Sarcouncil Journal of Arts Humanities and Social Sciences

ISSN(Online): 2945-3488

Volume- 05| Issue- 02| 2026

Research Article

Received: 15-01-2026 | Accepted: 10-02-2026| Published: 25-02-2026

Electronic Evidence in Vietnam's Criminal Procedure Code Current State and Suggestions for Improvement

Nguyen Truc Thien[1] and Nguyen Hoai Phuong[2]

[1]*Dong Nai Province People's Court*

[2]*Institute for Social – Economic and Environment Development*

Abstract:. The rapid expansion of digital technologies has transformed both the nature of criminal activities and the evidentiary landscape of contemporary criminal justice systems. Vietnam's 2015 Criminal Procedure Code (CPC) formally recognizes electronic evidence as an independent evidentiary category, marking an important step toward adapting domestic procedural law to the digital environment. However, the current legal framework remains largely principle-based, leaving notable gaps in the collection, preservation, examination, and admissibility of electronic data. In practice, investigative and judicial authorities face substantial challenges due to the absence of unified technical standards, inconsistent chain-of-custody procedures, difficulties in cross-border data acquisition, and the tension between investigative needs and privacy protection. This article provides a comprehensive analysis of the theoretical foundations, current legal framework, and practical application of electronic evidence under Vietnam's CPC 2015. Drawing on comparative insights from advanced jurisdictions and international standards (UNODC, OECD, NIST, EVIDENCE2e-CODEX), the study identifies key normative and institutional shortcomings affecting evidentiary reliability, legality, and integrity. It then proposes a set of reforms aimed at modernizing Vietnam's procedural law, strengthening digital forensic capabilities, and ensuring a balanced, rights-respecting approach to electronic evidence in the digital age.

Keywords: Electronic evidence; digital forensics; criminal procedure; Vietnam CPC 2015; evidentiary integrity; chain of custody; admissibility; privacy protection; cross-border data; digital transformation.

INTRODUCTION

Legal Basis for Electronic Evidence in the 2015 Criminal Procedure Code

Electronic data as a source of evidence is acknowledged, and the basic principles for its collection and preservation are stipulated in Clause 3, Article 94 of the 2015 Criminal Procedure Code on evidence and the provisions in Articles 99 and 107 of the 2015 Criminal Procedure Code. Specifically, the 2015 Criminal Procedure Code stipulates that the evidentiary value of electronic data is determined based on how it is created, stored, and transmitted; how its integrity is ensured; and how the creator is identified… The current issue is the "credibility" of electronic evidence.

Article 107 2015 Criminal Procedure Code Article 107 of the 2015 Criminal Procedure Code stipulates the procedures for seizing and recovering electronic devices and data, requesting, sealing, reporting, and describing the seizure of electronic data in a timely manner. Article 183 2015 Criminal Procedure Code stipulates regulations in audio and video recording during interrogations, which currently only states that it is only done "at the request of" the suspect or the relevant authority and is not mandatory in all cases. The 2025 amendments stated in Law no. 99/2025/QH15 has adjusted and supplemented the terms of the 2015 Criminal Procedure Code, making it a legal basis that needs to be considered before proposing future changes, as these amendments have been in effect since July 1st 2025.

Current Issues with Electronic Evidence.

Firstly, the definition and scope of electronic evidence are yet to be clearly defined, leading to differences in application. The 2015 Criminal Procedure Code, while acknowledging electronic data as evidence, does not clearly stipulate several necessary working definitions, such as: classification of data, metadata, logs, cloud saves, data from international service providers. This article makes it difficult to distinguish between what constitutes original or copied evidence and in turn affects their validity as evidence.

In reality, judges, investigators, and expert witnesses handle evidence differently, and many pieces of evidence have differing opinions regarding their origin and integrity. Professional analyses indicate the need to classify the definition of "method of creation, storage, and dissemination" into specific criteria.

Secondly, the preservation of evidence is yet to be standardized. Article 107 of the 2015 Criminal Procedure Code currently requires timely seizure, sealing, and description of the current state of the

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

*Corresponding Author: Nguyen Truc Thien

DOI- DOI- https://doi.org/10.5281/zenodo.18775506

evidence, but lacks technical standards, mandatory forms, and criteria for proving the integrity of data.

In practice, the copying and extraction of data is done without following proper procedures, with high risks of tampering or manipulation. Courts are unlikely to accept data if the preservation process fails to prove its integrity. Therefore, data collection must be specifically regulated and carried out correctly and completely.

Thirdly, there is no effective mechanism regarding access to data owned by third parties and service providers. Article 107 of the 2015 Criminal Procedure Code lacks a specific process for handling and requiring cross-border service providers to provide data (preservation orders, MLATs, emergency disclosures), or guidance on technical coordination for data collection on foreign platforms.

In practice, collection of data from Facebook, Google, and other foreign platforms is often sluggish, rejected, or dependent on the internal policies of the providers themselves. This article leads to severe difficulties in handling cases of high-tech or cyber crimes. Therefore, it is necessary to improve the mechanism for international cooperation and domestic legal tools. Currently, there is no mandatory standard system for electronic evidence examination laboratories (ISO-like), and no requirement for periodic certification or verification. The 2015 Criminal Procedure Code does not specify the technical procedures for concluding that an examination has evidentiary value, leading to inconsistent conclusions, conflicting technical viewpoints, and the risk of dependence on internal examination by investigative agencies. Criteria for competency, independence, and quality assurance are needed.

Fifth, there are shortcomings in the protection of personal data and privacy rights when collecting electronic evidence. The 2015 Criminal Procedure Code lacks specific guidance on the limits and percentage of personal data being collected and the confidentiality of sensitive information in evidence gathering; it fails to balance between investigative rights and personal protection. This leads to violations of privacy rights, abuse of power, and the rejection of evidence collected in violation of these rights by the Court. It needs to be aligned with any law on personal data protection or other specialized laws.

Sixth, audio and video recording of interrogations is yet to be mandated and remains incomplete. Clause 6 Article 183 of the 2015 Criminal Procedure Code currently stipulates that recording is only required "when requested" by the suspect or the agency, and is not mandatory in all important cases such as serious or sensitive cases, contradictory statements, or when the accused denies guilt. Therefore, it needs to be expanded to include more situations until the case is resolved and has become legally effective.

Suggestions for Amending and Supplementing Provisions on Electronic Evidence in the 2015 Criminal Procedure Code.

Necessity for the Improvement of Laws Around Electronic Data in Criminal Prosecution

In the context of rapid digital transformation, electronic data (e-data) has become a crucial type of evidence in investigation, prosecution, and trial. However, the 2015 Criminal Procedure Code currently only acknowledges e-data as a source of evidence without establishing complete technical and legal standards for evaluation, verification, and admissibility according to international standards. This leads to a lack of uniformity among prosecuting agencies and difficulties in data examination, comparison, preservation, and verification.

Therefore, there is urgent need for the addition of core definitions and a framework for evaluating e-data, reflecting precedences set by the UNCITRAL Model Law on Electronic Commerce, Budapest Convention, and the legal systems of the EU, USA, Singapore, and Korea.

Supplementation of the Definition of "Electronic Data" Into the Criminal Procedure Code.

A legal definition of e-data must include its technical characteristics, diverse states of existence (dynamic and static data), as well as its backup and recovery capabilities. Internationally, e-data is recognized not only as "data messages" but also the entire information structure created in the digital environment**.**

As such, the author proposes the following definition: "Electronic data is information created, stored, or transmitted by electronic means, including but not limited to: files, system logs, metadata, cloud backups, mirrored copis, system snapshots, data messages, emails, content originating from social media platforms, mobile device data, and data from Internet-connected devices (IoT)."

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

This definition will create a standardized term used across different prosecuting agencies: Police, Procuracy, Courts, and Forensic agencies, in line with other digital law models such as EU eIDAS Regulation, US Federal Rules of Evidence 902(13), 902(14) and expands the scope of data available for collection and analysis (AI logs, blockchain records, IoT telemetry).

Establishing A Criteria for Evaluating the Validity of Electronic Data

Most developed nations (the USA, UK, Singapore, Japan, even Estonia) require that e-data be evaluated following technical and multi-factor legal standards, instead of simply relying on "validity". The new set of criteria must balance between traditional verification standards and the technical characteristics of the digital environment.

As such, the author proposes the following that the following elements must be considered when prosecuting agencies evaluate electronic data. Firstly, the source authenticity of the electronic data must be verified. This refers to the identification of the entity that creates, manages, or controls data, and the reliability of the system and data generation device must be evaluated. Secondly the Method of Creation or Data Generation Process must be identified and whether the data is generated by a system, sensor, IoT device, or by intentional human action; fully describing the technical process of its creation. Next, the metadata, or parameters regarding creation time, modification time, location, system version, device type, and other technical attributes need to be evaluated to verify authenticity and circumstances of origin. Prosecuting agencies must also consider the Hash/checksum of the data, using a standard hashing algorithm (SHA-256 or equivalent) to check integrity and ensure the data is not compromised or manipulated throughout the storage and transmission process. The Chain of Custody of the data must be fully and continuously recorded throughout the process of data collection, sealing, transportation, backup, analysis, and storage, defining the responsibilities of each individual involved. Other factors include the Technical Integrity of the data, to see whether data has been tampered with, altered, or falsified by software, equipment, or digital attack techniques and to determine the reliability of the storage and protection system, and the Reproducibility and Repeatability of the data to ensure data analysis produces consistent results using an independent process in the same technical conditions.

The above suggestions contribute to the creation of a complete, modern, transparent legal framework, in line with international conventions. This is an important step in bringing the Vietnamese Criminal Procedure Code closer to a digital procedural law model, improving the probative value of evidence in a high-tech crime environment and to protect human rights during prosecution.

Improving Article 107 2015 Criminal Procedure Code in Gathering Electronic Data During Prosecution Based on International Standards for Digital Evidence

The rapid rise of electronic data in modern criminal activity calls for the development of consistent legal and technical mechanisms within the criminal procedure system to ensure the integrity, origin, and admissibility of digital evidence. Article 107 of the 2015 Criminal Procedure Code currently only provides general regulations on the seizure of physical evidence but does not establish specific requirements for electronic data, leading to legal loopholes and practical challenges. This article proposes amending Article 107 of the 2015 Criminal Procedure Code to include the standardization of electronic data seizure records forms; mandating the recording of hash/checksum values at the time of seizure; establishment of a mechanism for storing original data on immutable media (WORM/immutable storage). These proposals are compared and benchmarked against international standards from NIST (USA), ENISA (EU), ISO/IEC 27037, and practices in Singapore, Japan, and the United Kingdom.

Necessity to Amend Article 107 2015 Criminal Procedure Code.

In the process of international integration and in light of recent developments, digital data has become a crucial source of evidence in most types of crimes, specifically in areas such as cybercrime, finance, banking, high-tech fraud, and even traditional criminal cases supported by mobile devices, cameras, and social media platforms. The volume, forms, and structures of data are becoming increasingly diverse, creating new challenges regarding preservation, integrity, and repeatability.

Although Article 107 of the 2015 Criminal Procedure Code has acknowledged digital data as a source of evidence and its "analog" nature, it does not fully reflect the specific technical and legal requirements of digital data. This article leads to

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

difficulties in determining authenticity and integrity of data, a lack of consistency among prosecuting agencies such as investigating agencies, prosecutors, courts, and forensic agencies, leading to the risk of the evidence being rejected due to failure to ensure chain-of-custody as well as conflicts between investigative practices and international data preservation standards.

All advanced prosecution systems used by the US, EU, UK, Singapore require a standardized and codified digital evidence collection and storage process to ensure forensic soundness and admissibility.

Suggestions for Amending Article 107 2015 Criminal Procedure Code Towards Modernization are As Follows:

Standardize Forms Used in Seizing Electronic Data, Creating A Mandatory Legal and Technical Standard.

The chain-of-custody form is the first and most important document within the chain-of-custody. In using electronic data as evidence, even minor technical omissions can lead to suspicion of tampering, loss of evidentiary credibility, and ultimately, rejection in court. The ISO/IEC 27037:2012 and the NIST and ENISA frameworks all require standardization of the Chain-of-custody form to ensure consistency and possibility for independent examination.

Therefore, the chain-of-custody form for electronic data must follow a standard national form, including the following elements: Time and location of seizure (accurate timestamp, including time zone); Description of the source device/equipment (model, serial number, firmware, OS version); Software version (operating system related to the data); Subject performing the seizure and witnesses; Technical tools used (imaging tool, forensic kit); Replication method (acquisition method): physical imaging, logical acquisition, live acquisition (if the machine is in operation); The hash (checksum) of each file or data packet at the time of seizure and the storage method after evidence seizure (original and working copy). These are fundamental information for fully recreating the seizure process and proving the validity of the data when authenticated in court.

The Hash(Checksum) of the Data Must be Recorded at the Time of Seizure to Ensure Integrity of Data

The hash/checksum is a unique string of characters generated by a hashing algorithm, allowing verification of whether the data has been altered. International standards (NIST SP 800-107, ACPO Guidelines) require the creation of a hash value before the data leaves the scene. This acts as the "birth certificate" of the electronic evidence.

International hashing algorithms such as SHA-256 or SHA-3 must be applied; The hash value must be included in the chain-of-custody form; every duplicate image of the data must have the same hash value as the original data. Before the data is submitted to the court, the hash value must be authenticated to ensure data integrity and limit alteration, manipulation, or interference and therefore enhancing evidentiary reliability and ensuring the transparency of the chain-of-custody.

The Original Data Must Be Stored on A WORM/Immutable Storage for Preserving Electronic Evidence

Electronic data can be accidentally or intentionally overwritten, manipulated, or destroyed which has led many countries to require original data to be stored on write-once-read-many (WORM) media or storage systems with immutability (cannot be edited after writing). After seizure, the original data must be stored on a device or system with immutability and working copies are used for investigation, analysis, and examination. Access to original data must be strictly controlled and logged. If immutable storage is not possible, the prosecuting authority must apply equivalent protective measures such as combining tamper-evident storage and cryptographic sealing which will prevent any risk of modification or destruction of original data. This process ensures the integrity of original data for court proceedings, especially in cases of evaluation disputes. This is compatible with the legal systems for electronic evidence of Singapore, Japan, and the EU.

Amendment of Article 107 of the Criminal Procedure Code must be centered around 3 main points: standardization of the Chain-of-custody form, mandatory logging of hash values and immutable evidence storage. This is a strategy move to modernize the Vietnamese criminal procedure code in the age of digital technology. This legal framework not only improves the quality of electronic evidence and enhances the confidence of the court in it but also promotes

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

consistency between prosecuting agencies. These amendments also bring Vietnamese laws closer to the international standards set by the NIST, ENISA, ISO and the legal practices of leading countries, creating a foundation for a modern, transparent, and effective digital litigation system.

Improve Regulations on Audio and Video Recording of Interrogations as Stipulated in Article 183 of The 2015 Criminal Procedure Code

Audio and video recording during interrogation is an important mechanism to ensure transparency and objectivity during investigation and also helps prevent risks of coercion and torture, identified by international legal science as inherent risks within the centralized investigative procedural model. As Vietnam further bolsters its drive towards judicial reform with emphasis on the rule of law, judicial principles, and respect for human rights, the need to amend and improve Article 183 of the 2015 Criminal Procedure Code has only become more urgent in order to align itself with international standards and enhance the evidentiary value of testimonies.

Improvements to Article 183 should also expand the scope of cases where audio and video recording with sound is mandatory. Currently, Article 183 of the 2015 Criminal Procedure Code only stipulates mandatory audio and video recording in a few cases which is narrow, lacking standardized criteria, and does not cover situations with a high risk of complaints regarding the voluntary nature of testimony. To overcome this limitation, the following cases should be added:

Firstly: Mandating audio and video recording in particularly serious cases with conflicting evidence, as cases that carry severe punishment or those relying heavily on testimony require stricter oversight. Conventional practices in Japan, South Korea, or some US states show that mandatory video recording improves the validity of litigation and minimizes complaints about the legality of testimony.

Secondly: Mandating recording in interrogations taking place outside of the investigative agency. This form of interrogation poses risks of subjectivity in terms of the conditions, context, and behaviors of the prosecutor. Therefore, it is necessary to make audio and video recording mandatory in cases where the accused are interrogated in hospitals, detention centers, or other locations.

Thirdly: Recording should be done at the request of the defendant or their defense counsel. In principle, the defendant's fundamental rights should be considered a core element of modern legal proceedings. Many advanced legal systems have recognized the right to request video recording and consider it one of the mechanisms protecting the right to remain silent and guaranteeing human and civil rights.

Fourth: Recording should be required when a testimony is considered key evidence that could influence identification of charges. These key testimonies need to be of the highest level of reliability, which is actually included in the UN standards in ensuring fair trials, especially in cases dependent on the identification and description of the defendant or their admission of guilt.

Fifth: Recording should be made mandatory in all cases involving adolescents. The principle of ensuring the “best interests of the child” requires that all prosecutive procedures involving adolescents must be observed through technological means, as is stated in the laws of Germany and the Netherlands, and the recommendations of the Council of Europe.

Sixth: Stricter rules in stopping or interrupting recording should be instated. Currently, pauses in recording are not fully recorded, posing risks of “empty clauses during interrogation.” Therefore, it is nececessary to supplement requirements that should be considered standard practice, such as: pauses must be fully recorded in the report with elements such as time started, time ended, reasons, the person who made the decision, and the witnesses. The reports must be signed by the investigator, the prosecutor (if any), the defendant, and the defense attorney. Archived versions must fully include any pauses and ensure that the video is not edited or cut. Countries like the UK or Japan have very strict regulations on this issue, considering it a key factor in preventing manipulation of interrogation content.

Seventh: Establishing technical standards in recording data security, archive, and integrity. To allow audio and video recordings to become legally binding evidence, it is necessary to create a minimum technical standard that includes: Applying end-to-end encryption and private keys managed by the archiving agency to data; Regulating data access, monitoring access logs/journals; Storing data in immutable storage with original data being stored in a WORM – write

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

once, read many storage system, meaning all copies used during prosecution are purely "working copies"; Creating identification codes and conducting integrity checks. The hash or checksum (SHA-256 for example) must be created right at the end of the interrogation session and be included in the interrogation report. Every later save must include the hash value to ensure data integrity when presented to the court. These requirements are in line with international standards such as NIST SP 800-101 (used by the US) and ENFSI (the EU) in processing electronic data during litigation.

Improving Article 183 of the 2015 Criminal Procedure Code as above would fit current practical requirements as this would help ensure objectivity and allow testimonies to be collected in an environment with technological oversight, reducing suspicions of coercion or illegal intervention to a minimum. It would also improve the value of the evidence as the court could directly assess the attitude and psychological state of the defendant, which would otherwise be impossible to record in a pen-and-paper report. Lastly, this could reduce risks of complaints in legal proceedings, ensuring that audio and video recordings become tools for resolving cases accurately, objectively, quickly, and transparently, saving resources for prosecuting agencies.

Improving International Data Collection Mechanism in Cooperation with Service Providers:

In the real world, the authority to investigate and collect evidence is tied to national territory. However, in the digital environment, data, as traces of criminal activity, is non-territorial, dispersed, and stored under the control of service providers (SPs), most of which are located in the US or EU countries. This gives rise to a "data sovereignty paradox": Vietnamese prosecuting authorities have jurisdiction over criminal acts occurring in Vietnam yet have no actual jurisdiction over evidentiary data stored in the infrastructure of foreign businesses. This raises three structural challenges:

Firstly, there are inherent limitations in the Mutual Legal Assistance in International Law (MLAT) system. This system was designed for the 20th-century litigation model, where evidence was primarily paper documents, witness testimonies, and physical evidence. Meanwhile, electronic data has an extremely short lifespan, with many logs only being stored for 7 to 30 days. The MLAT process, which lasts for months, drastically reduces or even completely erases data accessibility.

Secondly, electronic data access could lead to legal conflicts between national laws and foreign data protection laws. A legitimate request under the 2015 Criminal Procedure Code can easily violate the EU's GDPR or the US Stored Communications Act (SCA). Therefore, service providers (SPs) often refuse to provide data if the request does not meet international standards.

Thirdly, there is a wide gap between the technical competencies between local prosecuting authorities and international SPs. SPs often must conform to high technical standards, while requests from Vietnamese prosecuting authorities sometimes lack appropriate account identifiers, leading to a high failure rate. Given the limitations mentioned above, there is an urgent need to improve cross-border data collection mechanisms to ensure judicial sovereignty in the digital age, while simultaneously protecting the effectiveness of criminal proceedings.

Therefore, it is necessary to create a "preservation order" to mediate conflicts between national and international laws. The preservation order is a mechanism employed in modern international conventions, especially the Budapest Convention and its 2021 Additional Protocol, and is considered a cornerstone in collecting electronic evidence, which is volatile by nature.

It is crucial that an intervention mechanism be instated as soon as possible, one that instead of directly accessing the content, requires the service providers to put the data in a freeze state to await official procedures.

From the aforementioned points, we can conclude that amendments to the 2015 Criminal Procedure Code need to specify the following points: authority to issue the order, such as the investigating agency, the prosecutor's office, or the judge in charge of reviewing the investigation request; scope of application, including all domestic and foreign SPs according to the conflict-of-law friendly principle; a timeframe for preservation of content from 30 to 90 days, in line with international standards. Lastly, amendments must guarantee privacy, limiting orders to only requesting data preservation rather than access or analysis.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

This version of the article will reduce the limitations of the MLAT, eliminating risks of logs being automatically erased and extensive intervention, in turn, preventing violations of international laws. This is the least invasive but most effective method, as it opens up a "safe timeframe clause" to await further litigative procedures.

Emergency data collection protocols should also be established. One of the biggest points of contention in the 2015 Criminal Procedure Code is the lack of an emergency protocol for cross-border electronic data, while cybercrimes continue to take place by the minute, even second, and relevant data can be erased instantly. This article aims to prevent data at risk of immediate deletion, prevent ongoing crimes, as data is a crucial form of evidence for identifying perpetrators, especially in cases involving national security or organized crime.

Therefore, it is necessary to introduce regulations for the collection or temporary saving of data from foreign SPs before completing the MLAT process, followed by mandatory notification and legalization through judicial review. Only after approval by the Court or the Prosecutor's Office can the data be used as evidence to adhere to the principles of necessity, proportionality, and judicial oversight. This is the model that the United States, Canada, Singapore, and the EU have adopted to ensure both effective investigation and privacy protection.

Strengthening inter-agency capacity and standardizing cooperation with SPs via the establishment of a specialized technical unit able to handle requests following specifications from the SP is also necessary. This unit will also be responsible for programming and standardizing metadata to identify the account, operating security mechanisms in data transmission and reception, and serving as the sole point of contact with SPs to avoid information conflicts. As collecting cross-border data is both a highly complex legal and technical activity, the procedural model must also adapt to the forms used in international technical standards, since the lack of "necessary technical information" is often cited as a reason for SPs denying data collection requests.

A standardized set of forms must include the following elements: identifying information (UID, Device ID, Email, IP, URL); requested information (subscriber info vs. metadata vs. content); Timeframe for data retrieval; Clear legal basis; Level of urgency; Hash value and methods for ensuring integrity.

Improving the cross-border data collection mechanism is not just about individual technical modifications, but the restructuring of an entire procedural mindset in the digital age. It strengthens the effectiveness of digital judicial sovereignty, which the state cannot exercise without access to electronic evidence - the central evidence in high-tech crimes. This will also improve the quality of investigation, prosecution, and trial and shortens the time for evidence collection, enhancing the completeness and objectivity of case files, and reduces disputes over data legality. Lastly, this prevents criminal oversight or wrongful convictions.

Cybercriminals often exploit the tardiness of the MLAT process, which is what the newly proposed amendments aim to fix, bringing Vietnamese law in line with international standards. This is a necessary step to help Vietnam strengthen digital justice cooperation, towards joining the Budapest Convention, and raising its prestige in the international judicial system.

Standardizing Electronic Evidence Evaluation, Proposed Laws and Enforcement Mechanisms.
Electronic evidence evaluation (EEE) is a highly specialized scientific and technical task, susceptible to errors caused by inadequate methods, tools, or human capabilities. To ensure the legal validity, reliability, and independence of examination conclusions, it is necessary to establish a legal framework and conduct pilot implementation, including: Mandatory certification requirements for electronic evidence evaluation laboratories following the national referential standard ISO/IEC 17025 (with an appendix applicable to digital evaluation); A list of registered independent evaluation experts with clear entry criteria; Periodic quality assurance testing and external evaluation; Regulations on legal liability and handling of incorrect conclusions due to negligence or intentional acts; Legal recognition of evaluation results based on standards, transparency, and a mechanism to reduce dependence. These proposals are both in line with with international standards and meet practical requirements in the context of rapidly developing science and technology.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Current State, Issue, Risks, and Ongoing Problems:

The high level of specialization and rapid change in technology leads to the advent of various tools and methods for collecting and analyzing digital data (cloud storage, IoT, containers, ephemeral logs). Without updated competency criteria, forensic conclusions are prone to methodological errors or are unreproducible in different contexts.

The lack of uniformity in forensic operating standards also presents an issue. In many forensic systems, the ISO/IEC 17025 standard for laboratories is the foundation for demonstrating competence. However, ISO 17025 needs application guidance for digital forensic activities because some forensic activities require different procedures than standard testing. The lack of a "forensic application manual" could therefore lead to inconsistent practices and applications.

Due to only having a few key forensic laboratories, there is a risk of dependence and conflicts of interest, as prosecuting authorities could become easily reliant on a single source of conclusions; while the lack of transparency and a list of more diverse independent experts reduce objectivity. Studies also point to the risk of flawed conclusions due to human factors and a lack of independent verification and clear legal liability regulations. Currently, there is no unified mechanism for administrative, disciplinary, or civil compensation when forensic conclusions are incorrect due to professional negligence or intentional sabotage, which reduces the incentive to improve evaluation quality. These in turn reduce the likelihood of acceptance of forensic conclusions in court, increasing the risk of wrongful convictions or overlooked convictions, and erode public trust in the digital forensic examination system as a whole.

Legal and Technical Principles to Follow During Standardization

Competence - Technical competence and quality control must be evaluated using objective standards such as ISO/IEC 17025 with an addendum for forensic evaluation.

Transparency & reproducibility – The methods, tools, software version, hash/checksum, chain-of-custody must be recorded in detail in the evaluation report.

Independence - A clear distinction must be made between internal inspections (belonging to the prosecuting authority) and independent inspections (private/registered laboratories).

Continuous Quality Assurance - Proficiency testing, peer review, and external audits must be made mandatory.

Specific Suggestions for Legislation Amendments and Working Criteria

Firstly: Certification of competence for electronic data forensic laboratories must be required. All forensic examination laboratories performing electronic evidence examination for litigation purposes must be accredited according to the national standard compatible with ISO/IEC 17025:2017. This accreditation must include an application document for forensic annex, similar to the NATA/Forensic Science Application Document. Minimum national criteria should include: a quality management system compliant with ISO/IEC 17025; expert profiles (qualifications, specialized training, minimum experience); facilities: forensic equipment, immutable storage environment for digital evidence; standardized procedures: SOPs for acquisition, imaging, analysis, and reporting; traceability: logging, chain-of-custody, hash, and technical records. Certifying and supervising authority should be delegated to the National Accreditation Office (or a specialized agency designated by the Government) to be responsible for assessment and certification, with certifications being valid for 3 to 5 years with periodic audits.

Secondly, there should be a list or registry of independent experts. To achieve this, a national registry should be created - experts wishing to be appointed must register and meet selection criteria (degrees, professional certifications, experience, participation in proficiency testing). Experts should be categorized by field: mobile forensics, network/cloud forensics, malware analysis, IoT forensics, multimedia forensics… to match the specialization of each case. A lottery/rotation mechanism in appointments should be implemented to reduce the risk of abuse of relationships and ensure multiple sources of expert opinions.

Thirdly: Periodic quality assurance and proficiency testing should be conducted. Mandatory participation in proficiency testing, either annually or biennially, as organized or accredited by the accreditation body should serve as the basis for maintaining certification. All laboratories are to be subjected to mandatory periodic peer review and external audits. The assessment report must be archived and partially made public (e.g., non-conformity survival rate, proficiency results).

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Fourthly: There should be mechanisms for ensuring accountability and punishments for errors during evaluation, classified into levels such as: Negligence due to procedural errors; Serious violations due to incompetence; Intentional sabotage/forged documents. For procedural negligence, personnel should be subjected to mandatory training and SOP review and a public statement should be made to correct mistakes; For serious violations, certificates are to be withdrawn and the offending personnel be removed from the registry and subjected to administrative disciplinary actions; For intentional sabotage, offenders are to undergo criminal prosecution and civil compensation for any damages. Should there be disputes or suspicions with the forensic results, an independent re-examination based on the forensic master copy performed by a third party is to be conducted.

Fifth: The legal validity of evaluation conclusions must be guaranteed. The court will only accept an expert's conclusion if: The laboratory and experts are properly certified; the report complies with standard templates, listing SOPs, tool versions, hash/checksum, and chain-of-custody; has undergone proficiency testing within the past 24 months; and there is no conflict of interest. Defendants and parties involved have the right to request independent expert examination and re-examination using the forensic master copy; the law must clearly specify costs and access rights.

The aforementioned amendments are meant to protect human rights and fair prosecution. When forensic results lack credibility, rights to fair trial will also be affected, and standardization will also help reduce the risk of wrongful conviction and coercion. This will also help Vietnam keep up with the rapid pace of technological development – only with a constantly updated system of experimentation and proficiency testing will forensic methods keep up to date with new changes in storage, encryption, and anonymization methods. Labs that are certified following ISO/IEC 17025 standards and take part in international proficiency testing will have an easier time during cross-border MLAT and data preservation requests. Lastly, this will also be cost-effective in the long run, with reductions to risks of incorrect data handling, extended disputes, re-trials – all of which are more expensive than investing in a system for quality assurance and training.

Specific Suggestions

Firstly, supplement the following clause into the relevant law "All forensic examination laboratories performing electronic evidence evaluation for litigation purposes must be accredited according to the ISO/IEC 17025 criteria, with an appendix applicable to digital forensic examination; a registry of independent forensic experts must be created and managed jointly by the prosecuting authorities, including the Ministry of Public Security, the Supreme People's Procuracy, and the Supreme People's Court."

Secondly, the following clause should be added regarding quality control: "Forensic laboratories and experts must participate in proficiency testing at least once a year; failure to participate or consistently receiving poor scores will result in suspension of certification

Thirdly, the following clause should be added in terms of accountability: "Errors are to be classified according to severity and offenders are to be subjected to administrative, disciplinary, or criminal punishments accordingly; the rights to request independent evaluation must be secured."

Fourthly, in terms of report verification: " Evaluation reports must list in details the SOP, tools and versions, hash/checksum, chain-of-custody, and proficiency status reference."

Improving Private Data Protection in Gathering and Utilizing Electronic Evidence

As personal data becomes a "strategic resource" in both the public and private sector, the usage of private data as a form of evidence during criminal procedures poses urgent questions regarding the balance between the State's investigative rights and the privacy rights of individuals. From a theoretical perspective, this is a structural tension between the State's obligation to ensure security and order, and the obligation to protect the inviolable right to privacy and the right to personal confidentiality, as enshrined in Article 21 of the 2013 Constitution and further specified in Decree 13/2023/ND-CP on the protection of personal data.

This conflict only becomes more severe as electronic evidence is often entangled with a large volume of data outside the scope of investigation, including sensitive information (health, personal life, religion, social relationships, real-time location data) that is not directly related to the crime but is found within the same data source.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

The current state of Vietnamese law exposes a large gap in the criminal procedure code in terms of standards for gathering, filtering, limitations of usage and legal liability for disclosing or misusing personal data collected during investigations. This creates a risk of conflict of laws between the Criminal Procedure Code, the Cybersecurity Law, the Law on Network Information Security, and Decree 13/2023/ND-CP.

Therefore, amendments to the Criminal Procedure Code are necessary in establishing a personal data protection mechanism in line with international standards set by the EU's GDPR, OECD Privacy Guidelines, 2001 Budapest Convention, as well as legislative conventions set by Singapore, Japan, and Korea for the virtual space.

Amendments to the Criminal Procedure Code need to comply with the principle of "least intrusive means", meaning only data directly related to the investigation are collected, while bulk collection is to be prohibited. Data beyond the necessary timeframe and space are not to be aggregated, while specificity of the account, device, log, or timeline must be acquired, with every data collection request being documented and supervised by the Prosecutor's Office or the Court. This approach is consistent with EU standards, where the Courts require proportionality and necessity for all data processing activities in the criminal field.

Data Minimization & Filtering Before Being Used in Prosecution

A notable difficulty in current legal practice is that when seizing an electronic device or requesting data from service providers, investigators often receive large volumes of data, including: browsing history, images, videos, personal documents, location data, medical data, financial data, and private communications unrelated to the case. Without mandatory regulations on data filtering, there could be significant risks of violation of privacy, threatening the legitimacy of the evidence gathering process.

Therefore, amendments should be made to limit data gathering to only data related to criminal activities to be used as incriminating evidence. Irrelevant data must be filtered, censored, encrypted, or removed from the case file. This filtering must be performed by an independent technical unit (or electronic forensic expert), minimizing unauthorized access by investigators. All filtering operations must be documented with a technical report and hash value to ensure integrity. This approach is similar to the digital investigation models used in Germany, the Netherlands, and Canada when dealing with data overflow.

Limiting Usage of Data to the Purpose of the Investigation Without Further Speculation or Extension:

A serious problem in digital investigations is function creep – or usage of gathered data beyond its original purpose. Therefore, the Criminal Procedure Code needs to clearly stipulate that collected personal data is to only be used for the specific criminal case, strictly prohibiting sharing, exchanging, or using data for administrative, tax, or other public security purposes without a judicial order. Any expansion of the scope of use must be approved by the Court via judicial authorization. This is considered a minimum standard for privacy protection in criminal justice among OECD countries

Currently, the Vietnamese legal system does not clearly define the standards for data confidentiality in criminal investigations, leading to leaks of personal data of suspects, victims, and witnesses; data circulating on social media; unauthorized copying and sharing of investigation files; and the inability to determine individual responsibility when data is misused.

To address this problem, the Criminal Procedure Code needs to clearly outline the personal responsibility of investigators, prosecutors, experts, and technical staff are held accountable in the event of a data leak or misuse; distinguishing between unintentional errors, negligence, and intentional sabotage; applying disciplinary, compensatory, and criminal liability simultaneously depending on the severity of the violation. This is currently a weak point in Vietnamese law that poses many legal risks, especially in the context of cross-border data collection, where service providers require information security guarantees before providing data.

The aforementioned amendments are vital due to the increasingly sensitive and detailed nature of personal data, reflecting the entire lives of individuals, making it easy to be abused without proper regulation. Wanton data aggregation has become a prominent trned in hi-tech cases in Vietnam due to the current limitations in its legal framework. With international service providers heightening data protection requirements, should

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Vietnam fail to meet international standards, the likelihood that they will cooperate will be drastically reduced. Faith in the judicial system depends on the protection of privacy rights, especially the privacy of those uninvolved in the case yet have their data collected anyway. The protection of private data is an element of human rights, protected by the Constitution and must be specified in the Criminal Procedure Code. As such, supplementing mechanisms for the protection of private data in the Criminal Procedure Code is not only a technical requirement but a structural one, balancing State power and human rights in modern investigative procedures.

CONCLUSION

The accelerating digitalization of contemporary society has fundamentally reshaped evidentiary practices in criminal justice, positioning electronic evidence as an indispensable component of investigative and adjudicative processes. While the 2015 Criminal Procedure Code of Vietnam represents a significant legislative milestone by formally recognizing electronic evidence as an independent evidentiary category, this recognition remains primarily normative and lacks the operational depth required to address the complex technical and legal challenges inherent in digital data handling.

The analysis reveals that Vietnam's current framework exhibits substantial deficiencies across all key stages of evidentiary management—collection, preservation, forensic examination, authentication, and judicial evaluation. These shortcomings stem from the absence of harmonized technical standards, insufficient digital forensic capacity, fragmented inter-agency coordination, and a limited legal mechanism for accessing cross-border data. Moreover, the increasing reliance on intrusive investigative techniques raises concerns regarding proportionality, legality, and the protection of privacy and personal data, especially in light of Vietnam's constitutional commitments and international human rights obligations.

To ensure that electronic evidence can be reliably, lawfully, and effectively integrated into the criminal process, Vietnam must undertake a comprehensive reform agenda. This includes: establishing a detailed and technologically neutral legal framework**,** incorporating clear standards for authenticity, integrity, chain-of-custody, and admissibility; strengthening institutional capacity**,** particularly through investment in accredited digital forensic laboratories, specialized training for investigative authorities, and standardized procedural protocols; and enhancing international alignment and cooperation, adopting best practices from UNODC, NIST, and the Budapest Convention, and improving mechanisms for lawful cross-border data acquisition.

Ultimately, the modernization of Vietnam's electronic evidence regime is not merely a technical adjustment but a structural imperative to ensure procedural fairness, evidentiary reliability, and the effective administration of justice in the digital era. Achieving this alignment will advance Vietnam's legal harmonization with global standards, reinforce judicial credibility, and position the criminal justice system to respond proactively to the evolving landscape of cyber-enabled crimes.

REFERENCES

1. Casey, E. *Digital Evidence and Computer Crime.* 4th ed. Academic Press, 2019.
2. Central Committee of the Communist Party. *Constitution of the Socialist Republic of Vietnam 2013.* National Political Publishing House, 2013.
3. Council of Europe. *Budapest Convention on Cybercrime.* Council of Europe, 2001.
4. Council of Europe. *Guidelines on Electronic Evidence.* Council of Europe, 2004.
5. Hoang, V. "Electronic Evidence and Legal Issues in Vietnamese Criminal Procedures." *Journal of Prosecution* 7 (2021): 15–22.
6. International Organization for Standardization (ISO). *ISO/IEC 27041: Guidance on Assuring Suitability and Adequacy of Incident Investigation Methods.* ISO, 2015.
7. International Organization for Standardization (ISO). *ISO/IEC 27037: Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.* ISO, 2019.
8. Kerr, O. S. "The Fourth Amendment and the Global Internet." *Stanford Law Review* 70.2 (2018): 287–336.
9. Mason, S., and Seng, D., eds. *Electronic Evidence.* 4th ed. Institute of Advanced Legal Studies, 2017.
10. Ministry of Public Security – Ministry of National Defense – Ministry of Information and Communications – Supreme People's Procuracy – Supreme People's Court. *Joint Circular 01/2020 on the Procedures for Collecting, Preserving, and Using Electronic Data in Criminal Proceedings.* 2020.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

11. Ministry of Public Security. *Circular 119/2022/TT-BCA on the Process of Ensuring Cybersecurity and Processing Digital Data.* 2022.
12. Moore, T. "Authenticity and Reliability of Digital Evidence: A Comparative Analysis." *International Journal of Cybersecurity Law* 3.1 (2021): 45–72.
13. National Assembly of the Socialist Republic of Vietnam. *Criminal Procedure Code.* National Political Publishing House, 2015.
14. National Assembly of the Socialist Republic of Vietnam. *Criminal Code.* National Political Publishing House, 2015.
15. Ngo, V. H. "Issues in the Validity of Electronic Data in Investigating High-tech Crimes." *Vietnam Journal of Forensic Science* 4 (2021): 55–67.
16. Nguyen, N. C. "Electronic Evidence Collection and Evaluation Following the 2015 Criminal Procedure Code." *People's Court Journal* 18 (2020): 7–15.
17. National Institute of Standards and Technology (NIST). *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response.* 2012.
18. National Institute of Standards and Technology (NIST). *NISTIR 8286: Evidence Management in Digital Investigations.* 2020.
19. Reith, M., Carr, C., and Gunsch, G. "An Examination of Digital Forensic Models." *International Journal of Digital Evidence* 1.3 (2002): 1–12.
20. Standing Committee of the National Assembly. *Cybersecurity Law.* 2015.
21. Supreme People's Court. *Collection of Legal Precedents in Vietnam.* Vol. IV. Vietnam Judicial Publishing House, 2020.
22. Supreme People's Court. *Precedent No. 42/2021/AL on the Evidentiary Value of Electronic Data in Criminal Procedures.* 2021.
23. Supreme People's Court. *Resolution 110/2017/UBTVQH on the Process of Collecting, Evaluating, and Using Electronic Data in Criminal Proceedings.* 2017.
24. Tran, V. N. "Improving Laws on Electronic Evidence in Criminal Procedures." *Journal of State and Law* 6 (2022): 33–45.
25. United Nations Office on Drugs and Crime (UNODC). *Comprehensive Study on Cybercrime.* UNODC, 2015.
26. United Nations Office on Drugs and Crime (UNODC). *Handbook on Electronic Evidence in Criminal Justice Systems.* United Nations, 2021.
27. Vietnamese Government. *Decree 72/2013/ND-CP on the Management, Provision, and Use of Internet Services and Online Information.* 2013.
28. Vietnamese Government. *Decree 53/2018/ND-CP Detailing Some Articles of the Law on Cybersecurity.* 2018.
29. Vietnamese Government. *Decree 130/2020/ND-CP on Digital Signatures and Digital Signature Authentication Services.* 2020.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Thien, N. T. and Phuong, N. H. " Electronic Evidence in Vietnam's Criminal Procedure Code Current State and Suggestions for Improvement " *Sarcouncil journal of Arts humanities and social sciences* 5.2 (2026): pp 12-23.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher