American Journal of Open Research
Vol 5 (No 7), July, 2026
E-ISSN: 2834-7668

Issues Regarding The Validity of Electronic Evidence in The New Criminal Procedure Code

Dwinoven Lumban Tobing*, Irma Cahyaningtyas
Universitas Diponegoro, Indonesia
Email: dwinoven3@gmail.com*

Keywords:
Electronic Evidence; Legal Certainty; New CPC

Abstract

Rapid advances in information and communication technology have transformed the landscape of criminal evidence, making electronic evidence increasingly central to criminal proceedings. Indonesia's New Criminal Procedure Code (New CPC), enacted under Law Number 20 of 2025 and effective since January 2, 2026, formally recognizes electronic evidence yet provides limited procedural guidance. This study aims to analyze juridical problems concerning the validity of electronic evidence under the New CPC and assess its implications for legal certainty. The research employs normative legal research with statutory, conceptual, and comparative approaches, using secondary data analyzed qualitatively. Findings reveal four key issues: the absence of standardized authentication procedures, weaknesses in chain-of-custody mechanisms, disparities in judicial assessment, and unclear qualifications of digital forensic experts, all of which contribute to legal uncertainty and inconsistent judicial decisions. The study concludes that while the recognition of electronic evidence under the New CPC represents a major advancement, its effectiveness is limited by the absence of detailed technical regulations, requiring the urgent issuance of Supreme Court regulations to ensure uniform application and legal certainty. Strengthening procedural standards is essential to harmonize judicial practice and protect due process in digital-era criminal justice systems. This supports consistent evidentiary reliability across courts nationwide and reinforces the legal certainty framework needed.

INTRODUCTION

The rapid development of information and communication technology has brought fundamental changes in various aspects of human life, including the realm of criminal law (Amoo et al., 2024; Pallangyo, 2022; Tawil & Tarawneh, 2025; Wall, 2024). Crime no longer occurs only in physical space but has also penetrated the cyber realm with increasingly complex and sophisticated modus operandi. This phenomenon requires the criminal procedure law system to adapt quickly to ensure that law enforcement remains effective and fair in the digital era. The development of information technology has significantly altered the patterns and modus operandi of criminal acts, which increasingly involve electronic systems and digital data, thereby making electronic evidence an essential element in proving criminal cases.

Indonesia, as a state governed by law as mandated in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, has an obligation to ensure legal certainty for all its citizens (Achmad et al., 2026; Juanda, 2023; Phiau et al., 2025; Subhan et al., 2023). In

the context of criminal procedural law, legal certainty is reflected, among other things, in the clarity of norms regarding legal evidence, mechanisms for obtaining such evidence, and standards of admissibility at trial. Law No. 20 of 2025 concerning the Criminal Procedure Code (KUHAP Baru) updates Law No. 8 of 1981 concerning the Criminal Procedure Code (KUHAP Lama), particularly in relation to evidentiary rules. Under the old Criminal Procedure Code, there are five categories of evidence as stipulated in Article 184. Meanwhile, the New Criminal Procedure Code expands the categories of evidence to eight, as referred to in Article 235. The change includes the removal of one category of evidence, namely "instructions" (petunjuk), and the addition of four types of evidence, namely electronic evidence, judges' observations, and other materials that may be used for evidentiary purposes in court proceedings, provided they are obtained lawfully.

Indonesia's criminal evidentiary system under the former Criminal Procedure Code was based on a closed system of evidence (limitative evidentiary system), which strictly regulated five types of admissible legal evidence (Pribadi, 2018). This normative construction did not explicitly accommodate electronic evidence (Heniyatun et al., 2018). Based on Article 184 of the former Criminal Procedure Code, which did not specifically regulate electronic evidence, judges, within their discretionary authority, interpreted electronic evidence as an extension of documentary or circumstantial evidence, which remains valid evidence as stipulated in Article 5 paragraph (2) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) (Rahmad et al., 2022; Soroinda & Nasution, 2022). This provision affirms that electronic information and electronic documents constitute lawful evidence (Fitri, 2020). However, it is not accompanied by clear technical guidelines governing authentication procedures, integrity assurance, and electronic data security (Senajaya et al., 2026; Saputra et al., 2025). Such a condition creates significant legal uncertainty because the determination of the validity of electronic evidence depends heavily on individual judicial interpretation, without a standardized normative framework (Lubis & Purba, 2024; Hasanah et al., 2026).

Prior to the enactment of the New Criminal Procedure Code, regulatory gaps concerning electronic evidence were partially addressed through sectoral legislation, particularly the Electronic Information and Transactions Law (ITE Law), which recognizes electronic information and electronic documents as legal evidence. However, this recognition remains limited, as its application is predominantly confined to specific criminal offenses and is not supported by comprehensive technical regulations governing the examination and authentication of electronic evidence in court. This situation creates a form of regulatory dualism that has the potential to generate legal uncertainty for both law enforcement officials and defendants within the criminal justice process. Therefore, Indonesia's criminal evidentiary system requires fundamental reform, particularly regarding the regulation of electronic evidence, which was not explicitly accommodated in the former Criminal Procedure Code.

The Government and the House of Representatives of the Republic of Indonesia enacted the New Criminal Procedure Code on December 17, 2025, which came into effect on January 2, 2026. The New Criminal Procedure Code officially repeals and replaces the former Code. It expands the scope of evidence by explicitly strengthening the position of electronic evidence. This reinforcement is essential because modern crime is often

technology-based, with criminal acts increasingly conducted through social media, instant messaging applications, electronic transactions, and digital banking systems, making digital traces crucial evidentiary material. The New Criminal Procedure Code provides stronger legal legitimacy to electronic evidence, thereby reducing prolonged debates regarding its admissibility as valid evidence under Article 235 paragraph (1). Through this construction, the Code effectively codifies the exclusionary rule doctrine as a positive legal norm binding the entire criminal justice system.

The New Criminal Procedure Code introduces a paradigm shift in Indonesia's criminal evidentiary system from a closed system to an open system by recognizing eight categories of evidence under Article 235 paragraph (1), including electronic evidence and judges' observations, which were not previously recognized under the former Code. However, this shift is not unlimited; it is controlled through three sequential quality control mechanisms. First, the obligation of authentication and legality in obtaining evidence as stipulated in Article 235 paragraph (3). Second, judicial authority to assess compliance with these requirements under Article 235 paragraph (4). Third, the evidentiary sanction in the form of revocation of evidentiary value for evidence that does not meet the required standards, as stipulated in Article 235 paragraph (5).

The juridical recognition of electronic evidence in the New Criminal Procedure Code represents an important initial step but remains incomplete. Although normative legitimacy has been granted, the law does not provide an adequate procedural framework to uniformly measure and test the validity of electronic evidence, particularly regarding authentication mechanisms, data integrity, and verification of authenticity. As a result, the assessment of electronic evidence validity still relies heavily on judicial discretion. The absence of clear standards may generate interpretative debates and hinder the realization of legal certainty and the principle of due process of law. Moreover, the Code does not explicitly designate which technical regulations should serve as references for the acquisition, examination, and validation of electronic evidence.

The issue of electronic evidence validity is further complicated by its fundamentally different nature from conventional physical evidence. Electronic evidence is highly susceptible to alteration or loss and can be duplicated perfectly without leaving physical traces. In the absence of procedural rules that explicitly regulate technical standards for assessing electronic evidence, any such evidence presented at trial may be challenged, ultimately contributing to legal uncertainty in judicial proceedings. The New Criminal Procedure Code indirectly increases the burden on judges as guardians of evidentiary integrity in trials. Judges are required to assess not only relevance and probative value but also technical and procedural validity without clear normative guidance. This condition has the potential to create disparities in judicial decisions in substantively similar cases, solely due to differences in judicial interpretation and evaluation of electronic evidence. Such disparities not only undermine legal certainty but may also weaken public trust in Indonesia's criminal justice system.

Although the New Criminal Procedure Code marks progress by formally recognizing electronic evidence within the criminal evidentiary system, substantial normative gaps remain. This recognition has not been accompanied by sufficiently detailed regulatory instruments to ensure that the validity of electronic evidence can be assessed in a uniform,

measurable, and accountable manner. This gap gives rise to juridical issues with implications extending beyond technical dimensions. At a deeper level, it touches constitutional principles, particularly the guarantee of fair trial rights, the presumption of innocence, and the enforcement of due process of law as foundational elements of a rule-of-law state. Therefore, a systematic normative study of the validity of electronic evidence under the New Criminal Procedure Code has practical relevance for improving Indonesia's criminal justice system toward justice, utility, and legal certainty.

This study employs three legal theories as analytical frameworks. First, Gustav Radbruch's Theory of Legal Certainty, which asserts that law must reflect justice, utility, and legal certainty. Legal certainty requires clear, unambiguous, and consistently applied norms. In the context of electronic evidence, this theory is used to assess whether the New Criminal Procedure Code has clearly regulated standards of validity and authentication. Second, the Theory of Criminal Evidence, particularly the negative legal proof system (negatief wettelijk bewijsstelsel) adopted in the Criminal Procedure Code. Jan Remmelink states that judges are not absolutely free but remain bound by statutory evidentiary rules. This theory is used to evaluate whether the expansion of evidentiary categories in the New Criminal Procedure Code is accompanied by adequate evidentiary standards. Third, Friedrich Julius Stahl's Theory of the Rule of Law (Rechtsstaat), which emphasizes rule of law principles, human rights protection, and due process of law. Unclear standards regarding electronic evidence validity may conflict with these principles.

From the perspective of das sollen, Article 235 of the New Criminal Procedure Code recognizes electronic evidence as valid, requires authentication, and excludes unlawfully obtained evidence. However, the norm does not regulate technical standards for authentication, data integrity, chain of custody procedures, and qualifications of digital forensic experts. From the perspective of das sein, judicial practice shows that electronic evidence such as CCTV footage, digital messages, metadata, and location data is frequently used. However, due to the absence of standardized benchmarks, judicial assessment remains inconsistent and may result in sentencing disparities, creating a gap between normative provisions and practical application.

Previous national studies have been conducted by Puti Priyana et al. (2021) on electronic evidence in online fraud cases, Fransisca (2025) on evidentiary issues in the Criminal Procedure Code Bill, and Sacvio Fath Senajaya et al. on digital forensics in corruption cases. However, these studies have not specifically addressed the validity of electronic evidence following the enactment of the New Criminal Procedure Code. At the international level, Stephen Mason and Daniel Seng in the International Journal of Evidence & Proof (2017) emphasize the importance of authentication standards and chain-of-custody procedures in digital evidence. Additionally, Andrea Roth in the Harvard Journal of Law & Technology (2019) discusses challenges related to the reliability of algorithm-based digital evidence and fair trial guarantees.

The novelty of this research lies in three aspects. First, it is an initial study specifically examining the validity of electronic evidence under the New Criminal Procedure Code. Second, it employs legal certainty theory as an evaluative framework. Third, it offers recommendations for further regulatory development through PERMA or SEMA to ensure a more just, certain, and adaptive criminal evidentiary system in response to technological

advancement.

METHOD

The study used normative legal research, focusing on law as norms, principles, doctrines, and a system of rules used to address issues of norm gaps, conflicts, and ambiguity. The analysis focused on the regulation of electronic evidence under the New Criminal Procedure Code and its relevance to the principle of legal certainty.

The research employed statutory, conceptual, and comparative approaches. The statutory approach examined relevant legal instruments governing electronic evidence, including Law Number 20 of 2025 on the Criminal Procedure Code, Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, and other related regulations. The conceptual approach examined legal doctrines and theories, particularly legal certainty theory, criminal evidentiary theory, and the rule of law concept. The comparative approach was used to examine international practices on digital evidence, particularly regarding authentication standards and chain-of-custody procedures.

The study adopted a descriptive-analytical design, providing a systematic overview of the regulation of electronic evidence under the New Criminal Procedure Code and analyzing its normative adequacy and implications for legal certainty. It aimed not only to describe existing legal norms but also to critically evaluate their regulatory effectiveness.

The study relied on secondary data obtained through library research, consisting of primary, secondary, and tertiary legal materials. Primary legal materials included the 1945 Constitution of the Republic of Indonesia, the New Criminal Procedure Code, the former Criminal Procedure Code, the Electronic Information and Transactions Law, and relevant court decisions. Secondary legal materials included books, accredited national and international journal articles, research reports, and expert opinions. Tertiary legal materials included legal dictionaries, encyclopedias, and other supporting references.

Data collection was conducted through document analysis by identifying, inventorying, and reviewing relevant legal materials. The data were analyzed using qualitative methods, involving systematic interpretation and narrative description to draw conclusions on whether the regulation of electronic evidence under the New Criminal Procedure Code aligns with the principle of legal certainty.

RESULTS AND DISCUSSION

Juridical Problems of the Application of Electronic Evidence as Valid Evidence in the Criminal Justice Process

Absence of Standard Technical Standards for Authentication

Authentication is one of the most fundamental aspects in the process of proving electronic evidence in criminal trials. Conceptually, electronic evidence authentication encompasses two dimensions that are interrelated but substantially different. The first dimension is authentication in the formal sense, which is an assessment of the completeness and validity of the administrative documentation that accompanies the process of handling electronic evidence from the time it is found to be presented at trial. The second dimension is authentication in a material sense, which is an assessment of the authenticity of the content of

the electronic evidence itself to ensure that the data contained in it is not altered, falsified, or manipulated in any form.

In terms of formal authentication, there are several administrative documents that must be available to prove that an electronic evidence is obtained and handled in accordance with applicable legal procedures. First, the Seizure Minutes which contain a complete description of the confiscated electronic devices, the identity of the officer who carried out the confiscation, and the consent of the parties involved. Second, the Chain of Custody (CoC) document which records chronologically the entire movement and handling of electronic evidence, including a technical description of electronic devices including brands, model numbers, serial numbers, storage capacity, and all digital forensic activities carried out on the device. All documentation must be accompanied by validation in the form of a signature, both digital and written, a clear date listing, and an official stamp both digital and written. In addition, the documentation must explicitly include the source of the data, the identity of the owner of the data source, and the identity of the person who made the data acquisition.12 The Gospel of Jesus Christ

In terms of material authentication, there are three main conditions that must be met by electronic evidence in order to be declared valid to be used as a basis for proof at trial. The first condition is relevance, which requires that electronic evidence is substantially related to the criminal act charged and the defendant concerned. In practice, the relevance assessment includes verification that electronic evidence explicitly contains information that identifies the defendant, as well as that the date and time span contained in the electronic evidence are consistent with the temporal scope of the investigation or case being examined. In addition, it is necessary to ensure that the electronic evidence submitted is not related to the privacy of another party that is not relevant to the indictment The second condition is integrity, which requires that the electronic data submitted has not been altered, added, or deleted since it was first obtained. In practice, the fulfillment of integrity requirements is evidenced through a hash value mechanism that functions as a digital fingerprint to detect the presence or absence of data changes. The third condition is reliability, which requires that the process of obtaining and processing electronic evidence is carried out using methods that can be scientifically and legally accountable, and can be reproduced with consistent results if retested by different parties.

The three requirements for material authentication cannot be fulfilled optimally if they are not supported by standard and legally binding technical standards. This is where the most fundamental juridical problems lie in the regulation of electronic evidence in Indonesia. Article 235 paragraph (3) of the New Criminal Code does require the authentication of electronic evidence, but does not provide concrete technical parameters regarding how the authentication process should be carried out. The provision only states normative obligations without being accompanied by an operational mechanism that can be used as a uniform guideline for law enforcement officials and judges at trial.

Mason and Seng (2017) emphasized that in the context of digital evidence, authentication standards are at the core of the validity of an electronic evidence because without a clear authentication procedure, any electronic data submitted in court is vulnerable to legality attacks that lead to legal uncertainty. This view is relevant when it is associated with the conditions of the New Criminal Procedure Code which is normative in nature

without adequate technical details. In practice, this uniform standard of etiquette creates loopholes that can be exploited by certain parties to question the validity of electronic evidence solely based on differences in authentication methods used by investigators, even if the evidence is substantially valid.

By comparison, more mature legal systems such as the United States have regulated the obligation to authenticate electronic evidence in detail through Federal Rules of Evidence 901 (28 U.S.C.), which requires proof that electronic evidence is as claimed by the party submitting it, accompanied by a technical evidentiary procedure that can be cross-examined at trial. Similar provisions are not yet available to Indonesia in the New Criminal Procedure Code, thus creating a normative vacuum that has the potential to disrupt the consistency and certainty of the electronic evidence-based criminal proof process.

Weaknesses of Chain of Custody Procedures in Handling Electronic Evidence

The New Criminal Procedure Code introduces the principle of Chain of Custody (Coc) for evidence, which is the obligation to maintain the continuity of control and authenticity of evidence from confiscation to trial, in order to ensure the integrity of the evidence The existence of the CoC is a guarantee that the electronic evidence submitted at the trial is truly authentic and has not undergone changes or manipulation from the first time it was discovered until it was presented before the judge. Technically, the CoC is an official document that records chronologically and thoroughly each stage of handling electronic evidence, starting from the process of discovery, confiscation, preservation, analysis, to presentation at trial.

The substance contained in the CoC document includes various crucial information, including the initial condition and location of the evidence found, the technical description of the electronic device used as evidence, the results of the data integrity check, the forensic analysis procedures applied, and the identities of all experts involved in each stage of handling. In more detail, the CoC document at least contains the identity of the investigator who carried out the data acquisition, the license number or the legal basis for confiscating the device, the complete specifications of the electronic device including the brand, manufacturer, model, and unique code, the type of digital forensic equipment used, a record of every action taken against the device, and the digital signature of the acquisition and the results of the verification.

With the documentation of the entire series of evidence handling in an orderly and continuous manner, the CoC provides strong juridical protection for the evidentiary strength of electronic evidence. If the defendant questions the validity or authenticity of the electronic evidence submitted by the public prosecutor, the objection can be broken through the track record stored in the CoC. The function of the CoC in this case is not just administrative, but is an instrument of proof that directly confirms the integrity, authenticity, and legality of the acquisition of electronic evidence so that its validity can be legally accounted for before the court.

However, the recognition of the CoC principle in the New Criminal Code is still normative and has not been supported by a detailed technical mechanism. The New Criminal Procedure Code does not explicitly regulate the standard format of CoC documents, the recording procedures that must be taken, or strict legal sanctions if the CoC procedure is not fulfilled or violated. The absence of this standard poses a serious juridical risk, because

without clear guidance, each law enforcement institution has the potential to implement the CoC procedure differently according to their respective capacities and understandings. Such a condition not only creates a disparity in practice between one institution and another, but also opens a gap for the defendant to question the integrity of electronic evidence solely because of procedural inconsistencies that cannot be uniformly verified.

Disparity in Judges' Assessment of the Validity of Electronic Evidence

One of the factors that contributes to the weakness of electronic evidence-based evidence in criminal justice practice is the limited technical understanding of judges to the concept of digital forensics. In contrast to conventional evidence which is physical and relatively easy to verify with the naked eye, electronic evidence has much more complex characteristics. Its volatile nature, which cannot be verified without the help of special technical tools, and its dependence on the mastery of information technology make electronic evidence a type of evidence that requires its own competence from the law enforcers who handle it.

There are still judges who do not have an adequate understanding of how digital data is collected, stored, and analyzed, so excessive caution and even rejection of electronic evidence often occur solely because of the unclear source of data in their eyes. The limitation of technical competence also has an impact on the judge's inability to substantially evaluate digital forensic expert reports. In some cases, judges are not in a sufficient position to assess whether the digital examination procedures performed meet applicable scientific standards, so the decision to accept or reject electronic evidence is often based on purely subjective considerations, rather than on measured technical judgment. Most judges in the general courts still place physical evidence as the primary evidentiary instrument, while electronic evidence tends to be treated only as a secondary complement.

Various court decisions in Indonesia have significant differences in the way judges assess the validity of similar electronic evidence, ranging from CCTV recordings, screenshots of digital conversations, to banking transaction logs. Some judges require the validation of a digital forensic expert, while others simply accept the testimony of ordinary witnesses who acknowledge the authenticity of the evidence. Such differences in assessment standards directly sacrifice the principles of legal certainty and equality before the law.

In order to overcome these problems, a structured and continuous training program is needed for judges in connection with the enactment of the New Criminal Code which has recognized electronic evidence to include an understanding of the working mechanism of digital data, electronic evidence authentication procedures, and the application of chain of custody principles in the context of digital forensics. In addition, strengthening the integration of judicial institutions and digital forensic agencies is needed so that electronic evidence-based evidence can run consistently, objectively, and in line with applicable legal and technical standards.

Unclear Qualifications of Digital Forensic Experts

The rapid development of information technology has fundamentally changed the evidentiary landscape in criminal cases. Electronic devices are no longer just a means of communication, but have transformed into a rich source of evidence with digital information that can reveal the facts of the trial. In this context, digital forensics is present as an applied discipline that plays a role in tracing, recovering and analyzing data from electronic devices

in accordance with rules that can be legally accounted for. This field covers a wide spectrum of specialties, ranging from computer forensics, mobile forensics, audio forensics, video forensics, image forensics, to cyber forensics, each of which has different methodologies and analytical instruments. The breadth of this specialization confirms that not everyone can be immediately categorized as a competent digital forensic expert, so the regulation of qualifications and competency standards is an urgent legal need.

The method developed by the Digital Forensics Research Workshop (DFRWS) can be a relevant reference, especially in the aspect of maintenance and presentation of evidence which are the two critical points that determine the validity of electronic evidence in court from electronic evidence that through the procedure of confiscation and management of electronic evidence must be based on measurable digital forensic standards so that the strength of the evidence cannot be sued before the court. A much more crucial problem actually lies in the normative void in the New Criminal Code regarding the qualifications of digital forensic experts. The New Criminal Code does not expressly formulate the criteria for subjects who are fit to act as digital forensic experts at trial, does not establish the required educational or certification standards, and does not appoint an institution authorized to provide recognition of these competencies. One of the substantial obstacles to the use of electronic evidence in criminal justice stems from the lack of clarity in regulations regarding who actually has the authority and eligibility to examine and provide information on electronic evidence before the court. As a result, the expert testimony presented is easily questioned by the opponent, which ultimately has the potential to collapse the entire proof building that has been built by the public prosecutor.

This lack of regulation also has a direct impact on the quality of handling electronic evidence at the investigation level. Officials who have adequate digital forensic training are proven to be able to carry out all stages of evidence handling more systematically and accurately, from data acquisition to analysis using appropriate software. On the other hand, officials with minimal technical briefing tend to use inappropriate approaches in handling electronic evidence, which risks resulting in permanent data damage or loss. Such conditions not only harm the evidentiary process, but also have the potential to violate the rights of the defendant if the evidence that should have been mitigating is destroyed due to unprofessional handling. Therefore, it is necessary to improve the technical competence of law enforcement officials, including the establishment of binding qualification standards.

The use of digital forensic laboratories, interception technology, and teleconferencing mechanisms in criminal justice is growing and is beginning to gain wider acceptance in practice. However, this practical acceptance has not been balanced by the certainty of an adequate legal basis, so its legitimacy is still often debated. This has the potential to create new legal uncertainty that can harm all interested parties in the judicial process if technological advances in criminal justice are not accompanied by regulatory clarity regarding the qualifications and authority of experts.

Regulation of Electronic Evidence in the New Criminal Code in the Perspective of the Principle of Legal Certainty

The Principle of Legal Certainty as an Evaluative Parameter

Before evaluating the regulation of electronic evidence in the New Criminal Procedure Code, it is necessary to first understand conceptually what is meant by legal certainty as an

evaluative parameter in this study. Gustav Radbruch emphasized that good law must simultaneously fulfill three basic values, namely justice (Gerechtigkeit), utility (Zweckmäßigkeit), and legal certainty (Rechtssicherheit). In the context of this study, legal certainty is the main parameter used to measure the quality of electronic evidence regulation in the New Criminal Code.

Radbruch explained that legal certainty requires at least four things related to the meaning of legal certainty. First, that the law is positive, the meaning is legislation. Second, that the law is based on facts, not a formulation of the judgment that will later be made by the Judge. Third, that the fact must be formulated in a clear way so as to avoid errors in meaning, as well as to be carried out. Fourth, the positivity law must not change frequently. Lon L. Fuller through his work The Morality of Law perfected the idea of legal certainty by putting forward eight conditions for a legal system to have internal morality. These principles include: the rule of law must be generally applicable, published to the public, not retroactive, formulated clearly and easily understandable, not contradictory, not ordering something impossible to implement, have stability, and be applied consistently in accordance with the provisions that have been announced.

In the context of the regulation of electronic evidence, the two most important elements are the clarity of norms and the consistency of application. Clarity of norms is needed so that law enforcement officials, as well as litigants, can understand the requirements for the validity of electronic evidence with certainty. Meanwhile, consistency in application is needed so that there are no excessive differences in judgments between courts on the same type of evidence.

Based on the views of Gustav Radbruch and Fuller, the discussion of electronic evidence in the New Criminal Code can be tested through two basic questions. First, does the provisions in the New Criminal Code regulate electronic evidence in a clear, detailed, and easily identifiable manner by all parties in the criminal justice process? Second, can the rule be applied uniformly by judges at every level of the judiciary without causing disparities in verdicts that are detrimental to legal certainty? These two issues are the main focus of the next analysis. In line with that, Peter Mahmud Marzuki (2021) emphasized that legal certainty is not only determined by the existence of written rules, but also includes the firmness of the norm content material, clarity of implementation procedures, consistency of application, and ease of public access to these norms. These parameters are relevant to be used to assess whether the regulation of electronic evidence in the New Criminal Procedure Code has met the ideal standard of legal certainty. This measure will be used to evaluate whether the regulation of electronic evidence in the New Criminal Procedure Code has met the expected standards of legal certainty.

Normative Recognition of Electronic Evidence That Has Not Been Completed

The New Criminal Procedure Code, which was stipulated through Law Number 20 of 2025 and came into effect on January 2, 2026, marks a fundamental change in the criminal proof system in Indonesia. Through Article 235 paragraph (1), the lawmakers abandoned the closed proof model that had been adopted for decades by the previous Criminal Procedure Code, and then switched to a more open proof system by recognizing eight types of valid evidence, including electronic evidence. This change can be understood as a response to the need for judicial practice, considering that electronic evidence has long been used in handling

criminal cases even though it did not previously have a firm normative basis in the old Criminal Procedure Code.

Substantially, Article 235 of the New Criminal Code contains several important provisions regarding electronic evidence. Paragraph (1) places electronic evidence as one of the valid evidence in the trial. Paragraph (3) requires that every piece of evidence must be able to prove its authenticity and be obtained in a manner that does not violate the law. Paragraph (4) gives the authority to the judge to assess the authenticity and legality of the acquisition of the evidence. Furthermore, paragraph (5) adopts the principle of exclusionary rule, namely evidence that is inauthentic or illegally obtained cannot be used and has no evidentiary value. However, these regulations cannot be said to be comprehensive when measured by the parameters of legal certainty. There are a number of normative deficiencies in Article 235 of the New Criminal Code. The law also does not establish clear technical measures regarding authentication standards, even though these requirements are explicitly required and there is also no specific mechanism regarding procedures for obtaining electronic evidence, including procedures for confiscation, storage, and protection of the integrity of digital data.

There are no regulations regarding competency standards or minimum qualifications for digital forensic experts who carry out the authentication process which can result in no guarantee that the technical examination will be carried out by parties with adequate professional capabilities. Fifth, the New Criminal Procedure Code has also not specifically regulated electronic evidence outside the jurisdiction of Indonesia, even though data storage through cloud computing and cross-border digital services is now increasingly prevalent in law enforcement practices. The expansion of the type of evidence without a complete procedural mechanism has the potential to create a new form of legal uncertainty. On the principle of clarity of norms, this indicates that the current arrangement does not meet the ideal standard. Vague norms will be difficult to apply consistently, while inconsistent application has the potential to give birth to disparities in decisions. Therefore, the recognition of electronic evidence in the New Criminal Procedure Code is indeed an important progress, but it is still partial because it is not accompanied by a normative device that is sufficiently detailed to ensure uniform, effective, and accountable implementation in criminal justice practice.

Potential Uncertainty due to Dependence on Judge Discretion

The judge basically has the authority to assess and evaluate the evidence presented at the trial based on his beliefs. However, the conviction must not stand alone, but must rest on evidence that is valid according to the law and meets the minimum threshold of proof determined by the criminal procedure law. This principle on the one hand provides flexibility for judges in assessing the quality of evidence, but on the other hand still requires objectivity and a basis for consideration derived from legally proven facts.

In the context of the New Criminal Procedure Code, one of the most significant impacts of the incomplete regulation of electronic evidence is the widening of the judge's discretion in determining the validity of electronic evidence. Article 235 paragraph (4) gives the authority to the judge to assess the authenticity and legality of the acquisition of evidence, but this authority has not been equipped with clear and measurable normative parameters. As a result, the assessment process has the potential to depend heavily on the subjective considerations of

each judge. From the perspective of evidentiary theory, this situation has the potential to raise problems if the freedom to assess evidence is not limited by adequate guidelines. Too wide a lot of discretion can open up the space for injustice and inconsistency of decisions. Therefore, the discretion of judges must still be placed in a clear legal corridor to be in line with the principles of legal certainty and equality before the law.

Reliance on judicial discretion raises at least two serious legal issues. First, the emergence of disparity in decisions, namely differences in judgments between courts on cases that are essentially similar. In one case, a judge may accept electronic evidence because it considers the authentication process to be adequate, while another judge may reject it on the grounds of a different standard of proof. These differences have the potential to violate the principle of equality before the law, because the litigants do not receive equal legal treatment. In addition to harming the defendant and the public prosecutor, this condition can also reduce public trust in the consistency of the criminal justice system.

Second, this condition causes a loss of legal predictability. One of the main functions of legal certainty is to provide the ability for the public and law enforcement officials to estimate the legal consequences of the actions or evidence submitted. If the acceptance or rejection of electronic evidence is highly dependent on the judge's individual judgment, it will be difficult for the public prosecutor and legal counsel to devise a rational and measurable evidentiary strategy. Reliance on judges' discretion in cases involving digital technical aspects also poses a risk of misjudgment. The validity of electronic evidence is closely related to digital forensic issues, metadata, cryptography, and the integrity of data storage systems. Without clear normative guidelines, judges who do not have an adequate technical background have the potential to err in assessing evidence, either by accepting evidence that is actually flawed or by rejecting evidence that is actually valid and authentic. Both possibilities are equally dangerous because they can result in a verdict that does not reflect the material truth.

The Supreme Court of the Republic of Indonesia through its education and training module on electronic evidence has recognized the complexity of this issue and emphasized the need to standardize the handling of electronic evidence at all levels of justice. This recognition shows that the problem of dependence on the discretion of judges is not just a problem of individual capacity, but a structural problem that requires a comprehensive and binding reform of regulations.

Technical Regulation Vacuum as a Threat to Legal Certainty

The incompleteness of technical arrangements regarding electronic evidence in the New Criminal Procedure Code is a fundamental problem, not just an administrative shortcoming, but also a lack of norms that can hinder the realization of legal certainty in the criminal justice process. When technical standards are not yet clearly and binding available, any case that uses electronic evidence has the potential to be met with procedural debate. As a result, the focus of the trial can shift from an effort to find the material truth to a dispute about the procedure of proof.

One of the most important aspects yet not yet regulated in detail is the authentication of electronic evidence. From a material perspective, there are at least several conditions that are commonly used to assess the validity of electronic evidence. First, the evidence must be relevant to the crime and the party being examined. Second, the authenticity and integrity of

the data must be proven, for example through hash value verification or other digital methods. Third, the data must be reliable, meaning that the information displayed does not give rise to double meaning and is supported by other appropriate evidence. Without a standard measure on these matters, the judgment will depend heavily on the judge's subjective considerations, which ultimately has the potential to cause disparity in verdicts.

Practice in some countries shows the importance of detailed technical regulations as a basis for the acceptance of electronic evidence. In the United States, Federal Rules of Evidence Rule 901 requires proof that evidence is in fact consistent with the claim of the party making it. Meanwhile, in the United Kingdom, the Police and Criminal Evidence Act 1984 (PACE) and its derivative guidelines regulate the procedures for obtaining, maintaining, and examining digital evidence in a more systematic manner. Stephen Mason and Daniel Seng also emphasized that authentication standards are at the core of the validity of electronic evidence, because without a clear mechanism, digital data will easily question its legality in court.

In Indonesia, the New Criminal Code does not contain equivalent technical regulations, this situation shows that the existing norms are not clear enough and do not guarantee uniform application which not only interferes with the effectiveness of law enforcement, but can also have an impact on the protection of the right of defendants to obtain a fair and impartial trial. The result of this gap can also lead to a mismatch between practical needs and available legal rules, thereby triggering legal uncertainty and potential injustice. In addition, the existence of a technical regulatory gap makes the process of collecting and verifying digital evidence prone to procedural errors, which in turn can trigger lawsuits or appeals and slow down the judicial process. Therefore, the most realistic step in the short term is the drafting of technical regulations by the Supreme Court of the Republic of Indonesia (2019), both through the Supreme Court Regulation (PERMA) and the Supreme Court Circular Letter (SEMA), which specifically regulates authentication standards, chain of custody procedures, digital forensic expert qualifications, and procedures for testing the integrity of electronic evidence. In the long term, derivative or revised rules are needed that integrate all these standards into the criminal procedure legal system in a comprehensive and binding manner.

CONCLUSION

The New Criminal Procedure Code, enacted under Law Number 20 of 2025 and effective from January 2, 2026, marks a significant advancement in the reform of Indonesia’s criminal evidentiary system, particularly through the formal recognition of electronic evidence as one of the eight types of valid evidence under Article 235 paragraph (1). This recognition responds to the realities of technological development that have fundamentally transformed modern crime patterns. However, this normative recognition remains incomplete, as it is not accompanied by an adequate procedural framework, particularly regarding technical standards for authentication, chain-of-custody mechanisms, judicial assessment disparities, and the qualifications of digital forensic experts. This condition creates a gap between das sollen and das sein, which may hinder the realization of legal certainty in the criminal justice process.

The absence of standardized technical provisions in the New Criminal Procedure Code gives rise to four interrelated juridical problems. First, inconsistencies in electronic evidence authentication, as Article 235 paragraph (3) only requires normative authentication without establishing clear operational and technical parameters. Second, weaknesses in the chain-of-custody procedures, which lack standardized formats, thereby creating risks to the integrity of evidence presented at trial. Third, disparities in judicial assessment due to heavy reliance on individual discretion without measurable guidelines, potentially resulting in inconsistent decisions and undermining the principle of equality before the law. Fourth, unclear qualifications for digital forensic experts, which may weaken the credibility and admissibility of expert testimony in court. Collectively, these issues indicate that the regulation of electronic evidence under the New Criminal Procedure Code has not yet achieved the standard of legal certainty, which requires clear, applicable, and consistently implemented norms.

To address this normative gap, concrete and binding regulatory follow-up is required. In the short term, the Supreme Court of the Republic of Indonesia should issue a Supreme Court Regulation (PERMA) or Supreme Court Circular Letter (SEMA) specifically addressing authentication standards, chain-of-custody procedures, qualifications for digital forensic experts, and standardized methods for assessing the integrity of electronic evidence across all levels of the judiciary. In the long term, more comprehensive derivative regulations are needed to integrate these standards into the criminal procedural law system. These measures are essential not only to ensure effective law enforcement but also to uphold the principles of due process of law, protect defendants' rights to a fair trial, and establish an adaptive, accountable, and fair criminal justice system in Indonesia's digital era.

REFERENCES

Achmad, M., Ramli, M., Wahyudi, R. A., & Mattulanreng, A. S. (2026). Legal Politics in the Perspective of the 1945 Constitution of the Republic of Indonesia. *Masterpiece Journal Society Service Insight*, *2*(1), 71–79.

Achmad, M., Ramli, M., Wahyudi, R. A., & Mattulanreng, A. S. (2026). Legal politics in the perspective of the 1945 Constitution of the Republic of Indonesia. *Masterpiece Journal Society Service Insight, 2*(1), 71–79.

Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews, 21*(2), 205–217.

Fitri, S. M. (2020). Urgensi pengaturan alat bukti elektronik sebagai upaya mencapai kepastian hukum. *Amnesti: Jurnal Hukum, 2*(1), 1–15. https://doi.org/10.37729/amnesti.v2i1.659

Fransisca, F. (2025). Juridical analysis of evidence in the Criminal Procedure Bill: Implications for the evidentiary process. *Paul Law Review, 13*(2), 105–120.

Hasanah, S. F., Mersita, N., & Nurfitrah, M. A. (2026). Kesenjangan regulasi pembuktian elektronik di era Society 5.0: Analisis Putusan PA Sungailiat dan efektivitas regulasi Mahkamah Agung. *Jurnal Kajian Hukum dan Kebijakan Publik, 3*(2).

Heniyatun, Iswanto, B. T., & Sulistyaningsih, P. (2018). Kajian yuridis pembuktian dengan informasi elektronik dalam penyelesaian perkara perdata di pengadilan. *Varia Justicia, 14*(1), 30–39.

Juanda, O. (2023). The ideal law state concept in Indonesia: The reality and the solution. *Journal of Law, Politic and Humanities, 3*(2), 251–262.
Lubis, F., & Purba, S. R. (2024). Analisis kritik pembuktian elektronik dalam hukum acara perdata: Tantangan dan prospek di era digital. *Judge: Jurnal Hukum, 5*(2), 39–47.
Marzuki, P. M. (2021). *Penelitian hukum* (Edisi revisi). Kencana.
Mason, S., & Seng, D. (2017). *Electronic evidence and electronic signatures*. University of London Press.
Pallangyo, H. J. (2022). Cyber security challenges, its emerging trends on latest information and communication technology and cyber crime in mobile money transaction services. *Tanzania Journal of Engineering and Technology, 41*(2), 189–204.
Phiau, B. J., Rifai, A., & Latif, A. (2025). Legal certainty in the implementation of judicial review decisions by the Constitutional Court in Indonesia. *Asian Journal of Social and Humanities, 3*(5), 913–921.
Pribadi, I. (2018). Legalitas alat bukti elektronik dalam sistem peradilan pidana. *Lex Renaissance, 3*(1), 109–124.
Priyana, P., Baluqia, S. H., & Darmawan, W. (2021). Electronic information evidence of online fraud in the perspective of criminal procedure law in Indonesia. *IUS Kajian Hukum dan Keadilan, 9*, 184–198.
Rahmad, N., Arifah, K. N., Setiayawan, D., Ramli, M., & Daud, B. S. (2022). Efektivitas bukti elektronik dalam UU ITE sebagai perluasan sistem pembuktian dalam KUHAP. *University Research Colloquium*, 96–111.
Roth, A. (2019). *Machine testimony and digital evidence in criminal process*. Harvard Law Review Press.
Saputra, A. A., Seniwati, P., Ramhadella, A., Ananda, C. F., & Susanti, P. (2025). Penggunaan artificial intelligence dalam analisis putusan dan pemeriksaan bukti elektronik: Tinjauan hukum acara di Indonesia. *Causa: Jurnal Hukum dan Kewarganegaraan, 15*(10), 51–60. https://doi.org/10.5281/zenodo.16919724
Senajaya, S. F., Bakhtiar, H. S., & Wahyudi, S. T. (2026). Reformulasi peraturan digital forensic di dalam proses pembuktian perkara tindak pidana korupsi di Kejaksaan Agung Republik Indonesia. *Jurnal Kajian Hukum dan Kebijakan Publik, 3*(2), 473–486. https://doi.org/10.62379/av9bjg92
Senajaya, S. F., Bakhtiar, H. S., & Wahyudi, S. T. (2026). Reformulation of digital forensic regulations in the process of proving corruption cases at the Attorney General's Office of the Republic of Indonesia. *Journal of Law and Public Policy Studies, 4*(1), 473–486.
Soroinda, D. L., & Nasution, A. A. R. S. (2022). Kekuatan pembuktian alat bukti elektronik dalam hukum acara perdata. *Jurnal Hukum & Pembangunan, 52*(2), Article 4. https://scholarhub.ui.ac.id/jhp/vol52/iss2/4
Subhan, A., Rato, D., & Anggono, B. D. (2023). Equal legal standing of citizens in judicial review of Constitutional Court law: A multicultural perspective to achieve legal certainty. *Kawanua International Journal of Multicultural Studies, 4*(2), 139–151.
Supreme Court of the Republic of Indonesia. (2019). *Electronic evidence: Phase 3 training module*. Center for Judicial Education and Technical Training of the Supreme Court of the Republic of Indonesia.
Tawil, S., & Tarawneh, A. (2025). Technology and the law: Countering cybercrime and fraud in the digital age. In *Artificial intelligence in the digital era: Economic, legislative and media perspectives* (pp. 1095–1105). Springer.
Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.