Vol. 7, No. 11, November 2026. pp. 4184-4196
E-ISSN:2723 – 6692
P-ISSN:2723– 6595
https://doi.org/10.59141/jiss.v7i11.2613

Criminal Law Development in the Digital Era: Reconstruction of the Electronic Evidence Assessment System and Strengthening the Role of the Prosecutor's Office in Realizing Accountable Justice

Kuo Bratakusuma
Universitas Sumatera Utara, Indonesia
Email : kuobrata@gmail.com

Keywords:
Law and Development; Electronic Evidence; Prosecutor's Office; Prosecution; Criminal Code; Criminal Proof;

This is an open access article under the CC BY-SA license.

Copyright © 2026 by Author. Published by Publikasi Indonesia

Abstract

The increasing use of electronic evidence in Indonesian criminal proceedings has revealed significant gaps in the procedures used by investigators, prosecutors, and judges to assess its authenticity, integrity, and reliability. This study examined these deficiencies, evaluated the role of the Indonesian Prosecutor's Office in ensuring evidentiary quality, and proposed a structured, multistage framework for assessing electronic evidence. The study employed evaluative and prescriptive normative legal research methods, integrating statutory and conceptual approaches with illustrative analyses of selected judicial decisions. The findings identified a discrepancy between the formal legal recognition of electronic evidence and the operational standards required to determine its admissibility and probative value. The proposed assessment framework began with an examination of the legality of evidence acquisition and authentication, followed by evaluations of data integrity, technical reliability, relevance, corroboration, coherence with other evidence, and probative weight. The final stage considered whether the evidence, assessed within the applicable legal framework and in conjunction with other admissible evidence, could support the judicial conviction required for a criminal finding of guilt. Within this framework, investigators were responsible for securing, preserving, and documenting electronic evidence; prosecutors were tasked with reviewing case files, identifying evidentiary deficiencies, and coordinating with investigators to ensure evidentiary completeness; and judges retained independent authority to evaluate the legality, authenticity, credibility, and probative weight of the evidence presented at trial. The study concluded that standardized national guidelines governing the chain of custody, digital forensic documentation, procedural opportunities for the defense to challenge electronic evidence, and reasoned judicial assessment, supported by specialized training for prosecutors in interpreting digital forensic findings, could strengthen consistency in evidentiary practices throughout investigation, prosecution, and adjudication. These measures could enhance procedural fairness, legal certainty, transparency, and institutional accountability within Indonesia's criminal justice system.

INTRODUCTION

Legal development is inseparable from social, economic, and technological transformations. In an increasingly digitalized society, the relationship between law and development extends beyond the establishment of regulations supporting administrative modernization. The legal system must also define the limits of institutional authority, protect fundamental rights, provide fair mechanisms for dispute resolution, and ensure accountability in the state's use of technology (Singh, 2023). Accordingly, the effectiveness, fairness, and accountability of the criminal justice system serve as important indicators of the quality of legal development (Fauzia, 2019; Kusumaatmadja, 1976; Savitri et al., 2026).

The United Nations 2030 Agenda for Sustainable Development recognizes access to justice, the rule of law, and effective, accountable, and transparent institutions as essential components of Sustainable Development Goal (SDG) 16 (United Nations General Assembly, 2015). Target 16.3 emphasizes the promotion of the rule of law and equal access to justice, while Target 16.6 focuses on developing effective, accountable, and transparent institutions at all levels. Within the criminal justice system, achieving these targets requires more than expanding digital court infrastructure and electronic judicial services. It also necessitates strengthening the integrity and transparency of judicial decision-making. Fair and accountable judicial decisions depend on reliable and verifiable evidence, lawful procedures, and clearly articulated legal reasoning.

The digital transformation of Indonesia's criminal justice system, including the development of the Information Technology-Based Integrated Criminal Justice System (Sistem Peradilan Pidana Terpadu Berbasis Teknologi Informasi, SPPT-TI) and the Electronic Integrated Criminal Justice Administration (Elektronik Berkas Pidana Terpadu, e-Berpadu), demonstrates the increasing integration of technology into criminal case management. Concurrently, electronic evidence has become increasingly prominent in criminal proceedings, encompassing instant messaging records, emails, closed-circuit television (CCTV) recordings, electronic transaction records, metadata, and digital forensic examination results (Giri Santosa & Kamali, 2022; Reedy, 2023). Unlike conventional physical evidence, electronic data can be copied, transferred, modified, deleted, or reproduced without immediately apparent alterations. Furthermore, visually identical electronic records do not necessarily share the same origin, metadata, contextual information, or acquisition history. These characteristics create distinct evidentiary challenges concerning authentication, data integrity, reliability, and the preservation of digital evidence.

A significant development in Indonesia's criminal procedural law occurred with the enactment of Law No. 20 of 2025 concerning the Criminal Procedure Code (Kitab Undang-Undang Hukum Acara Pidana, KUHAP), which entered into force on January 2, 2026, replacing Law No. 8 of 1981. Article 235(1)(f) expressly recognizes electronic evidence as a category of admissible evidence in criminal proceedings. Article 235(3) requires evidence to be capable of authentication and to have been obtained lawfully, while Article 235(4) authorizes judges to assess its authenticity and the legality of its acquisition. Furthermore, Article 235(5) stipulates that evidence declared inauthentic and/or unlawfully obtained cannot be used as evidence during judicial proceedings and has no probative value. These provisions strengthen

the statutory recognition of electronic evidence while emphasizing judicial responsibility for evaluating evidentiary authenticity, lawful acquisition, and admissibility.

Nevertheless, formal statutory recognition does not automatically establish a comprehensive operational framework for assessing electronic evidence. Important challenges remain concerning the procedures required to authenticate digital records, preserve data integrity, evaluate the reliability of forensic acquisition and examination methods, maintain a verifiable chain of custody, and establish the relevance of technical findings to the elements of an alleged criminal offense (D'Anna et al., 2023; Rakha, 2024). Inconsistencies in evidentiary standards across investigation, prosecution, and judicial examination may result in different assessments of comparable electronic evidence without sufficiently articulated or objectively verifiable justifications. Such inconsistencies risk undermining legal certainty, procedural fairness, and the equal treatment of parties involved in criminal proceedings (Samudra et al., 2026).

The preliminary examination of selected judicial decisions underlying this study revealed variations in approaches to evaluating electronic evidence. Certain judgments emphasized digital forensic examinations as essential mechanisms for establishing the authenticity and integrity of electronic records. Others relied on screenshots, electronic recordings, or digital communications corroborated by witness testimony, defendants' statements, or additional evidence, without providing extensive explanations of technical verification procedures. In some cases, electronic evidence was presented during trial but received limited substantive consideration in the court's written reasoning. These variations did not necessarily indicate that particular judgments were legally correct or incorrect, as evidentiary requirements and judicial assessments depend on the facts and circumstances of individual cases. Nevertheless, they highlighted the importance of establishing consistent assessment parameters and requiring transparent, reasoned judicial explanations concerning the admissibility and probative weight of electronic evidence.

From the perspective of law and development, these challenges extend beyond technical digital forensic considerations and encompass broader issues of institutional governance, procedural coordination, and judicial accountability (Friedman, 1975; Kusumaatmadja, 1976). Legal modernization that focuses primarily on expanding legally recognized categories of evidence, without corresponding improvements in institutional capacity, interagency coordination, and accountability mechanisms, risks producing merely formal or procedural changes. Although technological advancements can accelerate information processing and facilitate access to electronic records, they do not necessarily improve the quality of justice. Substantive improvements require reliable mechanisms for verifying the origin, integrity, and relevance of electronic evidence, together with transparent judicial reasoning explaining how such evidence contributes to factual findings and legal conclusions.

Against this background, this study addressed three principal research questions: (1) how electronic evidence is positioned and assessed within the development of Indonesian criminal procedural law; (2) how the duties and statutory authority of the Indonesian Prosecutor's Office, particularly in coordinating with investigators, reviewing investigative case files, and conducting prosecutions, can strengthen the quality of electronic evidence assessment; and (3) how a structured, multistage assessment framework can integrate the respective responsibilities

of investigators, public prosecutors, and judges to promote accountable criminal justice. This study argued that the development of criminal procedural law in the digital era requires a transition from the formal recognition of electronic evidence toward an integrated system of evidentiary governance. Within this framework, the Prosecutor's Office occupies a strategic position in ensuring evidentiary completeness, procedural compliance, and continuity between investigation and trial, while preserving judicial independence in determining admissibility and probative weight. Such an approach is expected to strengthen legal certainty, procedural fairness, transparency, and institutional accountability within Indonesia's criminal justice system.

METHOD

This study employed an evaluative and prescriptive normative legal research approach. The statutory approach examined Law No. 20 of 2025 concerning the Criminal Procedure Code, Law No. 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law, and Law No. 16 of 2004 concerning the Prosecutor's Office of the Republic of Indonesia, as amended by Law No. 11 of 2021. The analysis focused on the legal recognition, admissibility, and assessment of electronic evidence; coordination between investigators and public prosecutors; prosecutorial review of investigation case files; prosecutorial authority; and the execution of criminal judgments. A conceptual approach was employed to examine the relationship between evidentiary law, legal theory, and legal development, while a case-based approach was used to analyze selected judicial decisions illustrating variations in the assessment of electronic evidence.

Primary legal materials consisted of relevant legislation, regulations, and selected judicial decisions, while secondary legal materials included scholarly books and journal articles addressing criminal evidence, digital forensics, judicial reasoning, and legal development. The collected materials were analyzed qualitatively through statutory interpretation, comparative examination of legal provisions, identification of normative and procedural gaps, and formulation of recommendations for improving electronic evidence assessment. The analysis of judicial decisions was based on case summaries available in the underlying research manuscript. Consequently, interpretations derived from these summaries were treated as illustrative and remained subject to verification against official court decisions and relevant procedural records.

RESULTS AND DISCUSSIONS

A shift in the problem: from confession to evaluation of the strength of the evidence

Article 235 of Law Number 20 of 2025 concerning the Criminal Procedure Code marks the explicit recognition of electronic evidence as evidence. This recognition is an advance in adapting criminal procedural law to the development of information technology. However, recognition as evidence does not mean that every digital information is automatically authentic, intact, reliable, relevant, or strong to prove a proposition. A distinction must be made between admissibility and probative value.

The Electronic Information and Transaction Law, especially Article 5 and Article 6, provides a basis for the recognition of electronic information and documents along with the requirements for access, display, guaranteed integrity, and accountability. These provisions need to be read systematically in conjunction with the new Criminal Procedure Code. The criminal procedure law regulates the evidentiary function in the judicial process, while the ITE regime provides a framework for the recognition and characteristics of electronic documents. The harmonization of the two must ensure that technical requirements are not treated as formalities and legal requirements are not reduced to mere device examinations.

Gap in the development of legal substance

Article 235 paragraphs (3) to (5) stipulate the principles of authentication and legality of acquisition, but its application requires more operational parameters. Authentication needs to answer whether the data comes from the claimed source; integrity answers whether the data has remained intact since it was obtained; reliability tests whether the devices, systems, and methods used are trustworthy; while the chain of custody describes the continuity of control and handling of evidence. Without guidelines that explain the relationship between these criteria, evaluation standards have the potential to develop non-uniformly.

The need for further regulation does not mean that all technical aspects must be incorporated into the law. Laws can establish basic principles and guarantees, while cross-agency technical guidelines can regulate procedures for documentation, acquisition, storage, handover, examination, and presentation of evidence. This division maintains flexibility in the face of technological changes without sacrificing legal certainty and supervision.

Gaps in institutional structure and evidence governance

Electronic evidence moves across the stages of discovery, security, confiscation, acquisition, examination, storage, submission to the Public Prosecutor, and presentation in court. Each institution has its own authority and procedures. Within the framework of the 2025 Criminal Procedure Code, coordination between Investigators and Public Prosecutors is no longer solely understood as communication after the investigation is completed. Articles 58 to 63 place coordination as part of case handling in an integrated criminal justice system, starting from the notification of the start of the investigation, can be done through information technology, must be documented in the minutes, and include research on formal and material aspects of the case file. This arrangement provides a basis for the Public Prosecutor to be involved early in ensuring that the electronic evidence collected by the Investigator can be accounted for when the case is submitted to the court.

From the point of view of institutional development, the main need is procedural interoperability, not just application interoperability. The integration of the case information system must be accompanied by metadata standards, documentation forms, access logging, handover procedures, forensic copy security, and mechanisms to test and uncover changes to data. Each institution needs to know its responsibilities and provide documentation that can be traced by subsequent institutions or tested by the defense.

Duties and Authorities of the Prosecutor's Office in Ensuring the Quality of Electronic Evidence

The role of the Prosecutor's Office in the electronic evidence system needs to be understood through two layers of authority. First, the general authority of the Prosecutor's

Office in the criminal field is based on Law Number 16 of 2004 as amended by Law Number 11 of 2021, including conducting prosecutions, carrying out the determination of judges and court decisions that have permanent legal force, conducting investigations into certain criminal acts based on the law, and completing certain case files through additional examinations coordinated with investigators. Second, the authority of the Public Prosecutor in the 2025 Criminal Procedure Code includes receiving and examining case files, coordinating to complete the results of investigations, making indictments, delegating cases, and prosecuting. These two layers of authority must be read according to their respective limits and legal basis; does not mean that every Prosecutor has the general authority to take over all investigative actions or conduct their own digital forensic examinations.

The first strategic point lies in coordination from the beginning of the investigation. Articles 58 and 59 of Law Number 20 of 2025 concerning the Criminal Procedure Code require the handling of cases by involving the Public Prosecutor through equal, complementary, and mutually supportive coordination. Coordination begins from the date of the notification of the start of the investigation, can use information technology facilities, and must be stated in the minutes of the event. For electronic evidence, the coordination can be directed to ensure from the beginning that the Investigator records the source of the data, the basis and method of acquisition, the identity of the device or account, the time of acquisition, the extraction method, the hash value if relevant, the party who controls and moves the evidence, and the location of the storage. Thus, the Public Prosecutor does not only know the weaknesses of the evidence when the file has been completed, but can identify the need for proof since the investigation process has taken place.

The second strategic point is in the research of the case file. Article 59 paragraph (6), Article 61, and Article 62 of Law Number 20 of 2025 concerning the Criminal Procedure Code place the Public Prosecutor's opinion on formal and material aspects, provide room for the return of the file with instructions to be completed, and regulate the title of the case if the results of the additional investigation are still incomplete. In the context of electronic evidence, it is not enough to just check the existence of the minutes or the list of evidence. The Public Prosecutor needs to assess whether the documents obtained and submitted are available, whether the identity of the evidence is consistent, whether the security and storage procedures can be traced, and whether access to the data has been documented. The material research needs to assess whether the data obtained is really related to the elements of the crime, whether the context of the conversation or transaction is intact, whether the user's identity can be linked to the defendant through supporting evidence, and whether the expert report explains the methods and limitations of the examination.

The authority to provide instructions to complete the results of the investigation must be used in a targeted and proportionate manner. If there are authentication gaps, the Public Prosecutor may request clarification of the source of the data or the relevant expert examination. If there is an ambiguity of integrity, the lead may be directed to the acquisition documentation, the examination of forensic copies, or the explanation of the hash value according to the character of the evidence. If the chain of custody is incomplete, the investigator needs to be asked to explain the transfer, access, and storage of evidence. The instruction is not an

instruction for the expert to come to a specific conclusion, but rather an effort to ensure that the methods and results of the examination can be tested objectively. The prosecutor should also not assume that technical deficiencies can always be corrected; some deficiencies may not be recoverable and must be assessed for their impact on the feasibility or weight of evidence.

The third strategic point is the preparation of the indictment and the prosecution strategy. Articles 65 and 70 of Law Number 20 of 2025 concerning the Criminal Procedure Code give the Public Prosecutor the authority to make an indictment and file a case with the court if the results of the investigation are deemed prosecutable. In cases that rely on electronic evidence, the Prosecutor needs to establish a clear relationship between the digital data, its source, the person suspected of operating or controlling it, the time and context of the event, and the elements of the criminal act charged. Electronic evidence should not be treated as an object that speaks for itself. For example, a screenshot of a conversation has not by itself proven who typed the message, whether the conversation was complete, or whether the content of the message is contextual. Therefore, the Public Prosecutor needs to connect it to the original device, witness statements, metadata, expert examination results, transaction records, or other relevant evidence.

In the trial, the Prosecutor's Office is responsible for presenting evidence that supports the indictment in an honest and testable manner. The Public Prosecutor can present experts and witnesses, explain the process of obtaining evidence, and test evidence submitted by other parties in accordance with procedural law. However, the authority to assess the authenticity and validity of the acquisition of evidence remains with the Judge as per Article 235 paragraph (4) of the Criminal Code. The position of the Public Prosecutor does not replace the function of the Judge, but rather helps to present sufficient factual and technical basis so that the judge's assessment can be carried out rationally. The integrity of the prosecution also requires the Prosecutor not to hide material weaknesses of evidence or convey forensic conclusions beyond what can really be supported by the examination method.

It is also necessary to distinguish between the prosecutor's authority and the prosecutor's investigative authority. The Prosecutor's Law gives the Prosecutor's Office the authority to investigate certain criminal acts based on the law, so that in cases that fall within this scope, the Prosecutor's Office can act in the capacity of the Investigator in accordance with its special legal basis. Outside the scope of the special investigation, the Public Prosecutor's main role in the investigation results of other institutions is coordination, file research, provision of complementary instructions, prosecution, and implementation of the verdict. This distinction is important so that the strengthening of the role of the Prosecutor's Office is not interpreted as an expansion of authority without a legal basis.

The authority of the Prosecutor's Office in the field of asset recovery also has limited but important relevance to electronic evidence. Article 30A of the Prosecutor's Law gives the authority to search, confiscate, and return assets resulting from criminal acts and other assets to the state, victims, or legitimate parties. In economic cases, corruption, money laundering, or crimes based on digital transactions, account information, transaction records, electronic wallets, asset ownership data, and traces of fund transfers can be part of the proof as well as asset traces. The use of such data must still be subject to the basis of authority, lawful acquisition procedures, authentication, and protection of the rights of related parties.

From a legal and development perspective, strengthening the Prosecutor's Office should be directed at building evidence-based prosecution capacity, not institutional dominance. The Prosecutor's Office needs to have prosecutors who understand the basics of digital forensics, documentation standards, limitations of extraction methods, and evidentiary reasoning. On the other hand, there needs to be a joint working protocol with the police and forensic laboratories regarding the format of the minutes, minimum metadata, handover procedures, copy security, and procedures for requesting additional examinations. The protocol should allow the defense to examine evidence effectively and still maintain the independence of the Judge in determining the evidentiary value.

The Impact of the Role of the Prosecutor's Office on the Tiered and Coherent Assessment Model

The Tiered and Coherent Electronic Evidence Assessment Model consisting of legality, authentication, integrity, reliability, relevance, correlation, coherence, probative power, and Judge's conviction can serve as a conceptual framework for policy harmonization. This model integrates the responsibilities of the Investigator, Public Prosecutor, and Judge: The Investigator secures and documents evidence; The Public Prosecutor examines the adequacy of the results of the investigation and establishes fair evidence; The Judge determines the probative value and his conviction based on valid evidence. This model does not replace the Judge's independence or assign mathematical weight, but helps establish a consistent, transparent, and accountable standard of reason.

This role does not make the Prosecutor the final determinant of the power of proof. This model divides responsibilities functionally: The investigator is responsible for the search, security, and initial documentation of evidence according to his authority; The Public Prosecutor is responsible for assessing the adequacy of the results of the investigation for the interests of the prosecution, requesting legal completeness, and presenting evidence in a fair manner; while the judge assesses the authenticity, legality of the acquisition, the strength of the evidence, and the conviction based on the overall evidence at the trial. This division strengthens accountability without obscuring the principle of independence of judicial power.

Gap in legal culture and judicial reasoning

The assessment of electronic evidence requires adequate communication between technical knowledge and legal reasoning. A digital forensic report can explain the method of acquisition, metadata, hash value, and examination results, but the Judge must still assess the relevance of the findings to the alleged facts. Conversely, the Judge should not accept a technical claim simply because it is submitted by an expert without an opportunity for the parties to test their methods, assumptions, and limitations.

Wigmore’s (1937) theory of evidentiary inference helps map the relationship between evidence, the facts between, and the main facts. An account, phone number, or device location does not by itself prove the identity of the person operating it at any given time. There must be a chain of reasoning that explains the relationship between the data, the user, the time, the context, and the elements of the crime. Meanwhile, MacCormick’s (1978) idea of coherence demands that the reasoning of the verdict form a consistent and justifiable set of arguments.

Judges need to explain why a piece of evidence is believed, how it relates to other evidence, and why the conclusions drawn are stronger than the relevant alternative explanations.

The practice of judgments as an indication of the need for standards

The source manuscript identifies a number of decisions that show variations in the treatment of electronic evidence. The Palu District Court Decision Number 22/Pid.Sus/2024/PN Pal is said to show the use of WhatsApp conversations supported by forensic examination of the device. The Praya District Court Decision Number 126/Pid.B/2022/PN Pya describes the issue of screenshots that are considered not to meet the requirements for authenticity and integrity. The Penajam District Court Decision Number 4/Pid.B/2020/PN Pnj shows that the recognition or absence of rebuttals to the account and the content of the upload are also considered. Meanwhile, the South Jakarta District Court Decision Number 796/Pid.B/2022/PN Jkt.Sel and the Supreme Court Decision Number 813 K/Pid/2023 show the importance of tracing a series of sources of CCTV footage, recording devices, storage media, and the presentation process.

These examples need to be read carefully. It is inappropriate to conclude that forensic examinations are mandatory in every circumstance without considering the type of data, the nature of the dispute, the availability of original sources, and supporting evidence. Conversely, the absence of a rebuttal from the defendant does not necessarily resolve the entire authentication issue, especially if there are indications of manipulation or disputes regarding access and control of accounts. A more appropriate principle is the proportionality of the examination: the greater the dispute over the source, integrity, or method of acquisition, the stronger the need to conduct technical testing and provide judicial explanations.

Reconstruction of a tiered and coherent assessment model

To address these gaps, this article develops a Tiered and Coherent Electronic Evidence Assessment Model. This model does not set the weights of numbers that bind the Judge, but rather provides a sequence of questions and a standard of reasons to make the assessment more transparent and testable. The model consists of nine stages:

a) Legality. Assess whether evidence is obtained through lawful authority and procedures, taking into account the basis of the action, limits of authority, privacy protection, and rights of affected parties.
b) Authentication. Assessing whether the evidence is true from the claimed source. The examination may include the identity of the source, device or account, the context of creation, metadata, witness or expert testimony, and the relationship between the data obtained and the data submitted at trial.
c) Integrity. Assess whether the data is preserved from unexplained changes. Acquisition documentation, forensic copies, hash values, media security, and access records can be used according to the characteristics of the evidence.
d) Reliability. Assess whether the device, system, application, extraction method, and examination procedure are trustworthy. The examination also needs to uncover the limitations of the method and the possibility of errors.
e) Relevance. Assess the relationship between the evidence and the facts that must be proved, including the time, place, perpetrator, act, intention, or consequences according to the elements of the criminal act charged.

f) Correlations. Assess whether electronic evidence is supported or supports other evidence, such as witness statements, documents, physical evidence, transaction records, or other records. Correlation should not be understood as a repetition of information from the same source.
g) Coherence. Assess whether the overall evidence constitutes a rational, consistent, and able to answer contradictions or relevant alternative explanations.
h) Probate strength. Assesses the extent to which the evidence supports a particular factual proposition. This assessment considers the quality of the evidence, the strength of the inference, the context of the case, and the weaknesses that have not been resolved.
i) The Judge's Belief. Placing the Judge's belief as the result of reasoning on the whole of valid and tested evidence, not as an intuition that is independent of reason. The verdict needs to explain the relationship between the evidence and the facts and elements of the criminal act.

The flow of the model is: Legality → Authentication → Integrity → Reliability → Relevance → Correlation → Coherence → Probative Power → Conviction of the Judge. The legality and authentication stages serve as initial threshold checks, while the next stage assesses the quality, relationship, and carrying capacity of evidence. This model is tiered but not mechanical. If a stage is not met, the Judge needs to explain the consequences for the use or weight of evidence; not every administrative flaw should automatically produce the same conclusion without assessing its impact on the authenticity, integrity, fairness of process, and applicable legal provisions.

The model integrates three layers. The normative layer ensures the legality and suitability of the procedure. The technical layer ensures the source, integrity, and reliability of the data can be tested. The judicial layer ensures that evidence is linked to the facts through coherent reasoning. This synthesis is in line with Twining and Miers's (2010) thinking on the relationship between evidence, proof, and fact-finding; Wigmore (1937) on evidentiary inference; and MacCormick (1978) on the coherence and justification of legal decisions.

Policy implications for national legal development

First, the government, together with the Police, the Prosecutor's Office, and related agencies, need to develop national guidelines across institutions regarding the handling and assessment of electronic evidence. The guidelines must outline minimum standards for documentation, acquisition, storage, handover, authentication, and testing. The guidelines need to clearly regulate the coordination points of Investigators and Public Prosecutors from the beginning of the investigation, the format of instructions for completing files, and the technical consultation mechanism without compromising the independence of investigators and judges.

Second, it is necessary to increase institutional capacity and human resources, especially for investigators, prosecutors, judges, advocates, and digital forensic experts. Training for prosecutors needs to include assessing the completeness of formal and electronic evidence materials, understanding forensic reports, preparing evidence constructions, and the obligation to objectively disclose the limitations of evidence.

Third, it is necessary to establish a proportionate accountability and disclosure mechanism. Records of possession of evidence, access, copying, and examination must be

available to be tested in accordance with procedural law and legal information protection. The defendant and his or her legal counsel must obtain an effective opportunity to test the authenticity, integrity, and method of examination. This disclosure is not an obstacle to efficiency, but a condition for the legitimacy of proof.

Fourth, the update must pay attention to the capacity gap between regions. Not all law enforcement units have laboratories, equipment, and experts of the same quality. Therefore, the development of electronic evidence systems needs to be accompanied by reference laboratory services, expert assistance standards, examination financing, and fair access mechanisms. Without equitable capacity distribution, national standards risk only being met by regions or institutions with greater resources.

Fifth, implementation evaluation needs to be carried out periodically through measurable indicators, such as the completeness of the chain of custody documentation, the proportion of evidence that can be traced to the source, the availability of testing opportunities by the defense, the quality of the verdict consideration, and the consistency of the application of the guidelines. Indicators should not be directed to pursue the number of acceptance or rejection of evidence, but rather to measure the quality of the process and its accountability.

CONCLUSION

The development of criminal procedural law in the digital era requires a transition from the mere recognition of electronic evidence toward a comprehensive assessment framework that ensures evidentiary reliability, procedural fairness, and institutional accountability. Article 235 of Law No. 20 of 2025 concerning the Criminal Procedure Code (Kitab Undang-Undang Hukum Acara Pidana, KUHAP) expressly recognizes electronic evidence and establishes requirements concerning authentication and lawful acquisition. Furthermore, Articles 58–65 provide a statutory framework governing coordination between investigators and public prosecutors, the review of investigative case files, and prosecutorial responsibilities. These provisions provide a legal basis for strengthening the Prosecutor's Office's involvement in ensuring that electronic evidence presented at trial is supported by verifiable acquisition procedures, adequate documentation, and reliable methods of preservation and examination.

From a law and development perspective, deficiencies in electronic evidence assessment reflect the incomplete integration of legal substance, institutional structures, and legal culture within Indonesia's criminal justice system. The Prosecutor's Office occupies a strategic position in connecting the investigation and adjudication stages through procedural coordination, examination of the formal and substantive completeness of investigative case files, issuance of supplementary investigative instructions within its statutory authority, preparation of indictments, and conduct of prosecutions. Nevertheless, these responsibilities must be exercised within the limits established by criminal procedural law and must not encroach upon the judiciary's independent authority to determine the authenticity, admissibility, legality of acquisition, and probative weight of evidence.

The proposed Tiered and Coherent Electronic Evidence Assessment Model offers a conceptual framework comprising successive evaluations of lawful acquisition, authenticity, integrity, technical reliability, relevance, corroboration, coherence with other evidence, and probative weight, culminating in an assessment of whether the evidence supports the judicial conviction required under applicable criminal procedural law. The model does not replace judicial discretion, prescribe numerical evidentiary weights, or diminish judicial independence. Rather, it seeks to establish consistent, transparent, and legally reasoned standards for evaluating electronic evidence throughout criminal proceedings. Accordingly, reforming

electronic evidence assessment mechanisms could contribute to Sustainable Development Goal (SDG) 16, particularly Target 16.3 on the rule of law and equal access to justice and Target 16.6 on effective, accountable, and transparent institutions.

The government, in coordination with the Indonesian National Police, the Prosecutor's Office, and relevant judicial institutions, should develop harmonized national guidelines governing electronic evidence handling throughout investigation, prosecution, and adjudication. These guidelines should establish standardized procedures for documenting the chain of custody, authenticating electronic records, preserving data integrity, evaluating forensic reliability, and coordinating the completion of investigative case files. They should also safeguard meaningful opportunities for the defense to examine and challenge electronic evidence and promote reasoned judicial explanations concerning its admissibility and probative weight, consistent with judicial independence. Implementation should be supported by specialized training to strengthen prosecutors' ability to interpret, critically evaluate, and appropriately challenge digital forensic reports. Together, these measures could improve evidentiary consistency, procedural transparency, legal certainty, and institutional accountability within Indonesia's criminal justice system.

FUNDING

This research was conducted independently and self-financed by the authors. During the research process, no institution, organization, or external party provided financial support, either in the form of grants, sponsorships, or other forms of assistance.

CONFLICT OF INTEREST

The authors state that there is a conflict of interest in this study, which is related to the requirements for taking a diploma. The research and preparation of this manuscript is part of the academic obligations that must be fulfilled as a graduation requirement. However, these interests do not affect the objectivity of the research implementation, data analysis, or presentation of findings in this manuscript.

AUTHOR CONTRIBUTION

The author plays a role in all stages of research and preparation of this manuscript, starting from the development of ideas, the implementation of analysis, to the writing and refinement of the manuscript. The entire content of the manuscript is the responsibility of the author.

GENERATIVE ARTIFICIAL INTELLIGENCE USAGE STATEMENT

In the preparation of this manuscript, the authors make limited use of artificial intelligence (AI) technology. The use is only intended to help improve grammar and check the accuracy of the use of language. All ideas, analysis, and substance of the content of the manuscript are entirely the result of the authors' thoughts and responsibilities.

REFERENCES

D'Anna, T., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The chain of custody in the era of modern forensics: From the classic procedures for gathering evidence to the new challenges related to digital data. *Healthcare, 11*(5), Article 634. https://doi.org/10.3390/healthcare11050634

Fauzia, I. (2019). Indonesia in legal doctrine and development. *Ash-Sharia, 19*(2), 197–206. https://doi.org/10.15575/as.v19i2.4358

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

Giri Santosa, D. G., & Kamali, K. M. I. (2022). Acquisition and presentation of digital evidence in criminal trial in Indonesia. *Jurnal Hukum dan Peradilan, 11*(2), 195–218. https://doi.org/10.25216/jhp.11.2.2022.195-218

Kusumaatmadja, M. (1976). *Hukum, masyarakat, dan pembinaan hukum nasional* [Law, society, and national legal development]. Binacipta.

Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions [Undang-Undang Nomor 1 Tahun 2024]. (2024).

Law No. 16 of 2004 on the Prosecutor's Office of the Republic of Indonesia, as amended by Law No. 11 of 2021 [Undang-Undang Nomor 16 Tahun 2004 jo. Undang-Undang Nomor 11 Tahun 2021]. (2004/2021).

Law No. 20 of 2025 on the Criminal Procedure Code [Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana]. (2025).

MacCormick, N. (1978). *Legal reasoning and legal theory*. Clarendon Press.

Palu District Court Decision No. 22/Pid.Sus/2024/PN Pal. (2024).

Penajam District Court Decision No. 4/Pid.B/2020/PN Pnj. (2020).

Praya District Court Decision No. 126/Pid.B/2022/PN Pya. (2022).

Rakha, N. A. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review, 16*(2), 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy, 6*, Article 100313. https://doi.org/10.1016/j.fsisyn.2022.100313

Samudra, A. H., Basu, S., & Saenz Perez, C. (2026). Digital challenge, analogue mind-set: Assessing Indonesia's electronic criminal evidence framework. *Journal of Indonesian Legal Studies, 11*(1), 257–298. https://doi.org/10.15294/jils.v11i1.35378

Savitri, A. M., Murwadji, T., Lita, H. N., Putranto, R. D., & Tajudin, A. A. (2026). Mochtar Kusumaatmadja's legal development theory as an epistemological solution for Indonesian legal reform. *Journal of Law and Legal Reform, 7*(3), 1365–1400. https://doi.org/10.15294/jllr.v7i3.47279

Singh, B. (2023). Unleashing alternative dispute resolution (ADR) in resolving complex legal-technical issues arising in cyberspace lensing e-commerce and intellectual property: Proliferation of e-commerce digital economy. *Revista Brasileira de Alternative Dispute Resolution-Brazilian Journal of Alternative Dispute Resolution-RBADR, 5*(10), 81–105.

South Jakarta District Court Decision No. 796/Pid.B/2022/PN Jkt.Sel. (2022).

Supreme Court of the Republic of Indonesia Decision No. 813 K/Pid/2023. (2023).

Twining, W., & Miers, D. (2010). *How to do things with rules: A primer of interpretation* (5th ed.). Cambridge University Press.

United Nations General Assembly. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development* (A/RES/70/1).

Wigmore, J. H. (1937). *The science of judicial proof, as given by logic, psychology, and general experience, and illustrated in judicial trials* (3rd ed.). Little, Brown and Company.