Volume 4 Number 1 (2026)
July-December 2026
Page: 759-772

Journal of Creative Power and Ambition (JCPA)
https://edujavare.com/index.php/jcpa
E-ISSN: 3031-4054
DOI: 10.70610/jcpa.1834

Reconstruction of the Standards for Assessing the Probative Value of Electronic Evidence in the Indonesian Criminal Justice System: A Cyberlaw Perspective

Adrian Bima Putra[1]
[1] Faculty of Law, University of 17 Agustus 1945 Jakarta, Indonesia;
* Correspondence e-mail; adrianbima92@gmail.com

Article history Submitted: 2026/04/01; Revised: 2026/05/11; Accepted: 2026/06/20

Abstract

The rapid development of information technology has transformed the evidentiary system within Indonesia's criminal justice process. Although electronic information and electronic documents have been recognized as legal evidence under Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, there remains no comprehensive legal standard governing the assessment of their evidentiary value. This condition has created legal uncertainty regarding authenticity, integrity, reliability of electronic systems, chain of custody, and digital forensic verification. This research aims to analyze the legal framework governing electronic evidence in Indonesia and to formulate a reconstruction model for assessing the evidentiary strength of electronic evidence from a cyber law perspective. The study employs normative legal research using statutory, conceptual, and case approaches. Legal materials are analyzed qualitatively through descriptive-analytical methods. The findings reveal that the current legal framework remains fragmented and lacks comprehensive standards for evaluating electronic evidence. Consequently, this study proposes a reconstruction model consisting of five principal indicators: authenticity, integrity, reliability of electronic systems, chain of custody, and digital forensic verification. This model is expected to serve as a conceptual basis for reforming Indonesia's criminal procedural law in order to enhance legal certainty, justice, and the effectiveness of evidence assessment in technology-based criminal cases.

Keywords Electronic Evidence; Cyber Law; Criminal Evidence; Digital Forensics; Criminal Procedure.

INTRODUCTION

The Advances in information and communication technology have brought fundamental changes to various aspects of society, including the criminal justice system. Human activities that were previously conducted conventionally have now shifted to the digital realm through the use of social media, instant messaging apps, email, cloud computing services, and various other electronic platforms. This transformation has led to changes in the nature of evidence in criminal cases. Electronic

information and electronic documents have now become increasingly dominant sources of evidence, particularly in cases involving cybercrimes, fraud, extortion, defamation, online gambling, and other criminal offenses that exploit information technology.

In response to these developments, the legislature has recognized electronic information and/or electronic documents as valid legal evidence through Law No. 11 of 2008 on Electronic Information and Transactions, which has been amended several times, most recently by Law No. 1 of 2024. Article 5 of the Electronic Information and Transactions Law (ITE Law) affirms that electronic information, electronic documents, and their printed copies constitute valid legal evidence as an extension of the evidence regulated in the Criminal Procedure Code (KUHAP). This recognition represents a significant step in the modernization of the law of evidence in Indonesia.

Nevertheless, this normative recognition of electronic evidence has not yet been fully accompanied by the establishment of legal standards regarding how to assess its probative value. The KUHAP remains oriented toward conventional evidence as stipulated in Article 184(1), whereas the characteristics of electronic evidence differ significantly from those of physical documents. Electronic evidence can be easily copied, transferred, modified, or even manipulated without altering its physical form. Therefore, the use of electronic evidence requires specific parameters to ensure authenticity, integrity, the reliability of the electronic system, the chain of custody, and digital forensic verification.

In criminal judicial practice, differing approaches to evaluating electronic evidence are still observed. Some rulings accept screenshots or conversations via instant messaging apps as evidence with probative value, while other rulings require an examination by a digital forensics expert to ensure the authenticity and integrity of the electronic data. These differences indicate the absence of uniform standards regarding the probative value of electronic evidence, which has the potential to lead to disparities in rulings and reduce legal certainty.

Previous studies have generally focused on the admissibility of electronic evidence under the ITE Law or examined its use in specific types of criminal offenses. These studies have made important contributions to the development of the law of evidence; however, they have not comprehensively formulated normative parameters that judges can use as a basis for assessing the probative value of electronic evidence. Furthermore, previous studies have not integrated the approach to cyberlaw with aspects of digital forensics, the chain of custody, and the reliability of electronic systems as a unified whole within the evidentiary process.

Given these circumstances, there is a research gap: the absence of a conceptual model that can serve as a standard for assessing the probative value of electronic evidence within the Indonesian criminal justice system. This gap is becoming increasingly relevant given the rising use of electronic evidence in various criminal cases and the growing complexity of information technology developments.

This study aims to analyze the legal framework regarding electronic evidence in the Indonesian criminal justice system and to formulate a standard model for assessing the probative value of electronic evidence from a cyberlaw perspective. Unlike previous studies, this research offers a model that integrates five key indicators, such as authenticity, integrity, reliability of electronic systems, chain of custody, and digital forensic verification as parameters for assessing the probative value of electronic evidence.

It is hoped that this study will not only enrich the development of criminal procedural law and cyberlaw but also provide recommendations for lawmakers, the Supreme Court, law enforcement officials, and practitioners in formulating standards for electronic evidence that are more adaptable to advancements in information technology and capable of ensuring legal certainty, justice, and public benefit within Indonesia's criminal justice system.

METHODS

A normative legal research approach was chosen because the subject of study focuses on legislation, legal principles, legal doctrines, court decisions, and legal concepts related to electronic evidence. The approaches used include the statutory approach, the conceptual approach, and the case approach. The statutory approach was conducted through an analysis of the Criminal Procedure Code, Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 27 of 2022 on Personal Data Protection, as well as various other legal provisions related to electronic evidence. A conceptual approach was used to examine the theory of criminal evidence, the theory of legal systems, the theory of legal certainty, and the doctrine of cyberlaw. Meanwhile, a case based approach was employed by analyzing relevant court decisions to understand the application of electronic evidence in criminal judicial practice.

The legal materials used consist of primary, secondary, and tertiary sources. Primary legal materials include laws and regulations and court decisions related to electronic evidence. Secondary legal materials consist of books, scholarly journal articles, research findings, and expert opinions in the fields of criminal procedure law, evidence law, cyberlaw, and digital forensics . Tertiary legal materials include legal

dictionaries, legal encyclopedias, and other supporting sources that aid in understanding technical terms used in the research. The collection of legal materials was conducted through library research by reviewing various relevant legal sources, both in print and electronic formats. Subsequently, all legal materials were analyzed using qualitative legal analysis methods with descriptive-analytical techniques. The analysis was conducted through systematic, grammatical, and teleological interpretations of applicable legal norms, which were then linked to legal theory, doctrine, and developments in electronic evidence practice.

To generate prescriptive recommendations, this study employs legal reasoning techniques to evaluate the adequacy of existing regulations and to formulate a model for reconstructing standards for assessing the probative value of electronic evidence. The resulting model is expected to serve as a conceptual contribution to the reform of Indonesian criminal procedure law, particularly in light of advancements in information technology and the increasing use of electronic evidence in criminal judicial proceedings.

FINDINGS AND DISCUSSION

Legal Policy on the Regulation of Electronic Evidence in the Indonesian Criminal Justice System

The Advances in information technology have transformed the paradigm of the evidentiary system in Indonesian criminal procedure law.10 Whereas initially the evidentiary system recognized only conventional forms of evidence as stipulated in Article 184(1) of the Criminal Procedure Code (KUHAP), namely witness testimony, expert testimony, documents, circumstantial evidence, and the defendant's statement, advancements in information technology now necessitate the recognition of electronic evidence as an integral part of the modern evidentiary system. This change is a logical consequence of the increasing volume of public activities conducted through electronic media, such that various legal facts are no longer reflected solely in physical documents but also in the form of digital information.

Normatively, the recognition of electronic evidence is grounded in Law No. 11 of 2008 on Electronic Information and Transactions, which has been amended several times and was most recently amended by Law No. 1 of 2024.12 Article 5 of the ITE Law affirms that electronic information and/or electronic documents, along with their printed copies, constitute valid legal evidence. This provision expands the evidentiary regime in Indonesian criminal procedure law without eliminating the fundamental principles of evidence as stipulated in the Criminal Procedure Code (KUHAP).

This normative recognition represents the state's response to developments in digital technology. However, this recognition has not yet been fully accompanied by the establishment of comprehensive standards for the examination of electronic evidence . To date, the Criminal Procedure Code (KUHAP) remains structured around

a conventional evidentiary paradigm and thus does not provide detailed regulations regarding the mechanisms for examining, validating, or evaluating electronic evidence. This situation has resulted in a considerable margin of interpretation for law enforcement officials and judges in determining the probative value of electronic information.

From a legal policy perspective, the regulation of electronic evidence is part of the state's efforts to build a legal system that is adaptive to the development of a digital society. Legal policy is not only understood as the policy of lawmakers in producing legal norms but also reflects the direction of national legal development aimed at realizing legal certainty, justice, and public benefit. Therefore, the existence of electronic evidence cannot be viewed merely as the addition of a new type of evidence but rather as a paradigm shift in the system of proof that demands a comprehensive reform of criminal procedure law.

According to M. Yahya Harahap, Indonesia's criminal evidentiary system adheres to the "negatief wettelijk bewijs theorie," or the theory of legal proof based on statute combined with the judge's conviction. This means that a judge must not only rely on evidence deemed admissible under the law but must also form a conviction regarding the truth of the criminal events. In the context of electronic evidence, this theory poses new challenges because the judge's conviction depends heavily on the ability to assess the authenticity, integrity, and reliability of the electronic data presented in court. This issue becomes even more complex when electronic evidence originates from digital communication applications such as WhatsApp, Telegram, email Use the "Insert Citation" button to add citations to this document. (e-mail), social media, or cloud computing services. Unlike conventional documents, electronic information is easily altered, copied, transferred, or manipulated without changing its physical form. Therefore, proving the validity of electronic evidence requires not only demonstrating the existence of the electronic document but also ensuring that the document possesses a level of authenticity and integrity that is scientifically and legally verifiable.

On the other hand, developments in international law indicate that various countries have established more comprehensive standards regarding electronic evidence. Singapore, for example, through its Evidence Act, provides more detailed regulations on the admissibility of electronic documents, taking into account the reliability of the electronic systems used. Malaysia, through its Evidence Act 1950, also regulates the mechanisms for admitting electronic documents as evidence, along with specific certification requirements for them to be accepted as evidence in court. The experiences of these two countries demonstrate that the recognition of electronic evidence must be accompanied by clear evidentiary standards to ensure legal certainty.

When compared to practices in Indonesia, regulations regarding electronic evidence remain somewhat fragmented, as they are scattered across various laws and regulations without full harmonization with criminal procedure law. Consequently,

law enforcement officials often adopt differing approaches in obtaining, securing, and presenting electronic evidence in court. These differences have the potential to lead to inconsistent rulings and reduce the level of legal certainty.

Based on this discussion, it is clear that the legal policy regarding the establishment of electronic evidence has not yet been fully reflected in the reform of the criminal evidentiary system. The normative recognition through the ITE Law is a progressive step, but harmonization with the Criminal Procedure Code (KUHAP) is still necessary to ensure that electronic evidentiary mechanisms adhere to uniform standards. Such harmonization is crucial given that cybercrime is becoming increasingly complex and that the majority of evidence in such cases relies on electronic information.

From a cyberlaw perspective, reforming the evidentiary system requires not only expanding the types of evidence but also integrating the principles of authenticity, integrity, chain of custody, digital forensic verification, and reliability as key indicators in assessing the probative value of electronic evidence. Thus, Indonesia's criminal evidentiary system not only provides legal certainty for law enforcement officials but also ensures the protection of the human rights of all parties involved in legal proceedings in the digital age.

Issues Regarding the Evidentiary Weight of Electronic Evidence in Indonesian Criminal Judicial Practice

The recognition of electronic evidence as admissible evidence under the Law on Information and Electronic Transactions represents a progressive step in aligning Indonesia's legal system with advancements in information technology. However, this normative recognition has not yet been fully accompanied by the establishment of uniform evidentiary standards in criminal judicial practice. Consequently, the process of admitting electronic evidence still faces various issues that have implications for legal certainty, the protection of human rights, and the achievement of substantive justice.

One fundamental issue lies in the absence of standardized parameters regarding the probative value of electronic evidence. In court proceedings, judges often accept evidence in the form of screenshots, WhatsApp conversations, emails, audio recordings, or video recordings without a uniform standard for their examination. This situation leads to disparities in the evaluation of electronic evidence because not all digital evidence has the same level of reliability. A screenshot, for example, may have been edited, had its metadata manipulated, or had its content altered using specific software, so its authenticity is questionable unless supported by a digital forensic examination.

The next issue relates to the aspect of authenticity. From the perspective of the law of evidence, authenticity is a primary requirement for evidence to be considered credible. With conventional evidence, authenticity is relatively easier to prove through signatures, official stamps, or physical examination of documents. Conversely, with electronic evidence, authenticity depends not only on the form of the document but

also on the electronic systems that generate, store, transmit, and secure the data. Therefore, verifying authenticity requires a more comprehensive approach through analysis of metadata, system activity logs, and digital forensic examination.

In addition to authenticity, the integrity of electronic data is also a critical issue. Integrity ensures that electronic information has not been altered from the time it was first created until it is presented in court. Even the slightest change to the content, creation date, storage location, or metadata can affect the probative value of an electronic document. Unfortunately, in the practice of the Indonesian criminal justice system, there is currently no standardized mechanism requiring law enforcement officials to verify the integrity of electronic evidence before it is used as the basis for proof in court. Another issue of equal importance is the chain of custody for digital evidence. In the field of digital forensics, the chain of custody is a procedure that ensures electronic evidence from the moment it is discovered, seized, and analyzed through to its presentation in court remains under continuous, documented supervision. This documentation is crucial for preventing any manipulation or alteration of the electronic evidence. However, the handling of digital evidence in Indonesia still lacks uniform operational standards, which leaves room for doubts regarding the validity of electronic evidence.

In addition, advancements in cloud computing, end-to-end encryption, and cross-border data storage present new challenges in the evidentiary process. Much electronic information is no longer stored locally on users' devices but resides on servers located in the jurisdictions of other countries. This situation raises issues regarding the authority of law enforcement officials to obtain electronic evidence, as well as the mechanisms for international cooperation to obtain the data necessary for investigations and the presentation of evidence in court. From a human rights protection perspective, the use of electronic evidence must also respect the right to privacy and the protection of personal data. The collection of electronic information without a clear legal basis has the potential to violate citizens' constitutional rights. Therefore, the process of obtaining electronic evidence must adhere to the principles of due process of law, necessity, proportionality, and accountability to prevent the abuse of authority by law enforcement agencies.

In the context of evidence, this issue demonstrates that the admissibility of electronic evidence cannot be based solely on the existence of the electronic document itself, but must also consider the processes of its acquisition, preservation, analysis, and presentation in court. In other words, the probative value of electronic evidence stems from the entire process that ensures the authenticity, integrity, and reliability of the electronic data. When analyzed using Lawrence M. Friedman's legal systems theory, the issue of electronic evidence is not only caused by weaknesses in legal substance but is also influenced by legal structure and legal culture. From a substantive perspective, there is still no harmonization between the Criminal Procedure Code (KUHAP) and the Information and Electronic Transactions Law (ITE Law) regarding standards for electronic evidence . From a structural perspective, the capacity of law

enforcement officials to handle digital evidence remains inconsistent. Meanwhile, from a legal culture perspective, both the public's and officials' understanding of the characteristics of electronic evidence is still evolving; consequently, a uniform practice for assessing the probative value of digital evidence has not yet been established.

Based on these various issues, it can be concluded that the system for admitting electronic evidence in Indonesia still faces normative, technical, and institutional challenges. The recognition of electronic evidence as admissible evidence does not automatically guarantee legal certainty if it is not accompanied by clear standards of proof that can be consistently applied. Therefore, a reconstruction model is needed that can integrate the principles of authenticity, integrity, chain of custody, reliability of electronic systems, and digital forensic verification as the basis for assessing the probative value of electronic evidence within Indonesia's criminal justice system.

Reconstructing the Evidentiary Weight of Electronic Evidence from a Cyberlaw Perspective

Advances in information technology have transformed the nature of evidence in the criminal justice system. Evidence, which was once dominated by physical documents, has now shifted to electronic information stored in various digital devices and electronic systems. This change demands a transformation of the criminal evidentiary system to accommodate the characteristics of electronic evidence, which differ from those of conventional evidence. Therefore, the recognition of electronic evidence as admissible evidence, as stipulated in the Law on Information and Electronic Transactions, must be accompanied by a reconstruction of the standards for assessing its probative value.

The reconstruction referred to in this study does not mean changing the status of electronic evidence as admissible evidence, but rather establishing an assessment framework that can be used by judges and law enforcement officials in determining the probative value of electronic evidence. This framework is necessary because, to date, there are no normative parameters governing the indicators that must be met for electronic evidence to be assessed as having optimal probative value. From a cyberlaw perspective, electronic evidence is not merely viewed as a digital document but is part of an electronic system with specific technical characteristics. Therefore, the assessment of electronic evidence must take into account both legal and information technology aspects. This approach aligns with developments in cyberlaw, which regard technology as an integral part of the law enforcement process.

Based on an analysis of various regulations, legal doctrines, and judicial practices, this study proposes a Model for Reconstructing the Probative Value of Electronic Evidence consisting of five key indicators:

1. Authenticity

Authenticity is the first requirement that every piece of electronic evidence must meet. The judge must be convinced that the electronic document truly originates from a legitimate source and was not created by an unauthorized party. Authenticity can be verified through account identification, IP addresses, metadata, electronic signatures,

or digital forensic examination. Thus, authenticity is not based solely on the parties' acknowledgment but is also scientifically proven through a digital verification process.

2. Integrity (Data Integrity)

The second indicator is the integrity of electronic data. It must be ensured that electronic information has not been altered from the time it was first created until it is submitted as evidence in court. Integrity can be proven through the examination of hash values, metadata, system activity logs, or other security mechanisms that guarantee the document's content has not been modified. Without a guarantee of integrity, an electronic document risks losing its evidentiary value because it no longer reflects the actual circumstances.

3. Reliability (Reliability of the Electronic System)

This study argues that the assessment of electronic evidence should not focus solely on the document itself but must also consider the electronic system that generated it. An electronic system that meets information security standards, has an audit trail mechanism, and implements adequate security procedures will produce more reliable electronic information. Therefore, the reliability of the electronic system is a key indicator in determining the probative value of electronic evidence.

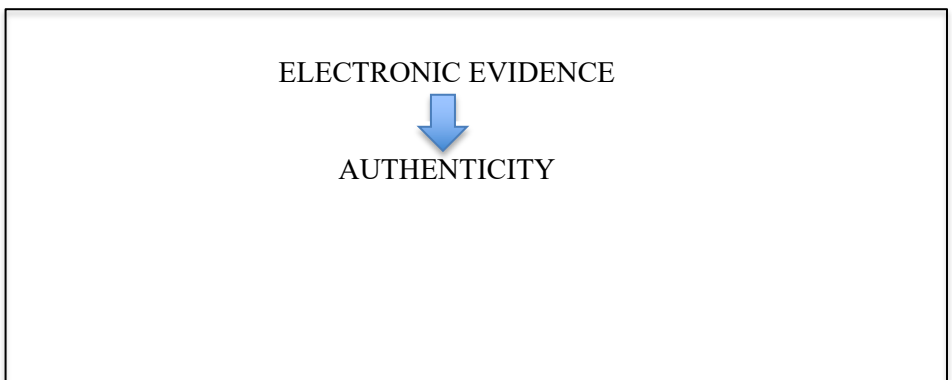
4. Chain of Custody (Chain of Custody for Digital Evidence)

The validity of electronic evidence is also determined by the existence of clear documentation regarding the process of seizure, storage, examination, and presentation of the evidence in court. Every transfer of digital evidence must be fully documented to ensure that no manipulation or alteration of the electronic data occurs. This study proposes that the concept of the chain of custody be regulated in greater detail in criminal procedure law as a formal requirement for the admissibility of electronic evidence.

5. Digital Forensic Verification

The final indicator is digital forensic verification. In cases involving highly complex electronic evidence, digital forensic examination serves as a crucial tool for ensuring the authenticity, integrity, and reliability of the evidence. Therefore, the findings of digital forensic experts should be given a more strategic role in the evidentiary process, particularly when there are objections regarding the authenticity of electronic documents.

These five indicators form an interconnected assessment system. It is not sufficient for electronic evidence to meet just one indicator; it must satisfy all indicators for to possess high probative value. Thus, judges no longer merely assess the existence of electronic documents but also evaluate the processes of creation, storage, security, and verification of those documents.



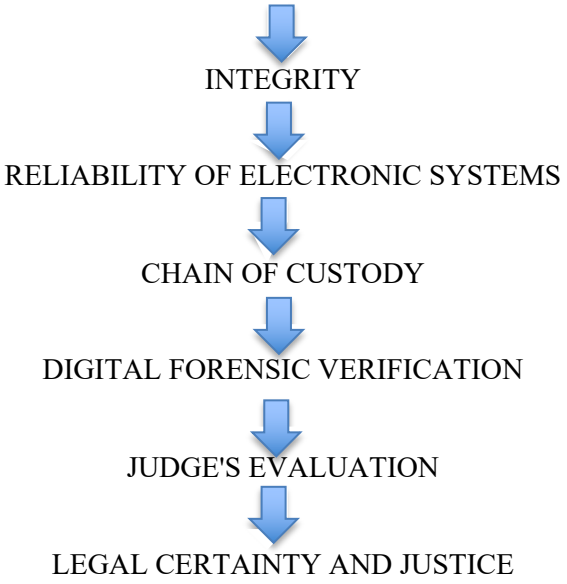


Fig 1. Model for Reconstructing the Evidentiary Weight of Electronic Evidence

This model demonstrates that the probative value of electronic evidence is not determined by the mere existence of an electronic document, but rather by the fulfillment of all indicators that constitute an electronic evidentiary chain. The more indicators that are met, the higher the level of confidence in that evidence. This reconstruction also has implications for the reform of Indonesia's criminal procedure law. Lawmakers need to incorporate electronic evidentiary standards into the new Criminal Procedure Code so that it no longer merely recognizes electronic evidence as admissible evidence but also regulates the mechanisms for its evaluation in greater detail. Thus, judges will have more objective guidelines for assessing the probative value of electronic evidence, thereby minimizing disparities in rulings and enhancing legal certainty.

Implications of Reconstructing the Probative Value of Electronic Evidence for the Reform of Indonesian Criminal Procedure Law

The digital transformation occurring across various aspects of society has led to changes in the nature of evidence within the criminal justice system. Crimes that exploit information technology no longer rely on conventional evidence but are dominated by electronic information, electronic documents, digital data, communications via instant messaging apps, electronic transactions, and digital footprints. These conditions necessitate an update to the criminal evidentiary system that not only recognizes the existence of electronic evidence but also establishes objective and legally accountable standards for its evaluation.

The results of this study indicate that the main issue does not lie in the recognition of electronic evidence as admissible evidence, but rather in the absence of normative standards regarding how to assess the probative value of electronic evidence. Consequently, judicial practice still exhibits variations in the assessment of digital evidence, particularly that derived from electronic conversations, social media,

emails, or documents stored in cloud computing systems. Such variations have the potential to lead to inconsistent rulings, reduce legal certainty, and create room for disparities in the treatment of cases with similar characteristics. From the perspective of legal reform, the reconstruction proposed in this study has several important implications:

1. Harmonization of Regulations between the Criminal Procedure Code and the ITE Law

Reforms to criminal procedure law should focus on harmonizing the Criminal Procedure Code (KUHAP) with Law No. 1 of 2024 on the Second Amendment to the Law on Information and Electronic Transactions. To date, regulations concerning electronic evidence have been scattered across various statutes, preventing the formation of a unified evidentiary system. Therefore, the revision of the Criminal Procedure Code must adopt provisions that explicitly regulate the definition, classification, procedures for obtaining, examining, storing, and evaluating electronic evidence.

2. Development of National Standards for Digital Evidence

This study proposes that the Supreme Court, the Attorney General's Office of the Republic of Indonesia, the National Police of the Republic of Indonesia, and relevant agencies develop national guidelines on digital evidence. These guidelines could cover procedures for examining electronic evidence, methods for documenting the chain of custody, standards for digital forensic examination, and mechanisms for presenting electronic evidence in court. The existence of uniform guidelines will reduce disparities in practices among law enforcement officials while improving the quality of the evidentiary process.38

3. Strengthening the Role of Digital Forensics in the Evidence-Presentation Process

Technological advancements have made it increasingly easy to manipulate electronic data using various software tools. Therefore, this study positions digital forensic verification as a critical element in the evidentiary process for electronic-based criminal cases. Digital forensic examination not only serves to ensure the authenticity of electronic documents but also provides a scientific basis for judges in forming their convictions. Thus, the use of digital forensic experts is no longer viewed as supplementary but as an integral part of the evidentiary process regarding electronic evidence.

4. Capacity Building for Law Enforcement Officials

The restructuring of the electronic evidence system also requires an enhancement of law enforcement officials competencies. Judges, prosecutors, investigators, and legal counsel must possess an adequate understanding of the characteristics of digital evidence, information security principles, metadata, hash values, the chain of custody, and digital forensic examination techniques. Without such capacity building, even well designed regulations will be unable to effectively provide legal certainty.

5. Strengthening the Protection of Human Rights in Digital Evidence

Reforms to criminal procedure law must continue to prioritize the protection of human rights as a fundamental principle. The use of electronic evidence must not disregard the right to privacy, the protection of personal data, or the principle of due process of law. Therefore, every process including the collection, seizure, analysis, and use of electronic information as evidence must be conducted based on lawful authority, adhere to the principle of proportionality, and be legally accountable.

From the perspective of the theory of legal certainty proposed by Gustav Radbruch, the law must not only provide certainty but also realize justice and utility. The reconstruction of the evidentiary weight of electronic evidence proposed in this study is an effort to balance these three fundamental values. Legal certainty is realized through clear evaluation standards; justice is realized through objective evaluation of evidence based on scientific verification; and utility is realized through the creation of an evidentiary system that is adaptive to developments in information technology.

Thus, the reconstruction of the evidentiary system for electronic evidence is not merely a technical necessity in the evidentiary process but also forms part of the national legal reform toward a modern, responsive criminal justice system oriented toward the protection of the constitutional rights of every citizen. It is hoped that the implementation of the reconstruction model proposed in this study will serve as a conceptual foundation for lawmakers in drafting criminal procedural law that is more adaptable to developments in digital technology while simultaneously strengthening the integrity of Indonesia's criminal justice system.

Based on the research findings, it can be concluded that regulations regarding electronic evidence in Indonesia's criminal justice system have been established through Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions. However, these regulations have not yet fully established normative standards for assessing the probative value of electronic evidence. The Criminal Procedure Code (KUHAP) remains oriented toward the conventional system of evidence and thus has not yet accommodated the specific characteristics of electronic evidence, which require proof of authenticity, integrity, and reliability of the electronic system, as well as the process of obtaining digital evidence. As a result, discrepancies in the evaluation of electronic evidence are still found in judicial practice, which has the potential to create legal uncertainty.

This study proposes a Model for Reconstructing the Evidentiary Weight of Electronic Evidence as a conceptual contribution to the development of evidence law in Indonesia. The model identifies five key indicators, such as authenticity, integrity, reliability of electronic systems, chain of custody, and digital forensic verification as parameters that must be met before electronic evidence is deemed to possess optimal evidentiary weight. The application of this model is expected to enhance the objectivity of judicial assessments, strengthen the protection of human rights, reduce disparities in rulings, and support the creation of legal certainty within the criminal justice system in the digital age.

In line with developments in information technology, updates to criminal

procedure law should focus on harmonizing the Criminal Procedure Code (KUHAP) with the Law on Information and Electronic Transactions by establishing more comprehensive regulations regarding the mechanisms for obtaining, examining, storing, verifying, and evaluating electronic evidence. In addition, it is necessary to develop national guidelines on digital evidence involving the Supreme Court, the Indonesian National Police, the Attorney General's Office of the Republic of Indonesia, academics, and digital forensics practitioners. This reform is expected to create an evidence system that is adaptive to technological developments while striking a balance between legal certainty, justice, and effectiveness in the enforcement of criminal law in Indonesia.

CONCLUSION

Based on the research findings, it can be concluded that regulations regarding electronic evidence in Indonesia's criminal justice system have been established through Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions. However, these regulations have not yet fully established normative standards for assessing the probative value of electronic evidence. The Criminal Procedure Code (KUHAP) remains oriented toward the conventional system of evidence and thus has not yet accommodated the specific characteristics of electronic evidence, which require proof of authenticity, integrity, and reliability of the electronic system, as well as the process of obtaining digital evidence. As a result, discrepancies in the evaluation of electronic evidence are still found in judicial practice, which has the potential to create legal uncertainty.

This study proposes a Model for Reconstructing the Evidentiary Weight of Electronic Evidence as a conceptual contribution to the development of evidence law in Indonesia. The model identifies five key indicators, such as authenticity, integrity, reliability of electronic systems, chain of custody, and digital forensic verification as parameters that must be met before electronic evidence is deemed to possess optimal evidentiary weight. The application of this model is expected to enhance the objectivity of judicial assessments, strengthen the protection of human rights, reduce disparities in rulings, and support the establishment of legal certainty within the criminal justice system in the digital age.

In line with developments in information technology, updates to criminal procedure law should focus on harmonizing the Criminal Procedure Code (KUHAP) with the Law on Information and Electronic Transactions by establishing more comprehensive regulations regarding the mechanisms for obtaining, examining, storing, verifying, and evaluating electronic evidence. In addition, it is necessary to develop national guidelines on digital evidence involving the Supreme Court, the Indonesian National Police, the Attorney General's Office of the Republic of Indonesia,

academics, and digital forensics practitioners. This reform is expected to create an evidence system that is adaptive to technological developments while striking a balance between legal certainty, justice, and effectiveness in the enforcement of criminal law in Indonesia.

REFERENCES

Books

Arief, B. N. (2017). Kapita selekta hukum pidana. Citra Aditya Bakti.

Friedman, L. M. (1975). The legal system: A social science perspective. Russell Sage Foundation.

Hamzah, A. (2019). Hukum acara pidana Indonesia. Sinar Grafika.

Harahap, M. Y. (2016). Pembahasan permasalahan dan penerapan KUHAP (Ed. rev.). Sinar Grafika.

Kelsen, H. (1967). Pure theory of law. University of California Press.

Makarim, E. (2013). Pengantar hukum telematika. RajaGrafindo Persada.

Makarim, E. (2016). Kompilasi hukum telematika. RajaGrafindo Persada.

Pound, R. (1954). An introduction to the philosophy of law. Yale University Press.

Radbruch, G. (1950). Legal philosophy. Harvard University Press.

Sjahdeini, S. R. (2009). Kejahatan dan tindak pidana komputer. Grafiti.

Constitution

Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.