanwhile, the case approach involves the analysis of a number of court decisions related to cyber fraud criminal offenses, in which electronic evidence constitutes the primary basis of the evidentiary process [14].

The legal materials used in this study consist of primary, secondary, and tertiary legal sources. Primary legal materials include legislative regulations, court decisions, and official state documents. Secondary legal materials comprise academic journals, scholarly books, research articles, and seminar proceedings relevant to the research topic. Tertiary legal materials encompass legal dictionaries, legal encyclopedias, and other supporting references [15].

The technique for collecting legal materials is conducted through library research (*library research*) by examining legal literature, reputable academic journals, and official documents pertaining to electronic evidence and cyber fraud criminal offenses. Data collection also

involves searching various national and international academic journal databases whose scholarly validity is academically accountable [16].

Analysis of legal materials is conducted qualitatively using a descriptive-analytical method. This analysis involves the interpretation of legal norms, the synchronization of legislative regulations, and the construction of legal arguments based on prevailing legal theories and law enforcement practice. In the analytical process, the authors also employ a prescriptive approach to formulate an ideal model of electronic evidence legal reconstruction within Indonesia's criminal justice system [17].

This research methodology is considered appropriate as it provides a comprehensive overview of both the normative and practical weaknesses in the use of electronic evidence in the handling of cyber fraud criminal offenses. Furthermore, the normative approach enables the authors to formulate legal solutions that are more systematic, responsive, and adaptive to the rapidly evolving landscape of digital technology.

Results

1. Weaknesses of the Electronic Evidence System in Handling Cyber Fraud Criminal Offenses in Indonesia

Electronic evidence in cyber fraud cases has fundamentally obtained normative legitimacy through provisions stipulated in the Electronic Information and Transactions Law (ITE Law). Nevertheless, such formal recognition has not yet fully addressed the various challenges encountered in law enforcement practice. One of the primary weaknesses lies in the lack of harmonization between the Criminal Procedure Code (KUHAP) and modern electronic regulations. The KUHAP, which has been in force since 1981, remains oriented toward conventional evidentiary mechanisms and does not comprehensively regulate the use of digital evidence [18].

This situation creates a legal vacuum in electronic evidence practice. Law enforcement officers frequently apply divergent interpretations regarding the validity and admissibility of digital evidence. In several cyber fraud cases, evidence in the form of screenshots (*screenshot*), digital communication recordings, and electronic transaction data have often become the subject of legal dispute due to the absence of adequate authentication procedures [19].

In addition to normative concerns, weaknesses are also evident in the technical aspects of digital forensics. Not all law enforcement institutions are equipped with adequate digital forensic laboratory facilities. Moreover, the competency of human resources in the field of digital investigation remains relatively limited in comparison to increasingly complex and evolving cyber fraud methodologies [20]. As a result, the evidentiary process frequently encounters technical obstacles in identifying perpetrators and verifying the integrity of electronic data.

The issue of *chain of custody* also constitutes a serious concern in electronic evidence practice. Digital evidence is highly susceptible to modification, deletion, and data manipulation. If data security procedures are not properly implemented from the stage of seizure through to presentation at trial, the integrity of the evidence may be called into question [21]. In practice, cases continue to arise in which electronic evidence is submitted without complete procedural documentation.

A further weakness concerns the suboptimal inter-agency synchronization in the handling of cyber fraud criminal offenses. Cybercrime investigations frequently involve the police, prosecutors, courts, banking institutions, telecommunications service providers, and cybersecurity authorities. Nevertheless, inter-agency coordination has not yet functioned effectively [22]. Consequently, the process of tracing electronic data and digital transactions often experiences significant delays.

From a human rights perspective, the use of electronic evidence also carries the risk of authority abuse if not strictly regulated. The collection of digital data without clear legal procedures may violate the privacy rights of the public. Therefore, electronic evidence practice

must remain within the framework of *due process of law* in order to safeguard the constitutional rights of citizens [23].

In this context, Lawrence M. Friedman's legal system theory demonstrates that the issues surrounding electronic evidence are not solely related to legal substance, but also concern legal structure and legal culture. Incomplete regulations, limited institutional capacity, and insufficient understanding of digital technology among law enforcement personnel collectively contribute to the weakened effectiveness of the electronic evidence system.

Based on the foregoing analysis, weaknesses in the electronic evidence system in cyber fraud cases may be identified across several dimensions, namely regulatory weaknesses, technical limitations in digital forensics, inadequate inter-agency coordination, insufficient human resource capacity, and suboptimal human rights protection. These issues collectively underscore the urgency of undertaking a more adaptive and comprehensive reconstruction of the electronic evidence system.

2. Legal Reconstruction of Electronic Evidence in Handling Cyber Fraud Criminal Offenses in Indonesia

The legal reconstruction of electronic evidence must be conducted systematically through regulatory reform, institutional strengthening, and the enhancement of law enforcement capacity. The first step required is the harmonization of electronic evidence regulations within the revision of the Criminal Procedure Code (KUHAP). Reform of criminal procedural law must explicitly address the definition, classification, collection procedures, authentication mechanisms, seizure protocols, and judicial examination of electronic evidence [24].

The establishment of national digital forensic standards is also an urgent necessity. Such standards must encompass *chain of custody* procedures, digital data examination methods, digital forensic expert certification systems, and digital forensic laboratory accreditation mechanisms. The application of uniform standards will enhance the validity of electronic evidence while simultaneously reducing interpretive disparities among law enforcement officers [25].

Furthermore, the strengthening of human resource capacity constitutes a critical dimension of the legal reconstruction of electronic evidence. Investigators, prosecutors, judges, and legal practitioners require specialized training in information technology and digital forensics. The complexity of cyber fraud criminal offenses demands that law enforcement personnel possess multidisciplinary competencies encompassing not only criminal law, but also technical knowledge of information technology.

From an institutional perspective, an integrated coordination system between law enforcement agencies and cybersecurity authorities is required. Data integration and rapid information-sharing mechanisms will enhance the effectiveness of cyber fraud investigations. In addition, the state must strengthen international cooperation given the transnational nature of cyber fraud criminal offenses (*transnational crime*) [26].

The reconstruction of electronic evidence must also place the protection of human rights as a paramount priority. The use of digital evidence must be grounded in clear legal procedures and accountable oversight mechanisms. Surveillance activities, electronic data retrieval, and access to digital systems must be conducted on the basis of lawful authority and in accordance with the principle of proportionality [27].

From the perspective of progressive law, the legal system must be capable of adapting to social and technological developments. Accordingly, electronic evidence can no longer be regarded merely as a supplement to conventional evidence, but must be positioned as an integral component of the modern criminal justice system. Evidence law reform must be directed toward the establishment of a flexible evidentiary framework, without compromising the principles of legal certainty and justice.

This view is consistent with Siregar's assertion that Indonesia's legal system must be constructed in an adaptive manner in response to social transformation and global challenges

[28]. In the context of cyber fraud, the reform of electronic evidence law constitutes a vital component for maintaining the effectiveness of law enforcement in the digital era [29].

Furthermore, restorative and preventive approaches must also be integrated into the handling of cyber fraud criminal offenses. The state should not focus solely on the punishment of perpetrators, but must also strengthen public digital literacy, personal data protection, and national electronic system security. These efforts are essential for reducing the structural potential for cybercrime [30].

Thus, the legal reconstruction of electronic evidence in cyber fraud cases must be undertaken through regulatory reform, digital forensic standardization, the enhancement of law enforcement capacity, institutional integration, the protection of human rights, and the strengthening of international cooperation. Such reconstruction is expected to bring about an evidentiary system that is modern, effective, just, and legally certain in the handling of cyber fraud criminal offenses in Indonesia [31].

Conclusion

The electronic evidence system in the handling of cyber fraud criminal offenses in Indonesia continues to face numerous weaknesses, particularly in the areas of regulation, digital forensic technology, law enforcement capacity, and inter-agency coordination. The lack of harmonization between the Criminal Procedure Code (KUHAP) and modern electronic regulations has generated legal uncertainty in the practical use of electronic evidence. Furthermore, the absence of comprehensive national digital forensic standards and the inadequate implementation of *chain of custody* mechanisms have further undermined the effectiveness of the evidentiary process in cyber fraud cases.

The legal reconstruction of electronic evidence must be undertaken through the reform of criminal procedural law in a manner adaptive to technological developments, the standardization of digital forensic systems, the enhancement of law enforcement capacity and competency, and the establishment of integrated inter-agency coordination mechanisms. In addition, the protection of human rights must remain a fundamental principle in the use of electronic evidence in order to ensure that law enforcement processes are conducted fairly, proportionately, transparently, and accountably. Accordingly, the legal reconstruction of electronic evidence is expected to bring about a criminal justice system that is more effective, modern, just, and legally certain in the handling of cyber fraud criminal offenses in Indonesia.

References

[1] B. B. N. Nasional, “Annual Report on Indonesian Cybersecurity 2024,” Jakarta, 2024.
[2] R. Nugroho, *Cyber Crime and the Electronic Evidence System*. Jakarta: Kencana, 2022.
[3] Badan Siber dan Sandi Negara, “Indonesian Cybersecurity Landscape 2024,” Jakarta, 2024.
[4] Otoritas Jasa Keuangan, “Development of Cybercrime in the Financial Services Sector 2024,” Jakarta, 2024.
[5] Republik Indonesia, *Law Number 11 of 2008 on Electronic Information and Transactions*.
[6] Republik Indonesia, *Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions*.
[7] E. S. Wahyuni, “The Position of Electronic Evidence in Indonesian Criminal Procedural Law,” *Jurnal Ius Constituendum*, vol. 8, no. 2, pp. 145–160, 2023.
[8] M. Yahya Harahap, *Discussion of Issues and Application of the KUHAP*. Jakarta: Sinar Grafika, 2021.
[9] M. A. Siregar, R. F. Adrian, and M. J. Rambe, *Tracing the Origins of the Criminal Law System Concept in Indonesia*. Tahta Media, 2023.
[10] M. A. Siregar, *Human Rights in the Indonesian Legal System*. Medan: Pustaka Prima, 2024.

[11] L. M. Friedman, *The Legal System: A Social Science Perspective*. Bandung: Nusa Media, 2020.
[12] M. A. Siregar, R. F. Adrian, and M. J. Rambe, "Tracing the Origins of the Criminal Law System and Criminal Law Concepts in Indonesia," Penerbit Tahta Media, 2023.
[13] Andi Hamzah, *Indonesian Criminal Procedural Law*. Jakarta: Sinar Grafika, 2022.
[14] A. Rachman, "The Problematics of Electronic Evidence in Cybercrime Cases," *Jurnal Rechtsvinding*, vol. 12, no. 1, pp. 33–49, 2024.
[15] D. Sembiring, "Digital Forensics in Handling Cyber Criminal Offenses in Indonesia," *Jurnal Hukum dan Teknologi*, vol. 5, no. 2, pp. 88–102, 2023.
[16] Prakoso, "Chain of Custody in Electronic Evidence," *Jurnal Legislasi Indonesia*, vol. 20, no. 3, pp. 210–225, 2023.
[17] H. Aspan, "Challenges of Cyber Law Enforcement in Indonesia," *Jurnal Supremasi Hukum*, vol. 19, no. 1, pp. 67–81, 2024.
[18] M. F. Mahmud, "Privacy Rights Protection in Electronic Evidence," *Jurnal Konstitusi*, vol. 21, no. 2, pp. 140–156, 2024.
[19] Barda Nawawi Arief, *Criminal Law Reform from a Policy Perspective*. Jakarta: Kencana, 2022.
[20] S. Rahardjo, *Progressive Law*. Jakarta: Kompas, 2021.
[21] M. A. Siregar, *Human Rights in the Indonesian Legal System*. Medan: Pustaka Prima, 2024.
[22] T. M. A. Fitra, T. R. Zarzani, H. Aspan, and M. A. Siregar, "Inheritance distribution for heirs of different religions: A juridical review based on the compilation of Islamic law in Indonesia," in *Proceedings of International Conference on Islamic Community Studies*, Oct. 2025, pp. 6733–6738.
[23] S. Arikunto, *Legal Research Methods*. Yogyakarta: Deepublish, 2021.
[24] R. Soesilo, *Fundamentals of Criminal Procedural Law*. Bogor: Politeia, 2020.
[25] A. Widodo, "The Urgency of Electronic Evidence Reform in the New KUHAP," *Jurnal Yudisial*, vol. 17, no. 1, pp. 77–92, 2024.
[26] N. Kurniawan, "Cyber Fraud and the Challenges of Digital Law Enforcement," *Jurnal Media Hukum*, vol. 31, no. 2, pp. 201–218, 2024.
[27] M. Ali, "The Validity of Digital Evidence in the Criminal Justice System," *Jurnal Hukum Ius Quia Iustum*, vol. 30, no. 3, pp. 410–426, 2023.
[28] S. Susanto, "Reconstruction of Criminal Procedural Law in the Digital Era," *Jurnal Arena Hukum*, vol. 17, no. 1, pp. 55–73, 2024.
[29] T. R. Zarzani and B. Fitrianto, "The Idea of Renewing Terrorism Criminal Law in Indonesia as an Effort to Overcome Terrorism Based on the Justice Values," International Journal of Law Reconstruction, vol. 8, no. 1, pp. 38–55, 2024.
[30] R. Sepatia, T. R. Zarzani, and M. Purba, "Juridical Analysis of Criminal Liability for Website Creators Used for Online Gambling (Analysis of Decision No. 852/Pid.Sus/2020/PN.Mdn)," Jurnal Rectum: Juridical Review of Criminal Offense Handling, vol. 4, no. 2, pp. 430–442, 2022.
[31] B. A. M. Sitepu, T. R. Zarzani, and Y. M. Saragih, "Development of Criminal Procedure Law Norms Based on Constitutional Court Decisions," International Journal Reglement & Society (IJRS), vol. 4, no. 3, pp. 209–216, 2023.