

INTERNATIONAL JOURNALOF LAW AND CONSTITUTION STUDY

Journal home page:https://jurnal.asrypersadaquality.com/index.php/ijlacos

POSITION OF ELECTRONIC EVIDENCE IN THE LEGAL SYSTEM MODERN EVIDENCE

Chaisyah Aliffah Siswoyo, Dian Safitri Br Ginting, Eviana Sagala, Aura Ajrina
State Islamic University of North Sumatra

kesyahhh13@gmail.com ,sdian9386@gmail.com ,evianasagalaa@gmail.com ,auraajrina77@gmail.com

A B S T R A C T

The development of information technology and digital transformation has brought significant changes to the evidentiary system in modern law, particularly regarding the use of electronic evidence in the judicial process. The presence of electronic documents, e-mails, digital messages, electronic transaction records, and other digital data requires adjustments to the evidentiary legal system, which was previously oriented towards conventional evidence. This study aims to analyze the position of electronic evidence in the modern evidentiary legal system, its evidentiary strength, and the challenges of its application in judicial practice. The research method used is normative legal research with a statutory and conceptual approach through a literature review of various laws and regulations, legal doctrines, and relevant court decisions.The results show that electronic evidence has been recognized as valid legal evidence and is an extension of conventional evidence in the modern evidentiary system. Its validity and evidentiary strength depend on the fulfillment of the elements of authentication, integrity, reliability, and relevance of electronic data. In practice, the use of electronic evidence provides efficiency and legal certainty, but also faces challenges such as the risk of data manipulation, privacy protection, and the need for digital forensic standardization. Furthermore, the development of cybercrime and the complexity of cross-border digital transactions also impact the effectiveness of electronic evidence, necessitating a more optimal data monitoring and security system. This study also confirms that the implementation of electronic evidence requires support.

KEYWORDS

Electronic evidence; Modern evidence systems; Law of evidence; Digital forensics; Digital transformation; Validity of evidence; Electronic transactions; Cybercrime; Law enforcement; Information technology.

Corresponding Author: Chaisyah Aliffah Siswoyo

Article History	Submitted: March 16, 2026	Revision: March 18, 2026	Accepted: March 30, 2026	Published: July 30, 2026

https://doi.org/10.63736/ijlacos.v3i1

INTRODUCTION

The development of information and communication technology in the digital era has has brought about profound changes in various aspects of society. Nearly all human activities now utilize digital technology, from communication and education to commerce and banking to public services. These technological advances not only facilitate daily life but also influence the development of law and the judicial system. One of the most significant changes is the emergence of electronic evidence as part of the evidentiary system in law enforcement processes.

In the past, the evidence used in legal proceedings was mostly physical, such as letters, written documents, witnesses, clues, and confessions. However, with the development of information technology, various legal activities are now conducted electronically. Communication that used to be conducted by letter has been replaced by electronic mail (e-mail), instant messaging, messaging apps, and social media. Furthermore, various business and financial transactions are also conducted digitally. As a result, much information is stored in electronic form and can be used as evidence in a case.

The existence of electronic evidence in Indonesia has a clear legal basis through Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was later amended through Law Number 19 of 2016. Article 1 number 1 of the ITE Law states that electronic information is one or a collection of electronic data that has meaning or can be understood by people who are able to understand it. This electronic information can be in the form of writing, sound, images, maps, designs, photos, electronic mail, telegrams, telex, text copies, access codes, symbols, numbers, or other forms of data that are processed electronically.

In addition to electronic information, the term electronic document is also known. An electronic document is any electronic information created, forwarded, sent, received, or stored in digital, electromagnetic, optical, or other similar form that can be viewed, displayed, or heard via a computer or electronic system. Thus, electronic documents have a function that. The recognition of electronic information and electronic documents as evidence is one form of legal adaptation to technological developments. This is crucial because many legal incidents currently occur in the digital world. For example, online fraud, the spread of fake news (hoaxes), defamation through social media, computer system hacking, and e-commerce transactions. In these cases, conventional evidence is often insufficient to prove a legal act. Therefore, electronic information and documents are crucial to assist the evidentiary process in court.

For example, in cases of online fraud, instant messaging conversations, digital bank transfer receipts, transaction screenshots, and electronic communication recordings can be used to demonstrate a legal relationship between the perpetrator and the victim. Similarly, in cases of defamation on social media, electronically published posts, comments, photos, or videos can be used as evidence to prove that an act has harmed another party.

The existence of electronic evidence offers numerous benefits in law enforcement. First, electronic evidence can help uncover facts that are difficult to prove using conventional

evidence. Second, electronic data generally stores detailed information, including the time, location, and identity of the user who performed an activity. Third, electronic evidence can expedite the investigation, prosecution, and even trial processes because data can be obtained and analyzed with the aid of technology.

However, the use of electronic evidence also faces various challenges. One of the biggest challenges is the issue of data authenticity. Electronic data is very easily copied, altered, or manipulated by certain parties. Therefore, a mechanism is needed to guarantee that data presented in court is truly authentic and has not been altered since it was first created or stored.

Furthermore, there are also issues regarding the security of electronic systems. Data leaks, hacking, and cyberattacks can result in the loss of critical information needed for the evidentiary process. In some cases, electronic data serving as evidence can even be damaged or deleted by perpetrators to cover up their crimes. This situation demonstrates the importance of protecting electronic systems to maintain the integrity of evidence.

Another challenge relates to the validity and probative value of electronic evidence in court. Not all electronic data is automatically admissible as valid evidence. Judges must ensure that the evidence was obtained through legal means, originated from a reliable electronic system, and is relevant to the case being examined. Therefore, the assistance of digital forensic experts is often required to examine electronic data presented in court.

Digital forensics is the science of finding, collecting, securing, and analyzing digital evidence so it can be used in legal proceedings. Digital forensic experts play a crucial role in ensuring that electronic data submitted as evidence is unaltered and can be scientifically and legally accounted for. The presence of these experts is increasingly important given the increasingly complex nature of technology.

In the Indonesian legal system, electronic evidence essentially has the same standing as other evidence as long as it meets the requirements stipulated by law. Article 5 of the ITE Law explicitly states that electronic information and electronic documents, along with their printouts, constitute valid legal evidence. This provision expands the types of evidence previously recognized only in conventional procedural law.

Regulations regarding electronic evidence demonstrate that the law must keep pace with the times. Technology will continue to evolve and give rise to various new forms of activity that require adequate legal regulation. Therefore, legal updates in the field of information technology must be continuously implemented to ensure legal certainty, justice, and public benefit.

RESETACH AND METHOD

The study falls under the category of normative law study, a study aimed at learning and analyzing the principles of law, doctrine, law rules, and harmonizing law regulations at both national and international levels that relate to the concept of state sovereignty in the digital age. The main focus of the study was conceptual studies on understanding conventional international laws in responding to the phenomenon of global cyberintervention.

The legal materials used in this research are categorized into three layers:

- Primary legal materials, consisting of the Universal Declaration of Human Rights (UDHR) 1948, the International Covenant on Civil and Political Rights (ICCPR) 1966, the General Data Protection Regulation (GDPR) 2016, and Law Number 27 of 2022 on Personal Data Protection.
- Secondary legal materials, comprising academic journals, books, and scholarly works addressing personal data protection, international law, and cybersecurity.
- Tertiary legal materials, including legal dictionaries and encyclopedias used to support the interpretation of legal terminology throughout this study.

2.2 Data Collection

Legal collecting was done by means of literature study methods. This process involves searching, reading, recording, and compiling of academic literature and international documents of cyberlaw that are relevant to the reconstruction issue of state sovereignty**.**

2.3 Data Analysis

The collected legal material was analyzed using analytic qualitative descriptive methods. Researchers elaborated on the draft of the law, described the differences between the concept of physical sovereignty and digital space, and deductive conclusions to formulate responsive three dimensions of legal reconstruction.

RESULTS AND DISCUSSION

Results

1. Legal Review of Electronic Evidence in the Indonesian Evidence Legal System

In this study, electronic evidence demonstrates an increasingly important position in the modern evidentiary system because it has been recognized as valid evidence and is an extension of conventional evidence. This recognition emphasizes that changes in information technology have driven a renewal of the concept of evidence, from one that was originally based on physical evidence to also encompassing digital data (Maskun, 2014:120).

Since the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions (UUITE), there has been an addition to the types of evidence in court, namely electronic information and/or electronic documents. In the general provisions of UUITE, it can be seen that types of electronic data such as writing, photos, sounds, images are electronic information, while types of electronic information such as writing, photos, sounds, images stored on a flash disk that can be opened via a computer device are electronic documents. (Maskun, 2014:120).

Despite legal recognition, the use of electronic evidence must still meet certain requirements to be legally valid. The authenticity, integrity, and validity of electronic documents or information must be guaranteed. Therefore, in some cases, digital forensic expert examination is often required to ensure that electronic data has not been altered or manipulated. This is crucial to maintain legal certainty and prevent the misuse of technology in the evidentiary process. (makarim) Thus, the regulations regarding electronic evidence demonstrate that Indonesia's evidentiary legal system has undergone modernization and adaptation to developments in information technology. The presence of electronic evidence has become a crucial instrument in supporting effective law enforcement and providing legal certainty in resolving cases in today's digital age (Maskun, 2014:120).

Article 6 stipulates that electronic information and/or electronic documents can be considered valid evidence, even if they are not in written or original form like conventional documents. An electronic document is recognized as valid if the information it contains can be accessed, displayed, maintained intact, and accounted for, thus explaining a legal situation or event. (Isama) Based on these provisions, it can be understood that electronic

evidence basically includes electronic information, electronic documents, and other computer output. According to Article 1 paragraph (3) of the Electronic Information and Transactions Law (ITE Law), electronic information is a collection of electronic data that has meaning and can be understood by the party receiving it. It can be in the form of writing, sound, images, photos, electronic mail (e-mail), telegrams, telex, access codes, symbols, or other electronic data processed through an electronic system.

Meanwhile, Article 1 paragraph (4) of the ITE Law explains that electronic documents are any electronic information created, sent, received, or stored in digital or other electronic form. These documents can be displayed, viewed, or heard via a computer or electronic system. The forms of electronic documents are also very diverse, such as writing, images, sound, photos, maps, designs, codes, symbols, and various other data that have meaning and can be understood by the person using them. (ITE Law Article 1 numbers 3 and 4)

2. The position of electronic evidence in the law of evidence.

Based on the provisions of Article 5 paragraph (1) and paragraph (2) of Law Number 19 of 2009 According to Law No. 11 of 2008 concerning Electronic Information and Transactions, electronic information, electronic documents, and printouts are recognized as valid legal evidence in court proceedings. This recognition demonstrates that Indonesia's evidentiary legal system has evolved in line with advances in information technology. Electronic evidence is viewed not only as a complement but also as an extension of evidence previously regulated in criminal and civil procedural law. (Ramli)

The existence of electronic evidence facilitates the investigation of legal cases, particularly those involving digital activities. In practice, electronic evidence can take the form of electronic mail (e-mail), digital conversation recordings, text messages, digital documents, video recordings, and other electronic transaction data. The use of such evidence is increasingly important because many modern crimes are committed through electronic media and the internet. With the legal recognition of electronic documents, the evidentiary process in court becomes more flexible and relevant to current conditions. However, the use of electronic evidence must still meet the requirements of authenticity, integrity, and accountability to ensure its full evidentiary force before the law. (Makarim)

In judicial practice, the presence of electronic evidence often strengthens other evidence such as witness statements, letters, or clues. In terms of benefits, the use of electronic evidence provides efficiency in the evidentiary process because data can be obtained, stored, and displayed quickly. Furthermore, electronic evidence also helps uncover legal acts that are difficult to prove with conventional evidence, especially in cases related to digital transactions, online communications, and cybercrime. (Makarin)

Through these regulations, it is clear that electronic evidence plays a crucial role in supporting the effectiveness and modernization of Indonesia's justice system, particularly in addressing technological developments and digital-based crime. (Makarim)

The legal standing of electronic evidence is not only recognized in the Electronic Information and Transactions Law but is also reinforced by a Supreme Court regulation legitimizing the use of electronic evidence in state administrative court proceedings. This recognition demonstrates that advances in information technology have influenced various areas of law, including the resolution of government administrative disputes. Under this provision, digital documents and information can be used to support evidence in court as long as they meet applicable legal requirements. (Tutik)

The position of electronic evidence as an extension of existing evidence can be found in the Corruption Crimes Law (Corruption Law). Article 26A of the Corruption Law explains that electronic evidence can be used as a source of indicative evidence.

Basically, indicative evidence is not a stand-alone form of evidence, but must be supported by other evidence. This is in accordance with Article 188 paragraph (2) of the Criminal Procedure Code, which states that indicative evidence is obtained from

Discussion

Witness statements, letters, and statements of the accused. However, through the General Explanation of the Corruption Law, the sources of indicative evidence are expanded. Indications do not only come from witness statements, letters, and statements of the accused, but can also be obtained from electronic information and electronic documents, both in digital form and conventional documents recorded electronically. Thus, electronic evidence in corruption cases is positioned as part of indicative evidence. Because it is included in indicative evidence, the evidentiary strength of electronic evidence still depends on the judge's assessment in the trial. The judge has the authority to assess whether the electronic evidence can strengthen the belief in proving a crime.

(Tutik, 2011:215).

In addition to expanding the corroborative evidence base, electronic evidence is also beginning to be recognized as a stand-alone form of evidence in Indonesia's criminal justice system. The presence of electronic evidence demonstrates the development of evidentiary law that is adapting to advances in information and communication technology (Tutik, 2011:2016).

The development of information technology has driven fundamental changes in the evidentiary system in Indonesia. While previously procedural law emphasized physical and conventional evidence, electronic evidence has now been recognized as a valid evidentiary instrument. Regulations regarding this matter are primarily contained in Law Number 11 of 2008 concerning Electronic Information and Transactions, which has been amended by Law Number 19 of 2016. Within the national legal framework, the existence of electronic evidence is not merely a complement, but has become part of the evidentiary system that is increasingly relevant to the dynamics of the digital society. (Tutik, 2011:216).

Article 5 of the ITE Law stipulates that electronic information and/or electronic documents and/or printouts thereof constitute valid legal evidence. This provision demonstrates that lawmakers have recognized that data generated, sent, received, or stored electronically has evidentiary force that can be used in legal proceedings. This recognition is crucial because many modern legal events, particularly those related to digital transactions, electronic communications, and cybercrime, leave electronic traces that are more accurate than conventional evidence. (ITE Law Article 5) (Chatinakrob, T.2024). The recognition of electronic evidence has significant implications for the effectiveness of law enforcement. Investigators can solve cases more quickly, prosecutors can build charges with stronger evidence, and judges can obtain a more objective picture of an event. In many cases, the presence of electronic evidence is even a determining factor in establishing the material truth.

However, this effectiveness will only be achieved if supported by technological infrastructure, adequate regulations, and competent human resources. Without such support, electronic evidence has the potential to give rise to new disputes regarding authenticity, legality, and validity. Therefore, the successful implementation of electronic evidence depends heavily on the readiness of legal institutions to face digital

transformation.

Furthermore, electronic evidence encourages law enforcement to be more precise. Every step in the collection and assessment of evidence must be well-documented, as digital traces can be reexamined. This can increase accountability in the judicial process while strengthening public trust in the legal system.

Strengthening the capacity of law enforcement officers is an urgent need.

Continuing education in information technology, cybersecurity, and digital forensics must be part of the legal reform agenda. This way, electronic evidence will not only be formally recognized but also truly effective in practice. (Maskun, 2014:122).

CONCLUSION

The development of information technology has brought major changes to Indonesia's evidentiary legal system, particularly through the recognition of electronic evidence as valid legal evidence. The Electronic Information and Transactions Law (UU ITE) provides a clear legal basis for the use of electronic information, electronic documents, and printouts in judicial proceedings. With this regulation, electronic evidence is no longer viewed as supplementary evidence but can become primary evidence as long as it meets the requirements of validity, such as data authentication, integrity, reliability, and relevance. The use of electronic evidence offers numerous benefits in law enforcement, particularly in uncovering crimes and disputes related to digital technology.

Electronic evidence such as emails, CCTV footage, digital messages, and electronic documents can help law enforcement officers obtain legal facts more effectively and efficiently. Furthermore, the recognition of electronic evidence demonstrates that Indonesia's evidentiary legal system has evolved into a modern legal system capable of adapting to advances in information technology.

However, the use of electronic evidence also has various

Challenges and risks, such as data manipulation, digital identity forgery, and the threat of electronic system hacking, are present. Therefore, strict inspection and verification procedures are required to ensure the authenticity and validity of electronic data used in court. The role of digital forensic experts is also crucial in

maintaining the credibility of electronic evidence so that it can be legally accounted for.

REFERENCES

Andika, T. (2018). Information sovereignty in the digital age: A theoretical and international law review. *International Law Journal*.

Balarabe, K. (2025). Digital intervention and the development of digital power in international relations. *Global Governance Review*.

Chatinakrob, T. (2024). Strengthening multilateral frameworks for universal cyber norms: The roles of GGE and OEWG. *Journal of Cyber Policy and International Law*.

Darmawan, A. B., et al. (2022). National sovereignty in digital data ownership: Strategic steps by Australia in response to Facebook and Google. *International Relations Journal*.

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty as regulatory autonomy in the connectivity era. *Philosophy & Technology*.

Pierucci, F. (2025). Accountability and transparency in the European model for digital sovereignty: Examining the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA). *European Law Journal*.

Santaniello, M. (2025). Rebuilding national control: Understanding international law rules in the cyber world. *Digital Policy Studies*.

Shaw, M. N. (2021). *International law* (9th ed.). Cambridge University Press.

Tallinn Manual. (2013). *The Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

United Nations. (1945). *Charter of the United Nations*. United Nations.