The Legal Position of Electronic Systems in Digital Forensic Practices under Law Number 1 of 2023 concerning the Criminal Code of Indonesia

Eti Haryati[1], Dhanang Widijawan[2], Edy Santoso[3]
Program Studi Magister Ilmu Hukum, Universitas Langlangbuana, Bandung, Indonesia
email: etiharyati1068@gmail.com, dhanang.unla@gmail.com, edys39768@gmail.com

This study examines the legal position of electronic systems in digital forensic practices under Law Number 1 of 2023 concerning the Criminal Code of Indonesia. The development of information technology has transformed criminal activities and evidentiary processes, making conventional evidence insufficient to address crimes involving digital data. Therefore, the recognition of electronic information and electronic documents as lawful evidence marks an important step in the modernization of Indonesia's criminal law. This research uses a normative juridical method with statutory and conceptual approaches, relying on legal materials such as legislation, legal doctrines, journal articles, and scholarly opinions, which are analyzed qualitatively through legal reasoning and interpretation. The findings show that Law Number 1 of 2023 strengthens the position of electronic systems as sources of evidence and supporting infrastructures in the criminal justice system. Digital forensics plays a crucial role in ensuring the authenticity, integrity, and reliability of electronic evidence through identification, collection, analysis, and presentation processes. However, challenges remain, including the absence of standardized forensic procedures, limited institutional capacity, shortage of experts, cybersecurity threats, cross-border jurisdictional issues, and privacy concerns. In conclusion, the effectiveness of electronic evidence depends not only on legal recognition but also on harmonized regulations, adequate infrastructure, professional competence, and strong legal safeguards to ensure justice, legal certainty, and effective law enforcement in the digital era.

Keywords: Electronic Systems, Digital Forensics, Electronic Evidence, Criminal Law, Criminal Justice System.

Corresponding Author:
Eti Haryati
Program Studi Magister Ilmu Hukum, Universitas Langlangbuana, Bandung, Indonesia
etiharyati1068@gmail.com

1. Introduction

The rapid advancement of information and communication technology over the past two decades has fundamentally transformed the way individuals interact, work, and conduct daily activities. This digital transformation has not only influenced economic and social structures but has also significantly reshaped the landscape of criminal law. The emergence of electronic systems encompassing hardware, software, networks, and digital data has given rise to new forms of crime while simultaneously expanding the scope and complexity of criminal evidence (Kovalenko et al., 2025). As a result, legal systems are increasingly required to adapt to technological developments in order to maintain their relevance and effectiveness.

In the context of criminal justice, the evolution of digital technology has introduced new evidentiary challenges. Traditional legal frameworks, which were primarily designed to address physical forms of evidence, often struggle to accommodate intangible digital data. Prior to the enactment of Law Number 1 of 2023 concerning the new Criminal Code, Indonesia's criminal law system relied heavily on classical evidentiary instruments as stipulated in the Criminal Procedure Code (KUHAP), namely witness testimony, expert testimony, documents, indications, and the defendant's statement . This limitation created a gap between legal norms and technological realities.

The recognition of electronic information and electronic documents as valid legal evidence marks a significant milestone in the modernization of Indonesia's criminal law. This recognition is further reinforced by the provisions of the Law on Electronic Information and Transactions (ITE Law), which explicitly states that electronic information and/or electronic documents constitute lawful evidence, provided they meet certain legal requirements (Makarim, 2017). Such provisions signify a paradigm shift, where digital evidence is no longer considered supplementary but can serve as primary evidence in legal proceedings.

Despite this normative recognition, practical challenges persist in the use of electronic evidence. Issues related to authenticity, integrity, and reliability of digital data frequently arise in court proceedings. For instance, the admissibility of screenshots or digital communications often depends on the ability to verify their origin and ensure that they have not been altered. This highlights the crucial role of digital forensic science in bridging the gap between technological processes and legal standards of proof (Awaluddin et al., 2024).

Digital forensics serves as a scientific method for identifying, collecting, analysing, and presenting electronic data in a manner that is legally admissible. It ensures that digital evidence maintains its integrity throughout the investigative process, particularly through mechanisms such as chain of custody. The application of digital forensic techniques has become indispensable in modern law enforcement, as almost every human activity leaves a digital footprint that can be used as evidence in criminal cases (Selim & Ali, 2024).

Furthermore, the integration of electronic systems into the judicial process extends beyond evidentiary matters. The implementation of electronic court systems (e-Court) by the Supreme Court of Indonesia represents a broader effort to digitalize the administration of justice. This transformation demonstrates that electronic systems are not only sources of evidence but also function as essential infrastructure in the legal system. Consequently, their legal standing must be clearly defined and systematically regulated to ensure procedural fairness and legal certainty.

From a theoretical perspective, the development of law must be responsive to societal changes, including technological advancements. This view aligns with the progressive legal theory proposed by Satjipto Rahardjo (2010) which emphasizes that law should not be rigid but must adapt to social dynamics in order to achieve substantive justice. In this regard, the recognition of electronic systems within the new Criminal Code reflects an effort to align legal norms with contemporary realities.

Therefore, this study aims to examine the legal position of electronic systems in digital forensic practices under Law Number 1 of 2023 concerning the Criminal Code. It seeks to analyse how electronic evidence is recognized and utilized within the criminal justice system, as well as to identify the challenges associated with its implementation. By doing so, this research contributes to the ongoing discourse on the modernization of criminal law in the digital era.

2. Research Method

This study employs a normative juridical research method, which focuses on examining legal norms, principles, and doctrines related to the position of electronic systems in digital forensic practices. This type of research is commonly used to analyse law as a set of rules governing human behaviour and is conducted through the study of legal materials rather than empirical field data (Soekanto & Mamudji, 2010). The approaches used in this research include the statute approach and the conceptual approach. The statute approach is applied to analyse relevant legal frameworks, particularly Law Number 1 of 2023 concerning the Criminal Code and other related regulations, while the conceptual approach is used to examine legal theories and doctrines concerning evidence and digital forensics (Marzuki, 2017).

Furthermore, this research utilizes a qualitative method of legal analysis by relying on secondary data obtained from primary, secondary, and tertiary legal materials. Primary legal materials include statutory regulations, while secondary materials consist of legal literature such as books, journal articles, and expert opinions. These materials are analysed systematically using legal interpretation and reasoning techniques to identify legal principles and evaluate the consistency of regulations governing electronic evidence. This method aims to provide a prescriptive analysis of legal issues, which is characteristic of normative legal research in addressing contemporary legal developments (IRAC method approach) (Marzuki, 2017; Bhat, 2020).

3. Results and Discussion

Legal Position of Electronic Systems under the New Criminal Code

The enactment of Law Number 1 of 2023 concerning the Criminal Code represents a significant milestone in the development of Indonesia's criminal law, particularly in responding to the rapid advancement of information and communication technology. One of the most important transformations introduced by this law is the strengthened legal recognition of electronic systems and digital evidence within the criminal justice framework. In contrast to the previous legal regime, which relied heavily on conventional forms of evidence, the new Criminal Code acknowledges electronic information and electronic documents as valid legal evidence. This recognition reflects a paradigm shift in evidentiary law, where digital evidence is no longer treated as merely complementary but is increasingly positioned as primary evidence in criminal proceedings (Dmitrieva & Pastukhov, 2023).

Historically, Indonesia's evidentiary system was rooted in the provisions of the Criminal Procedure Code, which recognized five primary types of evidence: witness testimony, expert testimony, documents, indications, and the statement of the accused. While this framework was sufficient in a pre-digital era, it became increasingly inadequate in addressing crimes involving electronic systems and digital data. The absence of explicit recognition of electronic evidence often led to legal uncertainty and inconsistent judicial decisions. In many cases, digital evidence such as emails, electronic transaction records, or server logs was treated ambiguously, depending on judicial interpretation. The introduction of the new Criminal Code aims to resolve this ambiguity by formally integrating electronic evidence into the legal system, thereby providing clearer legal certainty for both law enforcement authorities and the judiciary (Makarim, 2017).

The recognition of electronic systems as part of the evidentiary framework is also closely linked to the broader development of digital governance and electronic-based legal processes. Electronic systems are not merely passive tools that store information; they function as active infrastructures that facilitate legal processes, including investigation, prosecution, and adjudication. For instance, the implementation of digital case management systems and electronic court (e-Court) mechanisms demonstrates how electronic systems have become integral to the administration of justice. These developments highlight the dual role of electronic systems: as sources of evidence and as operational infrastructures within the legal system. Consequently, their legal position must be clearly defined and supported by comprehensive regulatory frameworks to ensure their proper use in legal proceedings.

Moreover, the legal recognition of electronic systems must be understood in conjunction with existing legal instruments, particularly the Law on Electronic Information and Transactions. The ITE Law had previously established the legitimacy of electronic information and electronic documents as lawful evidence, provided that they meet certain requirements related to system reliability and data integrity. The new Criminal Code reinforces and expands this recognition by embedding it within the broader framework of criminal law. This harmonization between different legal instruments is crucial to avoid normative conflicts and to ensure

consistency in the application of legal principles related to electronic evidence (Makarim, 2020; Alkhseilat et al., 2024).

Despite these advancements, the legal position of electronic systems is not without limitations. The admissibility of electronic evidence is contingent upon the fulfilment of specific legal and technical requirements, particularly those related to authenticity, integrity, and reliability. Electronic data is inherently vulnerable to manipulation, duplication, and unauthorized access, which raises concerns regarding its evidentiary value. Therefore, the law requires that electronic evidence be obtained and processed through reliable electronic systems that comply with established legal standards. Failure to meet these requirements may result in the rejection of such evidence in court. This condition underscores the importance of ensuring that electronic systems used in legal processes are secure, transparent, and accountable.

In addition, the concept of due process of law plays a critical role in determining the legal position of electronic systems. The use of electronic evidence must not violate procedural fairness or infringe upon the rights of individuals, particularly the right to privacy and the protection of personal data. Law enforcement authorities must ensure that the collection, storage, and analysis of electronic data are conducted in accordance with legal procedures and ethical standards. Any deviation from these principles may not only undermine the admissibility of evidence but also lead to violations of fundamental human rights. Therefore, the legal recognition of electronic systems must be accompanied by strict safeguards to prevent abuse and ensure accountability (Satjipto Rahardjo, 2010).

Furthermore, the strengthened legal position of electronic systems has significant implications for law enforcement practices. The ability to utilize digital evidence effectively enhances the capacity of law enforcement agencies to investigate and prosecute crimes, particularly those involving complex technological elements. Crimes such as cyber fraud, hacking, identity theft, and online harassment often rely heavily on digital traces, which can only be properly analysed through the use of electronic systems and digital forensic techniques. By recognizing electronic evidence as legally valid, the new Criminal Code enables law enforcement authorities to respond more effectively to these types of crimes, thereby improving the overall efficiency of the criminal justice system (Sihombing et al., 2026; Broadhurst, 2006).

However, the effectiveness of this legal recognition ultimately depends on the readiness of supporting institutions and infrastructure. The implementation of electronic systems in the legal context requires not only adequate technological resources but also competent human resources. Law enforcement officers, prosecutors, and judges must possess sufficient knowledge and skills to understand and evaluate digital evidence. Without proper training and institutional support, the potential benefits of recognizing electronic systems as legal evidence may not be fully realized. This highlights the need for continuous capacity building and investment in technological infrastructure within the criminal justice system (Muhammad Hikmat Sudiadi, 2024).

From a theoretical perspective, the evolution of the legal position of electronic systems reflects the dynamic nature of law as a social institution. Law must adapt to changes in society, including technological advancements, in order to remain relevant and effective. This view is consistent with the theory of progressive law, which emphasizes that law should serve as a tool for achieving substantive justice rather than merely adhering to rigid formal rules. The incorporation of electronic systems into the legal framework demonstrates an effort to align legal norms with contemporary realities, thereby ensuring that the law remains responsive to the needs of society (Satjipto Rahardjo, 2010).

The legal position of electronic systems under the new Criminal Code represents a significant advancement in the modernization of Indonesia's criminal law. By recognizing electronic information and electronic documents as valid legal evidence, the law provides a stronger foundation for the use of digital evidence in

criminal proceedings. However, this recognition must be supported by robust legal safeguards, institutional capacity, and technological infrastructure to ensure its effective implementation. Only through a comprehensive and integrated approach can the legal system fully harness the potential of electronic systems in promoting justice and legal certainty in the digital era.

Digital Forensics as an Instrument of Proof

Digital forensics has emerged as a crucial instrument in modern criminal justice systems, particularly in addressing the growing complexity of crimes involving electronic data and digital environments. In the context of evidentiary law, digital forensics plays a central role in ensuring that electronic evidence is admissible, reliable, and legally valid in court proceedings. Unlike traditional forms of evidence, digital data is intangible, easily duplicated, and highly susceptible to manipulation. Therefore, the use of scientific and systematic forensic methods is essential to preserve the authenticity and integrity of such evidence. Digital forensic processes comprising identification, collection, analysis, and presentation are designed to ensure that electronic evidence meets the legal standards required for judicial examination (Muhammad Hikmat Sudiadi, 2024).

The identification stage represents the initial step in digital forensic investigations, where relevant electronic devices and data sources are located and determined. These sources may include computers, mobile devices, servers, cloud storage systems, and other digital infrastructures. This stage requires not only technical expertise but also legal awareness, as investigators must ensure that the identification process is conducted within the boundaries of lawful authority. Improper identification or unauthorized access to digital systems may compromise the legality of the evidence obtained, potentially rendering it inadmissible in court. Therefore, adherence to procedural rules is fundamental at this stage.

Following identification, the collection stage involves the acquisition of digital evidence in a manner that preserves its original state. This process is particularly sensitive, as any alteration to the data whether intentional or accidental can undermine its evidentiary value. To address this issue, digital forensic practitioners employ techniques such as forensic imaging, which creates an exact copy of digital data without modifying the original source. Additionally, the concept of chain of custody is strictly maintained throughout the collection process. Chain of custody refers to the documentation and tracking of evidence from the moment it is collected until it is presented in court. Maintaining an unbroken chain of custody is essential to demonstrate that the evidence has not been tampered with, thereby ensuring its credibility (Khanyile, 2025).

The analysis stage constitutes the core of digital forensic examination. During this phase, forensic experts utilize specialized software and tools to extract, recover, and interpret digital data. This may involve recovering deleted files, analysing metadata, tracing user activity, or reconstructing digital events. The analytical process must be conducted in a systematic and transparent manner, allowing for verification and replication by other experts. This principle of reproducibility is critical in establishing the reliability of digital forensic findings. Courts rely heavily on expert testimony during this stage, as judges and legal practitioners may not possess the technical knowledge required to fully understand complex digital evidence. Therefore, the role of forensic experts becomes indispensable in translating technical findings into legally comprehensible information (Canela et al., 2019).

The final stage, presentation, involves the communication of forensic findings in a clear, structured, and legally acceptable format. Digital forensic reports must be written in a manner that is both technically accurate and easily understood by non-experts, including judges, prosecutors, and defence attorneys. In addition to written reports, forensic experts may be called upon to provide expert testimony in court, explaining the methods used and the conclusions drawn from the analysis. The effectiveness of this stage

is crucial, as even the most accurate forensic findings may lose their evidentiary value if they are not properly communicated. Thus, the ability to present digital evidence convincingly is an essential component of digital forensic practice.

Beyond its technical functions, digital forensics serves as a bridge between technological processes and legal standards. The integration of scientific methods into the legal framework ensures that digital evidence can be evaluated according to objective and verifiable criteria. This bridging function is particularly important in addressing the inherent challenges of digital evidence, such as its susceptibility to manipulation and the difficulty of establishing authorship or ownership. By applying standardized forensic methodologies, digital forensics enhances the credibility of electronic evidence and facilitates its acceptance in court (Moussa, 2021).

Moreover, the role of digital forensics extends beyond cybercrime cases to encompass a wide range of criminal activities. In contemporary society, almost all forms of human interaction involve digital components, leaving behind electronic traces that can be used as evidence. For example, in corruption cases, digital evidence may include electronic financial transactions, emails, and internal communications. In terrorism cases, digital forensic analysis can uncover communication networks and online activities. Even in conventional crimes such as theft or homicide, digital evidence such as CCTV footage, GPS data, and mobile phone records can provide critical insights into the events surrounding the crime. This demonstrates that digital forensics has become an indispensable tool in modern criminal investigations (Selim & Ali, 2024).

However, the application of digital forensics as an instrument of proof is not without challenges. One of the primary concerns is the rapid evolution of technology, which often outpaces the development of forensic tools and legal frameworks. New technologies, such as encryption, cloud computing, and artificial intelligence, present additional complexities in the collection and analysis of digital evidence. For instance, encrypted data may be difficult to access without violating privacy laws, while cloud-based data storage raises jurisdictional issues, as data may be stored in servers located in different countries. These challenges require continuous adaptation and innovation in digital forensic practices, as well as the development of comprehensive legal regulations to address emerging issues.

Another significant challenge relates to the standardization of digital forensic procedures. The absence of uniform standards can lead to inconsistencies in the handling and analysis of digital evidence, potentially undermining its reliability. Different law enforcement agencies may use varying tools and methodologies, resulting in discrepancies in forensic findings. To address this issue, it is essential to establish national and international standards for digital forensic practices. Such standards would ensure consistency, enhance the credibility of forensic evidence, and facilitate cooperation between different jurisdictions.

Furthermore, the effective use of digital forensics depends on the availability of skilled professionals and adequate technological infrastructure. Digital forensic investigations require specialized knowledge and expertise, which may not be readily available in all law enforcement institutions. In many cases, limited resources and lack of training hinder the effective implementation of digital forensic techniques. This highlights the need for capacity building, including training programs, investment in forensic laboratories, and the development of interdisciplinary expertise that combines legal and technological knowledge (Bohan, 2010).

From a legal perspective, the use of digital forensics must also be balanced with the protection of fundamental rights, particularly the right to privacy. The collection and analysis of digital data often involve access to personal information, raising concerns about potential abuse and violations of individual rights. Therefore, legal safeguards must be established to ensure that digital forensic practices are conducted in accordance with due process and ethical standards. This includes obtaining proper authorization for data

access, limiting the scope of investigations, and ensuring transparency and accountability in forensic procedures.

Digital forensics plays a vital role as an instrument of proof in modern criminal justice systems. By providing scientific methods for handling electronic evidence, it ensures the admissibility, reliability, and integrity of digital data in legal proceedings. Its function as a bridge between technology and law enhances the effectiveness of evidence-based adjudication and supports the investigation of both cyber and conventional crimes. However, the successful implementation of digital forensics requires continuous adaptation to technological advancements, the establishment of standardized procedures, and the development of institutional capacity. Only through such efforts can digital forensics fully realize its potential in supporting justice in the digital era.

Challenges in the Implementation of Electronic Evidence

Despite the strengthened legal recognition of electronic evidence under the new Criminal Code, its practical implementation within the criminal justice system continues to face a number of significant challenges. One of the primary issues concerns the authenticity and integrity of digital data. Unlike physical evidence, electronic data is inherently fragile and can be altered, duplicated, or deleted without leaving visible traces. This characteristic raises serious concerns regarding the reliability and credibility of such evidence in legal proceedings. Ensuring that digital evidence remains in its original form from the moment of acquisition until its presentation in court requires strict adherence to forensic protocols and the use of reliable technological tools. However, in practice, these standards are not always consistently applied, leading to potential disputes over the validity of electronic evidence (Arshad et al., 2018).

Closely related to this issue is the challenge of maintaining the chain of custody. In digital forensic practice, the chain of custody refers to the chronological documentation of the handling, transfer, and storage of evidence. This process is essential to demonstrate that the evidence has not been tampered with or contaminated. Any break or inconsistency in this chain can significantly weaken the evidentiary value of digital data and may result in its rejection by the court. The complexity of digital environments, including the use of cloud storage and remote servers, further complicates the maintenance of chain of custody. In many cases, digital evidence may be stored across multiple jurisdictions, making it difficult to ensure continuous control and proper documentation throughout the investigative process.

Another major challenge lies in the lack of standardized procedures for handling electronic evidence. Although digital forensic science has developed various methodologies, there is still no universally binding standard that is consistently applied across all law enforcement agencies in Indonesia. Different institutions may adopt different tools, techniques, and protocols, which can lead to inconsistencies in the analysis and interpretation of digital evidence. Such inconsistencies not only undermine the reliability of forensic findings but also create difficulties for courts in assessing the evidentiary value of digital data. Therefore, the establishment of comprehensive national standards for digital forensic practices is essential to ensure uniformity and credibility in the handling of electronic evidence (Arshad et al., 2018).

In addition to procedural issues, the limited technical capacity of law enforcement institutions poses a significant obstacle to the effective implementation of electronic evidence. Digital forensic investigations require specialized knowledge and advanced technological tools, which are not always available in all regions. In many cases, law enforcement agencies, particularly at the regional level, lack access to modern forensic laboratories and equipment. This limitation often results in delays in the investigation process, as digital evidence must be sent to central facilities for analysis. Furthermore, the shortage of trained forensic experts reduces the overall effectiveness of evidence handling and may increase the risk of errors in the investigative process.

Human resource capacity is another critical factor influencing the implementation of electronic evidence. The rapid evolution of technology demands continuous learning and adaptation from law enforcement personnel. However, not all investigators, prosecutors, and judges possess sufficient technical understanding of digital evidence and forensic methodologies. This gap in knowledge can lead to misinterpretation of evidence, improper handling procedures, and inconsistent judicial decisions. As a result, there is a pressing need for comprehensive training programs that integrate legal and technological expertise, enabling practitioners to effectively manage and evaluate digital evidence in criminal proceedings (Goswami & Goswami, 2025).

Furthermore, legal and regulatory challenges also contribute to the complexity of implementing electronic evidence. Although the new Criminal Code provides a stronger legal basis for the use of digital evidence, its application must be harmonized with other relevant laws, such as the Law on Electronic Information and Transactions and data protection regulations. In some cases, overlapping or conflicting provisions may create uncertainty in the application of the law, particularly in relation to data access, privacy rights, and cross-border data retrieval. For instance, obtaining digital evidence stored on foreign servers often requires international cooperation mechanisms, which can be time-consuming and procedurally complex.

The issue of data security also represents a significant concern in the implementation of electronic evidence. Digital data is highly vulnerable to cyber threats, including hacking, unauthorized access, and data breaches. If electronic evidence is compromised during the investigative process, its integrity may be questioned, potentially affecting its admissibility in court. Therefore, robust cybersecurity measures must be implemented to protect digital evidence throughout its lifecycle. This includes the use of encryption, secure storage systems, and access control mechanisms to prevent unauthorized interference.

Finally, the balance between effective law enforcement and the protection of fundamental rights remains a critical challenge. The use of electronic evidence often involves accessing personal data, which raises concerns about privacy and potential abuse of authority. Law enforcement agencies must ensure that all investigative actions comply with legal procedures and respect individual rights. Failure to do so may not only violate human rights but also undermine public trust in the legal system. Consequently, the implementation of electronic evidence must be accompanied by strong legal safeguards and oversight mechanisms to ensure accountability and transparency.

While the recognition of electronic evidence represents a significant advancement in the modernization of criminal law, its implementation is hindered by a range of technical, procedural, institutional, and legal challenges. Addressing these challenges requires a comprehensive approach that includes the development of standardized procedures, enhancement of institutional capacity, strengthening of legal frameworks, and protection of fundamental rights. Only through such efforts can the full potential of electronic evidence be realized in supporting effective and fair criminal justice processes.

Legal Harmonization and Progressive Approach

The recognition of electronic evidence under Law Number 1 of 2023 concerning the Criminal Code represents a significant step toward modernizing Indonesia's legal system. However, this recognition cannot stand alone; it must be harmonized with other relevant legal frameworks to ensure coherence, consistency, and legal certainty. In particular, the integration between the Criminal Code, the Law on Electronic Information and Transactions, and regulations on personal data protection is essential. Each of these legal instruments governs different aspects of electronic systems and digital data, yet they are closely interconnected in practice. Without proper synchronization, the implementation of electronic evidence may lead to overlapping norms, legal ambiguity, and even conflicts in interpretation, particularly concerning issues of data access, admissibility, and privacy protection .

One of the primary challenges in legal harmonization lies in balancing the need for effective law enforcement with the protection of individual rights. On the one hand, law enforcement authorities require access to digital data in order to investigate and prosecute crimes effectively. On the other hand, such access must not violate the fundamental right to privacy, which is increasingly recognized as a core component of human rights in the digital era. The potential for conflict arises when investigative measures, such as data interception or digital surveillance, intersect with legal safeguards designed to protect personal information. In this context, harmonization is not merely a technical process of aligning legal provisions but also a normative effort to ensure that competing interests are balanced in a fair and proportionate manner.

Furthermore, the issue of cross-border data flow adds another layer of complexity to legal harmonization. In the digital environment, electronic data is often stored on servers located outside national jurisdictions, making it difficult for domestic law enforcement agencies to access such data through conventional legal mechanisms. This situation necessitates the development of international cooperation frameworks, such as mutual legal assistance agreements, to facilitate the lawful exchange of digital evidence. However, differences in legal standards between countries can create additional challenges, particularly in determining the admissibility of evidence obtained from foreign jurisdictions. Therefore, Indonesia must not only harmonize its internal legal frameworks but also align its regulations with international standards to ensure the effectiveness of cross-border evidence handling.

In addition to regulatory synchronization, institutional coordination plays a crucial role in achieving effective legal harmonization. The management of electronic evidence often involves multiple institutions, including the police, prosecution authorities, courts, and regulatory bodies responsible for information technology and data protection. Each of these institutions may operate under different legal mandates and procedural frameworks, which can lead to fragmentation in the handling of digital evidence. Strengthening coordination mechanisms and establishing clear procedural guidelines are essential to ensure that electronic evidence is managed consistently and efficiently across all stages of the criminal justice process.

From a theoretical perspective, the need for legal harmonization reflects the broader principle that law must evolve in response to societal and technological changes. This principle is closely aligned with the concept of progressive law, which emphasizes that legal systems should not be static but must adapt to dynamic social realities. Progressive law rejects rigid formalism and instead promotes a more flexible and purposive approach to legal interpretation, focusing on achieving substantive justice rather than merely applying rules mechanically (Satjipto Rahardjo, 2010). In the context of electronic evidence, this means that legal practitioners must be willing to interpret existing laws in ways that accommodate technological developments while still upholding fundamental legal principles.

The application of a progressive approach is particularly important in situations where legal norms have not yet fully caught up with technological advancements. For example, emerging technologies such as cloud computing, artificial intelligence, and encrypted communication systems present new challenges that may not be explicitly addressed in existing legislation. In such cases, a rigid interpretation of the law may hinder the effective use of electronic evidence, while a more adaptive approach can provide practical solutions that align with the underlying objectives of the legal system. This does not imply disregarding legal certainty but rather enhancing it through contextual and purposive interpretation.

Moreover, the progressive approach also underscores the importance of judicial discretion in interpreting and applying the law. Judges play a critical role in determining the admissibility and evidentiary value of electronic data, particularly in cases where legal provisions are ambiguous or incomplete. By adopting a progressive perspective, judges can ensure that legal decisions reflect both the realities of technological

development and the principles of justice. This approach is essential to prevent the law from becoming obsolete in the face of rapid digital transformation.

However, the implementation of a progressive legal approach must be accompanied by adequate safeguards to prevent arbitrary or inconsistent interpretations. While flexibility is necessary, it must be balanced with the need for legal certainty and predictability. This requires the development of clear guidelines and jurisprudence that can serve as references for legal practitioners. In addition, continuous legal reform is needed to update statutory regulations in line with technological advancements, thereby reducing reliance on interpretative flexibility alone.

The harmonization of legal frameworks and the adoption of a progressive legal approach are essential components in ensuring the effective implementation of electronic evidence within Indonesia's criminal justice system. Legal harmonization provides the structural foundation for consistency and coherence, while the progressive approach offers the flexibility needed to respond to technological change. Together, these elements create a legal environment that is both stable and adaptive, enabling the law to remain relevant and effective in addressing the challenges of the digital era.

4. Conclusion

The legal position of electronic systems in digital forensic practices under Law Number 1 of 2023 demonstrates Indonesia's commitment to modernizing its criminal justice system in response to technological developments. The recognition of electronic information and electronic documents as valid evidence strengthens the effectiveness of law enforcement, particularly in handling cybercrime and technology-based offenses, while digital forensics plays a crucial role in ensuring the authenticity, integrity, and reliability of such evidence through scientific methods. However, the practical implementation of electronic evidence still faces challenges, including limited institutional capacity, lack of standardized procedures, cybersecurity risks, cross-border jurisdictional issues, and concerns regarding privacy rights. Therefore, it is recommended that the government establish clearer implementing regulations, strengthen harmonization among relevant laws, improve forensic infrastructure, provide continuous training for investigators, prosecutors, and judges, develop national digital forensic standards, enhance international cooperation, and ensure the protection of personal data and fundamental rights so that justice, legal certainty, and efficiency can be fully achieved in the digital era.

5. References

Alkhseilat, A., Al-Billeh, T., Albazi, M., & Ali, N. Al. (2024). The authenticity of digital evidence in criminal courts: a comparative study. *International Journal of Electronic Security and Digital Forensics*, *16*(6). https://doi.org/10.1504/IJESDF.2024.142010

Arshad, H., Jantan, A. Bin, & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, *14*(2). https://doi.org/10.3745/JIPS.03.0095

Awaluddin, F., Amsori, & Mulyana, M. (2024). Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital. *HUMANIORUM*, *2*(1), 14–19. https://doi.org/10.37010/hmr.v2i1.35

Bhat, P. I. (2020). Idea and Methods of Legal Research. In *Idea and Methods of Legal Research*. https://doi.org/10.1093/oso/9780199493098.001.0001

Bohan, T. L. (2010). Review of: Strengthening Forensic Science in the United States: A Path Forward. *Journal of Forensic Sciences*, *55*(2). https://doi.org/10.1111/j.1556-4029.2009.01313.x

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing*, *29*(3). https://doi.org/10.1108/13639510610684674

Canela, C., Buadze, A., Dube, A., Jackowski, C., Pude, I., Nellen, R., Signorini, P., & Liebrenz, M. (2019). How do legal experts cope with medical reports and forensic evidence? The experiences, perceptions, and narratives of Swiss judges and other legal experts. *Frontiers in Psychiatry*, *10*(FEB). https://doi.org/10.3389/fpsyt.2019.00018

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of Electronic Evidence in Criminal Legal Procedure. *Journal of Digital Technologies and Law*, *1*(1). https://doi.org/10.21202/jdtl.2023.11

Goswami, D. P., & Goswami, A. (2025). Virtual Justice: The Role of Technology in Transforming Criminal Administration. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5121477

Khanyile, X. N. (2025). The Impact of a compromised Chain of Custody on the Admissibly of Evidence in South African Criminal Trails. *OIDA International Journal of Sustainable Development*, *18*(12).

Kovalenko, A., Kovalenko, V., & Nazymko, Y. (2025). ELECTRONIC (DIGITAL) EVIDENCE COLLECTION IN ECONOMIC CRIME INVESTIGATIONS. *Baltic Journal of Economic Studies*, *11*(2). https://doi.org/10.30525/2256-0742/2025-11-2-142-149

Makarim, E. (2017). KERANGKA KEBIJAKAN DAN REFORMASI HUKUM UNTUK KELANCARAN PERDAGANGAN SECARA ELEKTRONIK (E-COMMERCE) DI INDONESIA. *Jurnal Hukum & Pembangunan*, *43*(3). https://doi.org/10.21143/jhp.vol43.no3.1492

Marzuki, P. M. (2017). *Penelitian Hukum: Edisi Revisi* . Kencana.

Moussa, A. F. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, *11*(1). https://doi.org/10.1186/s41935-021-00234-6

Muhammad Hikmat Sudiadi. (2024). Implementasi Asas Dominus Litis dalam Sistem Peradilan Pidana Modern di Indonesia. *Jurnal Mahalisan*, *1*(1). https://doi.org/10.70837/9re7s725

Satjipto Rahardjo. (2010). Hukum Progresif: Sebuah Sintesa Hukum Indonesia. *Yogyakarta: Genta Publishing.*., *1*(1).

Selim, A., & Ali, İ. (2024). The Role of Digital Forensic Analysis in Modern Investigations. *Journal of Emerging Computer Technologies*, *4*(1). https://doi.org/10.57020/ject.1445625

Sihombing, L. A., Nuraeni, Y., Rozaan, R., Pranadita, N., & Syam, R. Z. A. (2026). CAN DIGITAL RESTORATIVE MEDIATION TRANSFORM INDONESIA'S CRIMINAL PROCEDURE LAW AND DELIVER JUSTICE? *PETITA: JURNAL KAJIAN ILMU HUKUM DAN SYARIAH*, *11*(1). https://doi.org/10.22373/petita.v11i1.886

Soekanto, S., & Mamudji, S. (2010). *Penelitian Hukum Normatif Suatu Tinjauan Singkat* . Raja Grafindo Persada.