



CADERNOS DE DEREITO ACTUAL

www.cadernosdedereitoactual.es

© *Cadernos de Direito Actual* Nº 33. Núm. Ordinario (2026), pp. 463-502

·ISSN 2340-860X - ·ISSNe 2386-5229

Digital evidence in Vietnamese criminal proceedings: Legal framework and adjudicative practice

Nguyen Tat Thanh¹

Van Lang University

Nguyen Duy Dzong^{2,*}

Nguyen Tat Thanh University

Summary: 1. Introduction. 2. Theoretical framework and research methodology. 2.1 Theoretical framework. 2.2 Research methodology. 3. Legal framework on electronic evidence in Vietnamese criminal proceedings. 3.1 Concept of electronic evidence. 3.2 Characteristics of electronic evidence under the Vietnamese legal framework. 3.3 Deficiencies in Vietnam's legal framework on electronic evidence. 3.4 Data protection and evidence collection: A broad exemption without conditions. 4. Electronic evidence in judicial practice from a systematic analysis of twenty judgments. 4.1 Classification: The mode by which the data came into existence. 4.2 Class (i): Data generated by a system. 4.3 Class (ii): Content composed by a person and stored electronically. 4.4 Class (iii): Artefacts created by the investigation itself. 4.5 Two cases at the boundary. 4.6 Observations on the judgment data. 5. Comparative perspectives on the deficiencies identified. 5.1 Authentication: From proof in each case to presumption. 5.2 Chain of custody: Standards that Vietnam has adopted but not required. 5.3 Cross-border access: From aspiration to obligation. 5.4 Pairing power with condition. 6. Recommendations. 6.1 Consolidating and completing Articles 107 and 196 (second tier: Amendment of the code). 6.2 A mandatory chain of custody and hash verification (first tier: Subordinate instrument). 6.3 A framework for cross-border access to data (third tier: Treaty implementation). 6.4 Conditions on the use of personal data as criminal evidence (second tier: Amendment of the Code). 6.5 Technical capacity and mandatory expert involvement (first and second tiers). 6.6 Institutional framework

¹ Doctor in Law, Lecturer of the Faculty of Law, Van Lang University, 69/68 Dang Thuy Tram Street, Binh Loi Trung Ward, Ho Chi Minh City, Vietnam. ORCID: 0000-0003-1476-8320. E-mail: thanh.nt@vlu.edu.vn

² Master in Law, Lecturer of the Faculty of Law – Nguyen Tat Thanh University, Ho Chi Minh City, Vietnam. ORCID: 0000-0001-8091-2103. E-mail: nddung@ntt.edu.vn (corresponding author).

for international cooperation (third tier). 6.7 Difficulties of implementation. 7. Conclusion. 8. References.

Abstract: This article examines the Vietnamese legal framework on electronic evidence under the 2015 Criminal Procedure Code (CPC 2015) and its application in adjudication by analyzing the theory of admissibility of evidence and the chain-of-custody doctrine and systematically reviewing of twenty criminal judgments delivered by Vietnamese courts between 2017 and 2025. It advances three arguments. Firstly, the conception of electronic evidence in the CPC 2015 is established, but the Code contains no codified requirement of a chain of custody for electronic data, and none of the twenty judgments articulates any basis for the authenticity or integrity of that data beyond the defendant's admissions. Secondly, electronic evidence now operates well beyond the high-technology offences on which practice and scholarship initially focused, appearing routinely in ordinary criminal cases. Finally, the Law on Personal Data Protection 2025 exempts criminal investigations from the consent requirement but delegates the applicable conditions to procedural law, where none currently exist - a gap that Vietnam's ratification of the United Nations Convention against Cybercrime in April 2026 now obliges it to close. The article proposes six reforms, focusing on procedural codification, chain-of-custody rules and cross-border access to data.

Keywords: Digital Evidence, Criminal Procedure, Vietnam, Chain of Custody, Comparative Law

1. Introduction

Technology has transformed the process of discovering, collecting, and processing evidence in the field of justice. Information disseminated on social media platforms, financial transactions recorded on bank servers, or video footage from surveillance cameras have become sources of evidence in many criminal cases. In his research conducted in Vietnam, Nguyen Van Dien shows that the use of the above-mentioned information is not limited to the prosecution of cybercrime, but is also increasingly employed to prove other offences, ranging from violent crimes and property crimes, to public order violations and political offences.³

By its nature, electronic data is intangible, easily copied, modified, or destroyed, and relies on technical means for storage and retrieval. Therefore, establishing a chain of evidence that is, a complete record of the subject, time, and manner in which electronic evidence is collected, stored, and evaluated is essential to ensure its integrity and reliability in court proceedings. As Bachmaier and Queralt have observed, the effectiveness of the trial stage depends largely on whether the electronic evidence was collected in full and on whether the rules governing its use were followed in the preceding stages.⁴

Furthermore, electronic data today is inherently cross-border in nature. It may be stored on servers located in different jurisdictions, which can generate jurisdiction disputes over electronic data processing and other legal disparities in handling cases involving this type of data.

For this reason, the use of electronic evidence, as well as the sequence in which this type of evidence is used to prove offences in Vietnam, is currently not uniform

³ NGUYỄN VĂN ĐIỀN. "Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015" [Electronic evidence in the 2015 Criminal Procedure Code]. Ministry of Justice, 17 June 2019. Available at: <https://moj.gov.vn/qt/tintuc/Pages/nghien-cuu-trao-doi.aspx?ItemID=2455> (accessed on 25 March 2026).

⁴ BACHMAIER WINTER, L. and QUERALT, J. *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge: Cambridge University Press. 2018. Available at: <https://doi.org/10.1017/9781009049771> (accessed on 25 March 2026).

across localities. Moreover, matters relating to electronic evidence, such as the concept of electronic evidence and the procedures for using such evidence, are being understood and operated according to different models in different countries. A comparative study by Kalancha et al. suggests that in common law systems, electronic evidence must meet very specific authentication requirements related to data integrity and the reliability of the system that generated that data, while many civil law countries are still in the process of developing equivalent frameworks.⁵

Vietnam is no exception to this trend. The choice of digital transformation as a national development strategy is crucial.⁶ This has led to two consequences: an increase in crimes committed using technology, and a growing reliance of investigative activities on digital data to prosecute those crimes.⁷ In that context, the CPC 2015 marks a turning point in the Vietnamese legal system by formally recognizing "electronic data" as a source of evidence in criminal proceedings in Article 87(1)(c).⁸ According to the view of some Vietnamese scholars, this legal milestone has narrowed the long standing gap between substantive criminal law which has criminalized offences in the field of information technology and telecommunications since 1999 and procedural law, which has lacked a corresponding evidentiary basis to prove those criminal acts.^{9,10,11} However, the provisions of the CPC 2015 stop at setting out a definition of electronic data and do not include any further rules describing in detail the specific features of the processes of collecting, preserving and using this special type of evidence.

Vietnamese scholarship on electronic evidence is now substantial, and it falls into four identifiable strands. Setting them out is necessary to state precisely what this article contributes and what it does not claim to offer.

The first strand concerns the concept itself. Nguyen Van Dien, Nguyen Duc Hanh, Pham Cong Tung and Bui Hai Hieu have examined the recognition of electronic data as an independent source of evidence and the relationship between the statutory

⁵ KALANCHI, I., BOZHYK, V., MUZYCHENKO, O. and VATSIYK, V. "Digital evidence in comparative criminal procedure: International experience and the practice of judicial review". *TPM - Testing, Psychometrics, Methodology in Applied Psychology*, v. 32, n. S2, 2025, pp. 34-46. Available at: <https://tpmap.org/submission/index.php/tpm/article/view/150> (accessed on 15 April 2026).

⁶ VNS. *Vietnam strives to facilitate digital transformation*. Vietnam News, 2023. Available at: <https://vietnamnews.vn/economy/1549806/viet-nam-strives-to-facilitate-digital-transformation.html> (accessed on 15 March 2026).

⁷ PHAM MINH ĐÔ, "Improving criminal law on high-tech crimes in the context of digital transformation in Vietnam". *Legal Affairs Journal*, 2023. Available at: <https://phaply.net.vn/hoan-thien-phap-luat-hinh-su-ve-toi-pham-cong-nghe-cao-trong-boi-can-h-chuyen-doi-so-tai-viet-nam-a260189.html> (accessed on 20 March 2026).

⁸ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Available at: <https://www.wipo.int/wipolex/en/text/585372> (accessed on 20 April 2026).

⁹ CAO ANH ĐỨC and NGÔ THỊ BÍCH THU. "Measures for collecting, transforming and using electronic evidence in high-tech crime cases". *Journal of Procuracy*, 2020. Available at: <https://kiemsat.vn/bien-phap-thu-thap-chuyen-hoa-su-dung-chung-cu-dien-tu-trong-vu-an-su-dung-cong-nghe-cao-62958.html> (accessed on 15 March 2026).

¹⁰ NGUYỄN PHI HÙNG. "Collection of electronic evidence in criminal procedure: Some shortcomings and recommendations for improvement". *Journal of Democracy and Law*, 2021. Available at: <https://danchuphapluat.vn/thu-thap-chung-cu-dien-tu-trong-to-tung-hinh-su-mot-so-bat-cap-va-kien-nghi-hoan-thien-8648-8648.html> (accessed on 25 April 2026).

¹¹ NGUYỄN ĐỨC HẠNH. "Provisions on electronic evidence in procedural law and the Law on Electronic Transactions". *People's Court Journal*, 2021. Available at: <https://tapchitoaan.vn/quy-dinh-ve-chung-cu-dien-tu-trong-phap-luat-to-tung-va-luat-giao-dich-dien-tu8114.html> (accessed on 05 March 2026).

term "electronic data" and the doctrinal term "electronic evidence".^{12,13,14,15,16} It is settled in this literature that the recognition itself was a necessary and coherent step. What remains contested is whether electronic evidence constitutes a distinct category of evidence or ordinary evidence in a distinct medium. This article does not reopen that debate; it treats the question as one of procedural regulation rather than of evidentiary taxonomy.

A second strand addresses the mechanics of collection. Le Nguyen Thanh has analysed the collection of electronic evidence in Vietnamese criminal proceedings in detail, including the role of forensic expertise and the technical capacity of the investigating authorities; Nguyen Phi Hung, Ngo Xuan Khang and Tran Ngoc Minh and Dang Minh Cuong have identified the drafting conflict between Articles 107 and 196 and the absence of technical standards for copying and recovery;^{17,18,19,20} Cao Anh Duc and Ngo Thi Bich Thu, and Pham Minh Do, have examined collection practice in high-technology cases.^{21,22} The recommendations made below on technical capacity, the involvement of forensic experts and the documentation of collection are therefore not novel. They are advanced as consolidation of an existing consensus, and what this article contributes is evidence, drawn from adjudication, of how far that consensus remains from implementation.

A third strand concerns authentication and integrity. Nguyen Thanh Minh Chanh has examined the authentication of electronic evidence derived from digital transactions and communications; Truong Thanh Thao Nguyen has addressed related questions of evidentiary reliability; and Duong Quynh Hoa has examined blockchain-based storage of electronic evidence, drawing on Chinese experience.^{23,24,25} This

¹² NGUYỄN VĂN ĐIỂN. "Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015" [Electronic evidence in the 2015 Criminal Procedure Code]. Ministry of Justice, 17 June 2019. Ibid.

¹³ NGUYỄN ĐỨC HẠNH. "Provisions on electronic evidence in procedural law and the Law on Electronic Transactions". 2021. Ibid.

¹⁴ NGUYỄN ĐỨC HẠNH. "Electronic data and electronic evidence". *Journal of Procuratorial Science, Special Issue 1, 2019*, pp. 37-42. Available at: <https://vjol.info.vn/tks/article/view/46336/37588> (accessed on 05 March 2026).

¹⁵ PHẠM CÔNG TÙNG, "Improving the provisions on electronic data in criminal procedure", *Protection of Law newspaper (Kiểm sát)*, 2022. Available at: <https://kiemsat.vn/hoan-thien-quy-dinh-ve-du-lieu-dien-tu-trong-to-tung-hinh-su-64101.html> (accessed on 05 March 2026).

¹⁶ BUI HẢI HIẾU. *On some aspects of electronic data in criminal procedure*. *Protection of Law newspaper (Kiểm sát)*, 2021. Available at: <https://baovephapluat.vn/cai-cach-tu-phap/dien-dan/ban-ve-mot-so-khia-canh-cua-du-lieu-dien-tu-trong-to-tung-hinh-su-116824.html> (accessed on 20 March 2026).

¹⁷ LE NGUYEN THANH. "Electronic evidence collection in Vietnamese criminal proceedings". *Vietnamese Journal of Legal Science*, vol. 3, no. 175, 2024, pp. 51-62. Available at: <https://doi.org/10.70236/tckhplvn.70> (accessed on 20 April 2026).

¹⁸ NGUYỄN PHI HÙNG. "Collection of electronic evidence in criminal procedure: Some shortcomings and recommendations for improvement". 2021. Ibid.

¹⁹ NGÔ XUÂN KHANG. "Identifying legal bottlenecks on electronic data and recommendations for improvement". *People's Court Journal*, 2023. Available at: <https://tapchitoaan.vn/nhan-dien-cac-diem-nghen-phap-ly-ve-du-lieu-dien-tu-va-kien-nghi-hoan-thien15042.html> (accessed on 05 March 2026).

²⁰ TRẦN NGỌC MINH & ĐẶNG MINH CƯỜNG. "Improving the law on investigative measures under the criminal procedure code 2015". *Protection of Law newspaper (Kiểm sát)*, 2023. Available at: <https://kiemsat.vn/hoan-thien-phap-luat-ve-cac-bien-phap-dieu-tra-theo-quy-dinh-cua-bo-luat-to-tung-hinh-su-nam-2015-65859.html> (accessed on 05 March 2026).

²¹ CAO ANH ĐỨC and NGÔ THỊ BÍCH THU. "Measures for collecting, transforming and using electronic evidence in high-tech crime cases". 2020. Ibid.

²² PHẠM MINH ĐÔ, "Improving criminal law on high-tech crimes in the context of digital transformation in Vietnam". 2023. Ibid.

²³ NGUYEN THANH MINH CHANH. "Authentication of electronic evidence derived from digital transactions and communications". *Futurity Proceedings*, n. 5, 2025, pp. 302-309

literature establishes that authentication is the weak point of the Vietnamese regime. What it has not done is identify the procedural device by which authentication might be operationalised within a codified system.

A fourth strand connects electronic evidence to privacy and to international frameworks. Dinh The Hung has traced the legal framework of electronic evidence from the Budapest Convention to Vietnamese domestic legislation and has argued that fairness and the protection of private life are constitutive principles of that framework rather than external constraints upon it.²⁶ The analysis of data protection below builds directly on that argument.

However, the current literature exhibits three notable limitations that remain unaddressed. First of all, they did examine what the law provides and what investigative practice is reported to do, but no study has figured out the provenance and integrity of electronic data, or treated judicial reasoning as the object of analysis. Second, no study has mapped the stages of the chain of custody against the specific provisions of the CPC 2015, nor noted that the Code subjects the covert collection of electronic data and the seizure of physical correspondence to procuratorial approval while leaving overt extraction from a suspect's device unconditioned. Third, and decisively, all of the work cited above predates the Law on Personal Data Protection 2025, the amendments made by Law No. 99/2025/QH15, and Vietnam's ratification of the United Nations Convention against Cybercrime in April 2026. The legal setting in which these questions must now be answered did not exist when that earlier scholarship was published.

This article aims to fill those above-mentioned gaps. In the authors' view, the Vietnamese legal framework although conceptually solid at its foundation, nonetheless contains shortcomings that are generating practical consequences which can be observed in the course of adjudication. These consequences can be properly understood only through the dual lens of evidentiary admissibility theory and the chain-of-custody doctrine and remedied only through legislative reforms guided by international experience.

To clarify the research objects mentioned above, the following core issues have been identified for the purposes of this study:

- Analyze the Vietnamese legal framework on electronic evidence, identifying the strengths and the serious gaps in the provisions of the CPC 2015.
- Analyze and systematically assess Vietnamese criminal judgments, in which electronic evidence is classified into four functional groups to highlight its role in the practical operation of criminal procedure in Vietnam as well as the limitations in the use of this type of evidence in court.
- Compare and analyze the legal provisions on electronic evidence under the Budapest Convention, the law of the European Union, and several Asian countries that share certain similarities with Vietnamese law, namely Singapore and Malaysia.

(*International Conference on Economic Sciences and Management in the Changing World*). Available at: <https://doi.org/10.5281/zenodo.17926441> (accessed on 20 March 2026).

²⁴ TRƯƠNG THÀNH THẢO NGUYỄN. "Digital evidence in criminal procedure: Legal challenges and solutions in Vietnam". *Journal of Science and Technology (Binh Duong University)*, vol. 8, no. 1, 2025. Available at: <https://jst.bdu.edu.vn/index.php/jst/article/view/297> (accessed on 05 March 2026).

²⁵ DUONG QUYNH HOA. "Electronic evidence and electronic evidence storage using Blockchain technology: China's experience and implications for Vietnam". *Vietnam Journal of Social Sciences*, 2024. Available at: <https://vjol.info.vn/khxbvn/article/view/108622> (accessed on 05 March 2026).

²⁶ DINH THE HUNG. "The legal framework of electronic evidence in vietnamese criminal procedure: From the budapest convention to domestic legislation". *Access to Justice in Eastern Europe*, vol. 8, no. 4, 2025, pp. 301-339. Available at: <https://doi.org/10.33327/AJEE-18-8.4-a000142> (accessed on 05 March 2026).

Building on these observations, this article examines these issues through the theoretical framework of evidence admissibility and the doctrine of chain of custody. Furthermore, the findings and proposals offered herein aim to refine Vietnam's legal framework on electronic evidence, thereby enhancing its efficacy in criminal proceedings.

2. Theoretical framework and research methodology

2.1 Theoretical framework

The article uses two complementary theoretical frameworks as the basis for analysis with a view to assessing both the normative completeness of the Vietnamese legal framework and the application of those provisions in trial practice.

First is the theory of admissibility of evidence. In its widely accepted form, this theory holds that electronic evidence must satisfy three interconnected conditions to carry legal weight in criminal procedure, namely authenticity, integrity and relevance. Authenticity requires demonstrating that the data are what they are claimed to be, that is, that the data records originate from the source attributed to them and have not been falsified²⁷. Integrity requires demonstrating that the data have been preserved without alteration from the time they were created or collected until the time they are presented in court.²⁸ Relevance, in the procedural sense, requires that the data relate to the facts that need to be proved in the case. These three conditions are not specific to any particular legal system. They are widely recognized, albeit expressed in different forms.^{29,30,31} It should also be noted that this theory is precisely the foundation of the criteria for admitting evidence set out in Article 99(3) of the CPC 2015. Yet the current provisions lack the necessary procedural mechanisms to operationalize those criteria. The theoretical contribution of the article lies in developing the connection between this theory and the concrete practice of collecting, examining and assessing evidence as revealed through the twenty judgments gathered.

The second theoretical framework is the doctrine of chain of custody of evidence. In the context of electronic evidence, this doctrine refers to a complete and uninterrupted record of the collection, handling and preservation of electronic data as well as electronic devices from the time of seizure until their presentation in court.³² It can be seen that the chain of custody of evidence is not merely a simple

²⁷ CASEY, E. *Digital evidence and computer crime: Forensic science, computers and the internet*, 3rd ed. Waltham (MA): Academic Press, 2011, pp. 7-12. Available at: <https://archive.org/details/digitalevidencece0003case> (accessed on 25 March 2026).

²⁸ NARASIMHAN, P. and KALA, N. "Ensuring the integrity of digital evidence: The role of the chain of custody in digital forensics". *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, v. 10, n. 6, 2024, pp. 2438-2450. Available at: <https://doi.org/10.32628/CSEIT2410612443> (accessed on 25 April 2026).

²⁹ KALANCHA, I., BOZHYK, V., MUZYCHENKO, O. and VATSIYK, V. "Digital evidence in comparative criminal procedure: International experience and the practice of judicial review". *TPM - Testing, Psychometrics, Methodology in Applied Psychology*. 2025. Ibid.

³⁰ UK PARLIAMENT. Police and Criminal Evidence Act 1984 (PACE), London, 1984, Code B. Available at: <https://www.gov.uk/government/publications/pace-code-b-2023> (accessed on 05 March 2026).

³¹ UNITED STATES CONGRESS. Federal Rules of Evidence, Washington DC, 1975 (Pub. L. 93-595, as amended), Rules 901-902. Available at: https://www.law.cornell.edu/rules/fre/rule_901 and https://www.law.cornell.edu/rules/fre/rule_902 (accessed on 05 March 2026).

³² GIOVA, G. "Improving chain of custody in forensic investigation of electronic digital systems". *International Journal of Computer Science and Network Security (IJCSNS)*, v. 11, n. 1, 2011, pp. 1-9. Available at: http://paper.ijcsns.org/07_book/201101/20110101.pdf (accessed on 25 April 2026).

procedural formality but a procedural mechanism through which the authenticity and integrity of electronic evidence are demonstrated before the adjudicator. For example, the ISO/IEC 27037:2012 standard provides that the identification, collection, acquisition and preservation of digital evidence must follow documented procedures that allow each step to be checked and verified.³³ In the authors' view, the most serious shortcoming in the Vietnamese legal framework lies not in the Code's silence on the handling of seized items, but in its failure to establish an integrated and traceable chain of custody covering every stage at which electronic data are handled. It is this structural deficiency that the legislature should prioritise remedying.

2.2 Research methodology

The article adopts three research methods that complement one another. The primary method is academic legal analysis which involves the systematic examination and critical evaluation of Vietnamese legal normative documents, including the CPC 2015 as amended, most recently by Law No. 99/2025/QH15 in force from 1 July 2025,³⁴ the Vietnam 2023 Law on Electronic Transactions, the Law on Personal Data Protection 2025 and Decree No. 356/2025/ND-CP. To accurately contextualize the examined judgments, this study also incorporates Decree No. 13/2023/ND-CP - the regulatory regime in force when those judgments were released - alongside supporting secondary legislation and official guidance documents.

The second method is comparative legal analysis, drawing on the Budapest Convention on Cybercrime and its Second Additional Protocol (2022), the European Union instruments on electronic evidence, the United Nations Convention against Cybercrime, and the evidence statutes of Singapore and Malaysia. The comparators were selected on three grounds. The first is exposure to the same practical problem: Singapore and Malaysia adjudicate on data held by the same transnational platforms and operate investigative bodies of comparable scale. The second is transferability of form. Singapore and Malaysia both resolved the authentication of machine-produced records by statutory amendment rather than by incremental judicial development, offering a legislative solution that can be readily integrated into another codified system in a way that case-law solutions do not. The third is obligation: the international instruments are examined because they address the cross-border problem, and because Vietnam has assumed obligations under the most recent of them. The self-authentication rules of the United States Federal Rules of Evidence are also drawn on at one point in section 5.1, not as a third core comparator but as a supplementary reference on the narrower question of authentication technique.

The third method is the analysis of judgments. The dataset consists of twenty criminal judgments delivered by Vietnamese courts between 2017 and 2025, at first instance and on appeal, all retrieved from the judgment publication portal of the Supreme People's Court. The search was conducted in the criminal collection using the Vietnamese key words: electronic data, electronic evidence, data extraction, backup, cameras, and text messages, across four search sessions carried out between 1 April 2026 and 30 June 2026.

Judgments were selected if the full text is available and electronic data served as the principal means of proof or as a significant corroborative element. Judgments were excluded if electronic data appeared only in the list of exhibits without bearing on the findings, or if the full-published text is not available. Where both first-instance

³³ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27037:2012, Guidelines for the Identification, Collection, Acquisition and Preservation of Digital Evidence, International Organization for Standardization, Geneva, 2012. Available at: <https://www.iso.org/standard/44381.html> (accessed on 20 April 2026).

³⁴ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Ibid.

and appellate decisions existed for the same proceedings, only the final appellate decision was retained (Total 20 judgments).

The figure of twenty was not fixed in advance. Selection continued until every cell of the analytical matrix described in section 4.1 (three classes of origin against two evidentiary functions) had been populated, and until additional judgments within a cell ceased to disclose forms of judicial treatment not already observed. The sample is purposive and designed for maximum variation across offence type, tier of court and region. It is not a probability sample. No inference is drawn from the frequency with which any feature occurs, and the figures presented in Part 4 describe this dataset and nothing beyond it.

The classification was applied by both authors independently to the full text of each judgment, and coded at the level of the individual item of electronic evidence rather than at the level of the case, since a single prosecution routinely relies on items of different origin. Disagreements were resolved by returning to the text of the judgment; where the text did not permit an item to be assigned with confidence, it was recorded as indeterminate rather than allocated. The final column of Table 3, which records what each judgment states about provenance or integrity, was checked against the original text of every judgment in the dataset.

The design is one of qualitative document analysis. What it examines is not investigative practice but the reasoning of published judgments, and the two must not be conflated: a judgment summarises the case file and does not reproduce it. The consequences of that distinction for the findings are set out at the beginning of Part 4.

3. Legal framework on electronic evidence in Vietnamese criminal proceedings

3.1 Concept of electronic evidence

The history of the concept of electronic evidence in Vietnamese law reflects an inconsistency between substantive law and procedural law: the CPC 2003 did not recognize electronic data as a source of evidence, even though the 1999 Criminal Code had already criminalized offences committed through information technology and telecommunications. This disconnection between substantive law and procedural law was partially addressed by Joint Circular No. 10/2012/TTLT BCA BQP BTP BTT&TT VKSNDTC TANDTC guiding the application of the Criminal Code's provisions on certain offences in the field of information technology and telecommunications, which provided that electronic data could be regarded as evidence in cases involving certain information technology offences,³⁵ but this was more a stopgap solution than a systematic legislative one. The issue was only formally resolved in the CPC 2015, when Article 87(1)(c) listed "electronic data" as a new and independent source of evidence alongside physical evidence, testimonies, expert conclusions and procedural records.

The CPC 2015 defines electronic data in Article 99 as "symbols, letters, numerals, images, sounds or similar forms that are created, stored, transmitted or received by

³⁵ Vietnam's Ministry of Public Security – Vietnam's Ministry of National Defence – Vietnam's Ministry of Justice – Vietnam's Ministry of Information and Communications – Vietnam's Supreme People's Procuracy – Vietnam's Supreme People's Court. Joint Circular No. 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC guiding the application of the provisions of the Penal Code on certain offences in the field of information technology and telecommunications, Hanoi, 2012. Available at: <https://congbao.chinhphu.vn/van-ban/thong-tu-lien-tich-so-10-2012-ttlt-bca-bqp-btp-btttt-vksndtc-tandtc-16819.htm> (accessed on 20 April 2026).

electronic means.”³⁶ This definition is deliberately aligned with the concept of “data” in the 2005 Law on Electronic Transactions,³⁷ and is essentially maintained in the 2023 Law on Electronic Transactions, with the addition that electronic data are data “created, processed and stored by electronic means.”^{38,39} This convergence shows that the Vietnamese legislature acknowledges that electronic data have a unified nature that transcends the specific context of criminal procedure. However, what the CPC 2015 has not done is to provide an official definition of the concept of “electronic evidence” while Vietnamese legal scholars continue to use this term in parallel with the statutory term “electronic data”.⁴⁰

Regarding the relationship between these two concepts, two scholarly positions have now taken shape. The first position regards electronic evidence as a subcategory of ordinary evidence, that is, factual elements originating from electronic data that satisfy the general criteria for admissibility of evidence concerning objectivity, relevance and legality under Article 86 of the CPC 2015.⁴¹ The second one regards electronic evidence as a conceptually independent category with distinct characteristics, separating it from all forms of traditional evidence.⁴²

In the authors’ view neither position should be accepted as stated, because both answer a question of classification when the question that matters is one of regulation. Electronic data satisfy the definition of evidence in Article 86 in the same way as any other material: they are things that are true, collected in the prescribed manner, and used to establish the facts in issue. Nothing is gained by declaring them a separate species of evidence. What distinguishes them is not their evidentiary nature but the procedural treatment their physical characteristics require. Electronic evidence is therefore best understood not as a conceptually independent category of evidence but as a procedurally distinct object of regulation.

Three terms must be kept distinct, and this article uses them consistently in the following senses. Electronic means are the hardware, software and systems by which data are created, transmitted or stored, as defined in article 3 of the 2023 Law on Electronic Transactions; they are physical objects and, when seized, they are exhibits within the meaning of article 89 of the CPC 2015. Electronic data are the signals, letters, numbers, images, sound and similar elements created, stored or transmitted by electronic means, and they are an independent source of evidence under article 87(1)(c). Electronic evidence is electronic data that has satisfied the conditions of admissibility and is relied on to establish a fact in issue. The distinction between the first and the second is not merely terminological: it explains why the sealing regime, which attaches to exhibits, reaches the handset and not the data extracted from it.

³⁶ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Ibid.

³⁷ VIETNAMESE NATIONAL ASSEMBLY. Law on Electronic Transactions 2005, Hanoi, 2005, Art. 4(5). Available at: https://www.wto.org/english/thewto_e/acc_e/vnm_e/wtaccvnm43_leg_5.pdf (accessed on 20 March 2026).

³⁸ VIETNAMESE NATIONAL ASSEMBLY. Law on Electronic Transactions 2005, Hanoi, 2005. Art. 3(6) and 7. Available at: https://www.wto.org/english/thewto_e/acc_e/vnm_e/wtaccvnm43_leg_5.pdf (accessed on 20 March 2026).

³⁹ VIETNAMESE NATIONAL ASSEMBLY. Law on Electronic Transactions 2023 (Law No. 20/2023/QH15), Hanoi, 2023. Art. 3. Available at: <https://thuvienphapluat.vn/van-ban/EN/Thuong-mai/Law-20-2023-QH15-Electronic-Transactions/577937/tieng-anh.aspx> (accessed on 02 Jun 2026).

⁴⁰ NGUYỄN VĂN ĐIỀN. "Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015" [Electronic evidence in the 2015 Criminal Procedure Code]. Ministry of Justice, 17 June 2019. Ibid.

⁴¹ NGUYỄN ĐỨC HẠNH. "Electronic data and electronic evidence". 2019. Ibid.

⁴² DUONG QUYNH HOA. "Electronic evidence and electronic evidence storage using Blockchain technology: China's experience and implications for Vietnam". 2024. Ibid.

The characteristics of electronic data matter because each of them generates a specific procedural requirement, and it is the absence of those requirements rather than the nature of the data that produces the difficulties examined in Part 4. Characteristic of electronic data under CPC 2015 show at table 1.

Table 1. Characteristic of electronic data under CPC 2015.

Characteristic of electronic data	Procedural consequence	Position under the CPC 2015
Immaterial: requires hardware and software to become perceptible	Rules are needed on the evidentiary status of copies, printouts and screen captures, and on who makes them	No provision; the artefacts examined in section 4.4 have no defined status
Volatile: may be altered or deleted before it can be secured	A preservation order and a time limit for acting on it	No preservation order exists; art. 107(2) prescribes no time limit
Alteration leaves no visible trace	Integrity must be fixed by a technical act at the moment of acquisition, in practice a hash value	Not required at any stage
Meaning depends on metadata as much as on content	Forensic imaging of the whole medium rather than selective copying	Art. 107(2) permits copying without specifying the method
Frequently stored outside the territory	A procedure addressed to a foreign service provider	No provision; see section 5.3
Volume greatly exceeds what is relevant	Rules for filtering and safeguards against over-seizure	No provision; connects to the data protection question in section 3.4

3.2 Characteristics of electronic evidence under the Vietnamese legal framework

Article 99(3) of the CPC 2015 provides that the evidentiary value of electronic data is determined on the basis of “the methods of creating, storing and transmitting electronic data; the methods of ensuring and maintaining the integrity of electronic data; the methods of identifying the originator and other appropriate factors.”⁴³ Drawing upon this provision, Vietnamese legal scholarship has constructed an evidentiary admissibility framework comprising five elements: objectivity, relevance, legality, authenticity and integrity.⁴⁴

Objectivity requires that the data exist as an objective fact, that they have a clear origin and that they remain unchanged in the original storage medium or an equivalent lawful copy. Relevance requires a demonstrable connection between the data and the facts to be proved whether these concern the alleged criminal act, the identity of the offender, the victim, or the consequences of the offence. Legality requires that the data be collected in strict compliance with the procedures laid down in the CPC 2015; data obtained in violation of statutory procedures have no legal value and cannot serve as a basis for any conclusion regarding guilt, regardless of

⁴³ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Ibid.

⁴⁴ BUI HAI HIEU. *On some aspects of electronic data in criminal procedure*. Protection of Law newspaper (Kiểm sát), 2021. Ibid.

their factual accuracy.⁴⁵ Authenticity requires identifying the person who created the data and assessing whether the data were generated automatically by a computer created by the offender or the victim or produced by a competent authority. Integrity requires that the data be shown to have preserved their accuracy and consistency from the moment of creation, through collection, up to their presentation in court.

It can be seen that the five elements outlined above broadly reflect the triad of authenticity, integrity and relevance found in international theories of evidentiary admissibility. The distinctive feature of the Vietnamese framework, as compared with international standards, lies in the fact that it provides no procedural mechanism by which those elements can actually be established.^{46,47} In the common law tradition, authentication is a distinct procedural requirement that the proponent of evidence must satisfy before that evidence can be admitted. Specifically, the US Federal Rules of Evidence require the proponent to "produce evidence sufficient to support a finding that the item is what the proponent claims it is,"⁴⁸ while the PACE Codes of Practice in England and Wales impose detailed recording obligations when seizing and examining electronic devices.⁴⁹

This shows that the civil law tradition has influenced the sequence of evidence authentication in Vietnamese criminal procedure. Although it should be noted that, at the level of formal rules, the CPC 2015 still requires that evidence be collected in accordance with prescribed procedures and sources of law. Conversely, the CPC 2015 formulates the criteria for evidentiary admissibility as abstract elements without specifying the procedural steps by which those qualities are to be established. As a result, courts must assess the admissibility of electronic evidence without a procedural roadmap, relying primarily on the defendant's confession, the investigator's testimony, and other inherently subjective narrative accounts.

The CPC 2015 is not silent on the handling of seized items. It defines exhibits and requires that they be preserved, requires items seized to be described and sealed, requires records to be drawn up of searches and seizures, and provides for expert examination; the sealing and unsealing of exhibits is governed in further detail by subordinate legislation.^{50,51} What the Code does not establish is an integrated and traceable chain of custody for electronic data: a continuous documentary record, running from seizure to presentation in court, of who handled the data, when, under what conditions and with which tools. The provisions that exist address physical objects and were not designed for a class of evidence whose alteration leaves no visible trace.

The controls the Code does impose on access to private information are, moreover, distributed in a way that no longer matches the risk. An order to seize letters, telegrams and postal items held by postal or telecommunications providers must be

⁴⁵ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Ibid.

⁴⁶ DINH THE HUNG. "The legal framework of electronic evidence in vietnamese criminal procedure: From the budapest convention to domestic legislation". 2025. Ibid.

⁴⁷ TRƯƠNG THÀNH THẢO NGUYỄN. "Digital evidence in criminal procedure: Legal challenges and solutions in Vietnam". *Journal of Science and Technology (Binh Duong University)*, vol. 8, no. 1, 2025. Available at: <https://jst.bdu.edu.vn/index.php/jst/article/view/297> (accessed on 05 March 2026).

⁴⁸ UNITED STATES CONGRESS. Federal Rules of Evidence, Washington DC, 1975 (Pub. L. 93-595, as amended), Rules 901-902. Ibid.

⁴⁹ UK PARLIAMENT. Police and Criminal Evidence Act 1984 (PACE), London, 1984, Code B. Ibid.

⁵⁰ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Ibid.

⁵¹ THE GOVERNMENT OF VIETNAM. Decree No. 127/2017/ND-CP of 16 November 2017 of the Government detailing the sealing and unsealing of exhibits, Hanoi, 2017. Available at: <https://vanban.chinhphu.vn/default.aspx?pageid=27160&docid=192054> (accessed on 20 April 2026).

approved by the procuracy of the same level before it is executed.⁵² Covert collection of electronic data is one of three special investigative measures, available only after prosecution has been instituted, only for offences against national security, drug offences, corruption offences, terrorism and money laundering and other organised offences classified as particularly serious, and subject to procuratorial approval and a statutory time limit.⁵³ By contrast, the overt extraction of the entire contents of a suspect's device under Articles 107 and 196 requires no approval, is confined to no defined scope and is subject to no time limit. The 2015 legislature located the risk to privacy in the covertness of the measure rather than in the volume and depth of the data reached, an allocation that is difficult to sustain once a single handset holds more private communication than the whole of a person's correspondence.

The 2025 amendments make the omission more visible rather than less. Law No. 99/2025/QH15 introduced provisions on the digitisation of case files, on digital signatures and on the service of procedural documents through shared digital platforms, so that the case file itself is now to be maintained in electronic form. The legislature has thus regulated the medium while leaving the integrity of what the medium carries unaddressed.

The consequence is evidential rather than merely formal. Without a documented record of how electronic data were handled from the moment of seizure to their presentation in court, it cannot be shown on the face of the case file that the data before the court are those originally acquired from the device, or that they remained unchanged in the interval. The criteria in Article 99(3) presuppose such a record; the Code does not require one. Table 2 sets the stages of the chain of custody in ISO/IEC 27037 and the first-responder guidance against the corresponding provisions of Vietnamese law, and identifies the gap at each stage.⁵⁴

Table 2. The chain of custody in ISO/IEC 27037 and in the CPC 2015.

Stage	Requirement under ISO/IEC 27037 and the first-responder guidance	Corresponding provision of Vietnamese law	Gap
Identification	Recognise and record potential sources of digital evidence, including volatile data, before any action is taken	Art. 107(1): electronic means must be seized promptly and completely	No requirement to record what was identified but not seized, or to address volatile data
Collection of the device	Seize the carrier, describe its condition, seal it and record the seal	Arts. 89, 105 and 90: exhibits described in a record, sealed, sealing and unsealing minuted in the file; Decree No. 127/2017/ND-CP	Complete for the device. But electronic data are a separate source of evidence under art. 87(1)(c), not an exhibit, so the sealing regime reaches the handset and not the data taken from it

⁵² VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Art. 197(1)-(2). Available at: <https://www.wipo.int/wipolex/en/text/585372> (accessed on 20 April 2026).

⁵³ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Art. 223 and 224. Available at: <https://www.wipo.int/wipolex/en/text/585372> (accessed on 20 April 2026).

⁵⁴ NGUYEN THANH MINH CHANH. "Authentication of electronic evidence derived from digital transactions and communications". 2025. Ibid.

Stage	Requirement under ISO/IEC 27037 and the first-responder guidance	Corresponding provision of Vietnamese law	Gap
Acquisition of the data	Forensic image of the whole medium; hash computed at the moment of acquisition; acquisition method and tool recorded	Art. 107(2): data may be copied to another medium where the device cannot be seized	No standard of imaging, no hash, no record of method or tool, and no time limit
Preservation of the device	Storage conditions that prevent alteration; documented transfers	Art. 90: exhibits preserved intact, not lost, mixed up or damaged	Framed for physical deterioration, not for alteration of data that leaves no trace
Preservation of the data	Working copy separated from the master; integrity re-verified before use	No provision	Absent
Chain of custody record	Continuous record of every person who handled the item, when, in what conditions and with what tool	No provision for electronic data; the sealing minute under art. 90 covers only two moments	Absent as a continuous record; only the moments of sealing and unsealing are documented
Verification	Independent examination of integrity where the evidence is relied on	Arts. 205–206: expert examination may be requested; art. 206(5) makes it mandatory only for a closed list of matters	Electronic data are not on the list of matters requiring mandatory expert examination
Presentation	Demonstrate to the tribunal that the item presented is the item acquired	Art. 99(3): evidentiary value assessed by reference to creation, integrity and identification of the originator	Criteria stated without any instrument by which they can be established

Read across, Table 2 shows that the Vietnamese framework is well developed at the two points where the object is a physical thing (the seizure and the sealing of the device),^{55,56} and empty at every point where the object is the data. The reason is structural rather than accidental. Article 105 requires exhibits to be sealed, and an exhibit is a physical object within the meaning of article 89; electronic data, however, are a distinct source of evidence under article 87(1)(c) and are not exhibits at all. The regime that guarantees integrity therefore attaches to the container and not to the content. The same structural point explains the position on verification: expert examination is mandatory only for the matters listed in article 206(5), and electronic

⁵⁵ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Art. 89, 90 and 105. Available at: <https://www.wipo.int/wipolex/en/text/585372> (accessed on 20 April 2026).

⁵⁶ THE GOVERNMENT OF VIETNAM. Decree No. 127/2017/ND-CP of 16 November 2017 of the Government detailing the sealing and unsealing of exhibits, Hanoi, 2017. Ibid.

data are not among them,⁵⁷ so the examination that the appellate court in Hai Duong obtained in 2025 was a matter of investigative choice rather than of legal requirement.

3.3 Deficiencies in Vietnam's legal framework on electronic evidence

The provisions on the handling of electronic data in the CPC 2015 are expressed mainly in two articles: Article 107, on the collection of electronic devices and electronic data, and Article 196, on the seizure of electronic devices and electronic data.⁵⁸ These two provisions contain conflicting content that creates significant difficulties in practical application. Article 107 (in terms of substance) is the primary provision on the collection of evidence. Yet its first paragraph states that "electronic devices must be seized promptly and in full," thereby implicitly introducing the term "seizure" into an article whose heading and stated regulatory focus concern collection.⁵⁹ By contrast, Article 196 with entitled "Seizure of electronic devices and electronic data," largely duplicates the content of Article 107, with overlapping provisions that generate confusion as to which article governs which investigative acts and which procedural requirements apply in each situation.⁶⁰

The inconsistency is not merely a defect of drafting technique. It produces genuine uncertainty in investigative practice as to which procedure must be followed and which record must be drawn up, with direct consequences for the admissibility of anything collected under either provision. Article 107 suffers in addition from two deficiencies, which are best stated in parallel because they share a structure.⁶¹

The first concerns copying. Article 107(2) permits electronic data to be copied to another medium where the original storage device cannot be seized, but prescribes no time limit within which the copy must be made, no method by which it must be made, no technical standard it must meet, and no means by which the result may be verified. Since the integrity of a copy depends entirely on the method used and on the record kept of that method, the permission is granted and the conditions of its reliability are left unstated.⁶²

The second concerns recovery. Article 107(3) addresses the recovery of data only in the context of expert examination of material already collected. It therefore leaves unaddressed the far more common situation in which data have been deleted and must be recovered before any collection can occur at all. In this context as well, statutory authority is granted for one situation and withheld, by silence, from the situation in which it is most often needed. In both instances the difficulty is the same: the provision authorises an act on electronic data without stating the conditions under which the result of that act can be trusted.

In practice, investigators and prosecutors still rely on the provisions of Joint Circular No. 10/2012 to fill procedural gaps left by the CPC 2015 regarding the handling of electronic evidence. It should be noted that this Circular was issued three years before electronic data was officially recognized as a source of evidence and was not designed as a comprehensive framework for digital forensic practice. Therefore,

⁵⁷ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Art. 206(5). Available at: <https://www.wipo.int/wipolex/en/text/585372> (accessed on 20 April 2026).

⁵⁸ LE NGUYEN THANH. "Electronic evidence collection in Vietnamese criminal proceedings". *Vietnamese Journal of Legal Science*. 2024. Ibid.

⁵⁹ NGÔ XUÂN KHANG. "Identifying legal bottlenecks on electronic data and recommendations for improvement". 2023. Ibid.

⁶⁰ TRẦN NGỌC MINH & ĐẶNG MINH CƯỜNG. "Improving the law on investigative measures under the criminal procedure code 2015". 2023. Ibid.

⁶¹ LE NGUYEN THANH. "Electronic evidence collection in Vietnamese criminal proceedings". *Vietnamese Journal of Legal Science*. 2024. Ibid.

⁶² PHẠM CÔNG TÙNG, "Improving the provisions on electronic data in criminal procedure", *Protection of Law newspaper (Kiểm sát)*, 2022. Ibid.

the continued reliance on that circular in practice is an indication of the extent to which legislative gaps still need to be addressed.

3.4 Data protection and evidence collection: A broad exemption without conditions

Vietnam's personal data protection regime was recast shortly before this article was written. The Law on Personal Data Protection, Law No. 91/2025/QH15, was adopted by the National Assembly on 26 June 2025 and took effect on 1 January 2026.⁶³ Decree No. 356/2025/ND-CP of 31 December 2025 details its implementation and entered into force on the same date,⁶⁴ replacing Decree No. 13/2023/ND-CP, which ceased to have effect on 1 January 2026. The judgments examined in Part 4 were all handed down under the earlier regime, and the analysis that follows therefore separates two questions: which rules governed the collection of data in those cases, and which rules govern it now.

The Law confers on data subjects the rights to be informed of processing, to consent or refuse consent, to inspect and correct their data, to request erasure or restriction of processing, and to complain, denounce, sue and claim damages.⁶⁵ When evaluated against the operational reality of criminal investigation, those rights appear difficult to reconcile with evidence collection: an investigation into messaging applications, social media accounts, banking records or telecommunications traffic necessarily processes the personal data not only of the suspect but of victims, witnesses and uninvolved third parties whose communications happen to be stored on the same device or account.

That apparent conflict, however, is not where the difficulty lies. Article 19(1) of the Law on Personal Data Protection expressly exempts five categories of processing from the consent requirement, and two of them cover criminal investigation directly: i) processing to address an emergency or a threat to national security falling short of a declared state of emergency, and to prevent and combat riot, terrorism, crime and violations of law; ii) and processing to perform the activities of state agencies and state administration as provided by law.⁶⁶ Consequently, investigative agencies, extracting data from a seized device, do not need the consent of the data subject, rendering legally unfounded the recurring concern that data protection legislation obstructs criminal investigations.

The real difficulty is the opposite one. Both exemptions are drafted by open-ended referral: to prevent and combat crime and violations of law, and as provided by law. The Law thus delegates the conditions, the permissible scope, the retention period and the control mechanism to sectoral legislation. In this context, however, the governing sectoral instrument - the CPC 2015 - fails to provide any of these necessary procedural standards. Article 19(2) makes the point sharper still. Where personal data are processed without consent, the Law requires the establishment of a supervision mechanism: documented processing procedures with allocated

⁶³ VIETNAMESE NATIONAL ASSEMBLY. Law on Personal Data Protection 2025, Hanoi, 2025. Available at: <https://english.luatvietnam.vn/dan-su/law-on-personal-data-protection-law-no-91-2025-qh15-405135-d1.html> (accessed on 05 Jun 2026).

⁶⁴ THE GOVERNMENT OF VIETNAM. Decree No. 356/2025/ND-CP of 31 December 2025 detailing certain articles of and measures implementing the Law on Personal Data Protection, Hanoi, 2025, (Article 42(1)). Available at: <https://vanban.chinhphu.vn/?pageid=27160&docid=216387> (accessed on 05 Jun 2026).

⁶⁵ VIETNAMESE NATIONAL ASSEMBLY. Law on Personal Data Protection 2025, Hanoi, 2025. Article 4(1). Available at: <https://english.luatvietnam.vn/dan-su/law-on-personal-data-protection-law-no-91-2025-qh15-405135-d1.html> (accessed on 05 Jun 2026).

⁶⁶ VIETNAMESE NATIONAL ASSEMBLY. Law on Personal Data Protection 2025, Hanoi, 2025. Article 19(1). Available at: <https://english.luatvietnam.vn/dan-su/law-on-personal-data-protection-law-no-91-2025-qh15-405135-d1.html> (accessed on 05 Jun 2026).

responsibility, appropriate protective measures, regular risk assessment, periodic compliance review, and a channel for receiving and handling representations.⁶⁷ No provision of the CPC 2015 performs any of these functions in relation to electronic data. The obligation exists in the data protection statute and has no counterpart in the procedural law through which it would have to operate.

The CPC 2015 does contain controls of this kind, but distributed in a way that no longer matches the risk. Seizure of letters, telegrams and postal items held by postal and telecommunications providers requires the approval of the procuracy.⁶⁸ Covert collection of electronic data is treated as a special investigative measure, available only for defined categories of offence, subject to approval by the Chief Procurator and to a statutory time limit.⁶⁹ Yet the overt extraction of the entire contents of a suspect's device under Articles 107 and 196 requires no approval, is subject to no limit regarding either scope or duration. The 2015 legislature located the risk to privacy in the covertness of the measure rather than in the volume and depth of the data reached. That allocation is difficult to defend once a single handset holds more private communication than the whole of a person's correspondence.

Framed in constitutional terms, the gap is more than an inconvenience. Article 21 of the 2013 Constitution guarantees the secrecy of correspondence, telephone and telegraph communications and other forms of private information exchange, and prohibits their opening, control or seizure otherwise than in accordance with law; Article 14(2) permits restriction of a constitutional right only by law and only where necessary on grounds of national defence, national security, social order and safety, social morality or public health.⁷⁰ A statutory power to extract an unlimited quantity of private data, unaccompanied by any condition of necessity, any defined scope, any retention limit and any authorisation requirement, sits uneasily with both provisions. The broad exemption in Article 19(1) of the Law on Personal Data Protection does not cure this, because it refers the matter back to the very procedural law in which the conditions are missing.

Comparable instruments address the same problem by pairing investigative powers with conditions. Article 14 of the Second Additional Protocol to the Budapest Convention makes data protection safeguards a condition of the cooperation mechanisms it establishes;⁷¹ Regulation (EU) 2023/1543 conditions the issuing of production and preservation orders and provides for review.⁷² For Vietnam this is now an implementation question rather than a comparative aspiration. Vietnam ratified

⁶⁷ VIETNAMESE NATIONAL ASSEMBLY. Law on Personal Data Protection 2025, Hanoi, 2025. Article 19(2). Available at: <https://english.luatvietnam.vn/dan-su/law-on-personal-data-protection-law-no-91-2025-qh15-405135-d1.html> (accessed on 05 Jun 2026).

⁶⁸ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Art. 197(1)-(2). Available at: <https://www.wipo.int/wipolex/en/text/585372> (accessed on 20 April 2026).

⁶⁹ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Art. 223-228. Available at: <https://www.wipo.int/wipolex/en/text/585372> (accessed on 20 April 2026).

⁷⁰ VIETNAMESE NATIONAL ASSEMBLY. The 2013 Constitution of the Socialist Republic of Vietnam, Hanoi, 2013, Art. 14(2) and 21. Available at: <https://www.wipo.int/wipolex/en/legislation/details/21482> (accessed on 20 April 2026).

⁷¹ COUNCIL OF EUROPE. Second additional protocol to the convention on cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), opened for signature in Strasbourg on 12 May 2022. Available at: <https://www.coe.int/en/web/cybercrime/second-additional-protocol> (accessed on 19 April 2026).

⁷² OFFICIAL JOURNAL OF THE EUROPEAN UNION. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings (OJ L 191, 28.7.2023). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1543> (accessed on 25 March 2026).

the United Nations Convention against Cybercrime, opened for signature in Hanoi in October 2025, on 7 April 2026.⁷³ The Convention requires States Parties to provide domestic procedural powers over electronic data together with corresponding conditions and safeguards. Codifying the conditions absent from Articles 107 and 196 is therefore no longer merely desirable: it is an obligation Vietnam has assumed. Because the Convention enters into force only ninety days after the fortieth ratification, and that threshold has not been reached,⁷⁴ the interval before it becomes operative is precisely the period in which domestic reform must do the work.

4. Electronic evidence in judicial practice from a systematic analysis of twenty judgments

A single limitation of the source material must be kept in view throughout this Part, because it conditions how every finding below should be interpreted. A Vietnamese criminal judgment records the facts found, the evidence the court considered material and the reasons for the decision. It is not a reproduction of the case file. It does not contain the record of seizure, the minutes of sealing and unsealing, the record of copying, the requisition for expert examination or any correspondence with service providers. Where a judgment is silent as to how an item of electronic evidence was obtained or preserved, that silence establishes that the court did not treat the question as one requiring reasoned treatment in the judgment; it does not establish that no such record was made during the investigation. The findings below are therefore claims about judicial reasoning, not about investigative practice. Establishing the latter would require access to case files and interviews with investigators, prosecutors and judges, which lies beyond the scope of this study and is identified in Part 7 as the necessary next stage of research.

4.1 Classification: The mode by which the data came into existence

The twenty judgments analyzed in this study were handed down by Vietnamese first-instance and appellate courts between 2017 and 2025, covering fifteen offense categories across the North, Central and South of the country. Classifying them requires a defined criterion, which must directly address the central research question of this study. Grouping cases by the role the data plays in the offence (as an element of the offence, as the means of its commission, as a financial record) mixes three different things: what is to be proved, the instrument of the crime, and the content of the data. Those groupings also cut across one another, since the same transaction log may be the principal proof in one case and corroboration in another.

The classification adopted here rests on a single criterion: the mode by which the data came into existence. That criterion is chosen because it determines what must be shown to authenticate the item. Its unit is not the case but the individual item of electronic evidence, since a single prosecution routinely relies on items of different origin, and it is precisely that difference which the four-part functional grouping obscures. Three classes result.

Class (i) comprises data generated by a system: the technical output of rogue base transceiver stations, server databases of gambling platforms, banking records, transaction logs and surveillance camera recordings. There is no human declarant. Authentication turns on the reliability of the generating system and on the integrity

⁷³ UNITED NATIONS. United Nations Convention against Cybercrime, Hanoi, 2025. Available at: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html> (accessed on 20 March 2026).

⁷⁴ UNITED NATIONS. United Nations Convention against Cybercrime, Hanoi, 2025. Art. 65(1). Available at: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html> (accessed on 20 March 2026).

of the acquisition, which is the point at which the rebuttable presumptions used in other jurisdictions do their work.

Class (ii) comprises content composed by a person and stored electronically: messages, posts, livestreams, and images or video recorded by an individual. Authentication turns on attributing authorship, and secondarily on integrity. This is the class most easily fabricated and, as Part 4 shows, the class in which Vietnamese judgments are most often silent.

Class (iii) comprises artefacts created by the investigation itself: screenshots, USB copies of camera footage, printed extracts of message threads, and transcripts of recorded material. These items did not exist prior to their creation in the course of the investigation. Their authenticity depends entirely on the documented process of their creation, that is, on the chain of custody in its strict sense. This category remains entirely unaddressed in both the existing scholarship and judicial decisions, yet it is precisely here that the procedural gap identified in Part 3 produces its most acute practical consequences.

A second and independent axis distinguishes evidence on which the conviction principally rests from evidence performing a corroborative role. The two axes yield a matrix, set out with the dataset in Table 3. Two features of the distribution are worth noting at the outset. No item of class (ii) in the dataset performs a merely corroborative function: content composed by a person is always relied on as principal proof. And with a single exception, no judgment records any examination of an item of class (iii), although these are the items whose reliability depends most completely on how they were made. Table 3 records, for each of the twenty judgments, the electronic evidence relied on, its class of origin and its evidentiary function, and what the judgment states about the provenance or integrity of that evidence; sections 4.2 to 4.6 discuss those entries class by class.

Table 3. The twenty judgments: electronic evidence, class of origin, evidentiary function, and what each judgment records on provenance or integrity.

No.	Judgment, court and level	Offence	Electronic evidence	Class · function	What the judgment records on provenance or integrity
1	56/2017/HSST – Kien Xuong District, Thai Binh (first instance)	Theft (art. 138 PC 1999)	Eight video discs, listed in the judgment under the heading “electronic evidence”	(i) · corroborative	Listed as electronic evidence; nothing on preservation, authentication or verification
2	108/2019/HSPT – High People’s Court, Da Nang (appeal)	Property appropriation by network	Facebook accounts, copied product images, bank accounts	(ii)+(i) · principal	None
3	406/2019/HSPT – High People’s Court, Hanoi (appeal)	Unlawful use of telecoms network (art. 290)	VoIP GSM Gateway devices (electronic means, not data)	boundary case · principal	Expert conclusion of the Ministry of Information and Communications on device function and conformity marking
4	141/2020/HS-PT – People’s Court of Ho Chi Minh City (appeal)	Property appropriation by network (art. 290)	Hotel camera footage; photographs of card faces; card transaction data	(i)+(iii) · principal	None

No.	Judgment, court and level	Offence	Electronic evidence	Class · function	What the judgment records on provenance or integrity
5	232/2020/HS-ST – Thu Duc District (first instance)	Indecent acts against a minor (art. 146)	USB containing camera clips	(i)+(iii) · principal	Forensic DNA conclusion only; nothing on the data
6	85/2021/HS-ST – People’s Court of Hai Phong City (first instance)	Organising gambling (arts. 321–322)	Server database of the RikVip/Tip.Club platform	(i) · principal	Records that the server data were “seized in accordance with criminal procedure”
7	93/2021/HSST – P District, Thai Nguyen (first instance)	Humiliating another person (art. 155)	Facebook posts and images; Zalo messages	(ii) · principal	Handset sealed in a marked envelope; both IMEI numbers and both subscriber numbers recorded
8	45/2022/HS-ST – Binh Thanh District, HCMC (first instance)	Theft	On-premises camera footage; USB copy	(i) +(iii) · corroborative	None
9	55/2022/HS-ST – Hoang Hoa District, Thanh Hoa (first instance)	Road traffic offence (art. 260)	USB containing data extracted from camera	(i) +(iii) · corroborative	Expressly declares the USB to be electronic evidence in the case, to be retained on the file
10	268A/2022/HSST – Hai Ba Trung District, Hanoi (first instance)	Gambling (arts. 321–322)	Handset seized on administrative check; contents not exploited	none exploited · –	Conviction rests on admissions; the judgment records no extraction from the seized handset
11	01/2023/HSST – Ky Anh District, Ha Tinh (first instance)	Extortion (art. 170)	Self-recorded video; Zalo messages; bank transfers	(ii) · principal	None
12	10/2023/HS-ST – Dak Song District, Dak Nong (first instance)	Extortion (art. 170)	Images taken from an iCloud account; Zalo and Facebook messages	(ii) · principal	None
13	626/2023/HS-PT – High People’s Court, HCMC (appeal)	Propaganda against the State (art. 117)	Facebook posts and livestreams; extraction report	(ii)+(iii) · principal	Extraction conducted by the security investigation body together with the cyber-security unit and the People’s Procuracy of HCMC; four expert conclusions; the judgment records that the investigating body had not proved when the material was composed, on which device, by whom it was posted or by what method

No.	Judgment, court and level	Offence	Electronic evidence	Class · function	What the judgment records on provenance or integrity
14	770/2023/HS-PT – High People’s Court, Hanoi (appeal)	Gambling (arts. 321–322)	Zalo message threads recording lottery bets	(ii) · principal	None
15	790/2023/HS-PT – High People’s Court, HCMC (appeal) ⁷⁵	Abuse of trust (art. 175)	Betting-site data on the accused’s computer; bank statements	(i)+(iii) · principal	Records that at the time of extraction the site data on the computer covered only 20 August to 20 November 2020
16	628/2023/HS-PT – High People’s Court, Da Nang (appeal)	Unlawful use of network data (art. 288)	Dataset of personal records; identity-document photographs; bank accounts	(i)+(ii) · principal	None
17	13/2024/HSST – Y District, Ninh Binh (first instance)	Humiliating another person (art. 155)	Facebook posts; Messenger videos	(ii) · principal	None
18	268/2024/HS-PT – High People’s Court, Da Nang (appeal)	Unlawful interference with telecoms (art. 289)	Output of simulated base transceiver stations; broadcast messages	(i) · principal	Expert conclusion of the Institute of Forensic Science on the function of the devices
19	18/2024/HS-ST – People’s Court of Quang Ngai Province (first instance)	Propaganda against the State (art. 117)	Ten Facebook livestreams; printed extracts of their content and of handset data	(ii)+(iii) · principal	Handsets sealed in numbered envelopes bearing the signatures of those present and the seal of the ward police; the accused signed each page of the printed extracts; requisition and expert conclusion of the provincial Department of Information and Communications
20	42/2025/HS-PT – People’s Court of Hai Duong Province (appeal)	Disturbing public order (art. 318)	USB containing eleven video files	(i) +(iii) · (ii) corroborative	Expert conclusion No. 4777: no trace of cutting or alteration found in the eleven files; sixteen-page annex; exhibits returned

⁷⁵ VIETNAMESE NATIONAL ASSEMBLY. Law on Treaties 2016, Hanoi, 2016. Art. 6(1). Available at: <https://vanban.chinhphu.vn/?pageid=27160&docid=184571> (accessed on 20 April 2026).

4.2 Class (i): Data generated by a system

Eleven of the twenty prosecutions rest wholly or partly on data produced by a machine without a human declarant: the technical output of devices, the databases of commercial platforms, banking records and surveillance recordings. Authentication of such material turns on two questions: whether the generating system was operating correctly, and whether the data were acquired without alteration. Neither question is answered in any of the eleven judgments, although several come close in ways that repay attention.

The clearest instance of machine-generated proof is the prosecution of a group who mounted simulated base transceiver stations on moving vehicles to intercept telecommunications signals and broadcast unsolicited messages to subscribers within a radius of 50 to 100 metres across several provinces.⁷⁶ The evidence was the output of the offending apparatus itself, together with an expert conclusion of the Institute of Forensic Science on the capability and function of the devices. That conclusion establishes what the equipment was capable of doing; it says nothing about whether the tendered logs were a complete and unaltered record of what the equipment did. The distinction matters, and neither the first-instance court nor the appellate court drew it.

Two judgments approach the question of acquisition. In the prosecution arising from the RikVip/Tip.Club platform the court recorded that the server data had been seized in accordance with criminal procedure,⁷⁷ which is a statement about the lawfulness of the acquisition rather than about the integrity of what was acquired; the two are related but not identical, and only the first is addressed. In a prosecution for abuse of trust the court noted that, at the moment of extraction, the betting-site data surviving on the accused's computer covered only the period from 20 August to 20 November 2020.⁷⁸ That is the single observation in the dataset bearing on the completeness of recovered data, and it was made in passing.

Surveillance recordings furnish the widest spread of judicial treatment, from silence to examination. At one end, a theft prosecution lists "electronic evidence: eight video discs attached" among the materials and says nothing further about them;⁷⁹ a hotel theft in which on-premises footage identified the accused is treated as probative without procedural comment;⁸⁰ and in a card-cloning prosecution the extraction of hotel camera images is reported as an investigative result rather than as an evidentiary act.⁸¹ At the other end, a road-traffic prosecution states expressly that the USB holding the data extracted from the camera constitutes electronic

⁷⁶ Judgment No. 268/2024/HS-PT of 20 June 2024 of the High People's Court in Đà Nẵng. Available at: <https://congbobanan.toaan.gov.vn/2ta1528785t1cvn/chi-tiet-ban-an> (accessed on 20 March 2026).

⁷⁷ Judgment No. 85/2021/HS-ST of 21 June 2021 of the People's Court of Hải Phòng City. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-to-chuc-danh-bac-so-852021hsst-220986> (accessed on 20 March 2026).

⁷⁸ Judgment No. 85/2021/HS-ST of 21 June 2021 of the People's Court of Hải Phòng City. Ibid.

⁷⁹ Judgment No. 56/2017/HSST of 28 September 2017 of the People's Court of Kiến Xương District, Thái Bình Province. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).

⁸⁰ Judgment No. 45/2022/HS-ST of 31 March 2022 of the People's Court of Bình Thạnh District, Ho Chi Minh City. Available at: https://cdn.thuvienphapluat.vn/uploads/danluat/FileAttack/BA/313899/45_2022_HS-ST_HCM.pdf (accessed on 20 March 2026).

⁸¹ Judgment No. 141/2020/HS-PT of 5 March 2020 of the People's Court of Ho Chi Minh City. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-1412020hspt-ngay-05032020-ve-toi-su-dung-mang-may-tinh-phuong-tien-dien-tu-thuc-hien-ha-156002> (accessed on 20 March 2026).

evidence in the case and is to be retained on the file,⁸² and a public-order prosecution sent the eleven video files for forensic examination, which reported that no trace of cutting or alteration of the images had been found, returning the exhibits with a sixteen-page annex.⁸³ The last is the only integrity examination of an electronic item anywhere in the dataset. A prosecution for indecent acts against a child relied on a USB of camera clips and obtained a forensic conclusion, but on DNA rather than on the recording.⁸⁴

Finally, a prosecution for the unlawful acquisition, storage and resale of a dataset containing the records of more than 300,000 individuals rested on platform transaction records, banking records and the compromised dataset itself.⁸⁵ The judgment addresses neither the provenance of the dataset in the hands of the investigation nor the question, now unavoidable, whether its collection was consistent with data protection requirements. The case was decided before the Law on Personal Data Protection 2025 took effect, so the question could not have arisen in those terms; it will arise in those terms in comparable cases from now on.

4.3 Class (ii): Content composed by a person and stored electronically

Eight prosecutions rest on material authored by an individual: posts, messages, livestreams and self-recorded images. Here the decisive question is not whether a system functioned correctly but whether the person charged is the person who created and published the material. That is a question of attribution, and it is answered in the dataset only once.

In the two prosecutions for humiliating another person under article 155 of the Penal Code the courts relied on screenshots, access records and platform activity. In the first the accused entered his wife's Facebook account and posted intimate video and defamatory material visible to her entire network;⁸⁶ in the second the accused disseminated sensitive images of a former acquaintance over several months.⁸⁷ The second judgment records that the handset was sealed in a marked envelope with both IMEI numbers and both subscriber numbers noted: careful treatment of the device, and no treatment at all of the screenshots on which the conviction turned.

⁸² Judgment No. 55/2022/HS-ST of 14 September 2022 of the People's Court of Hoàng Hóa District, Thanh Hóa Province. Reproduced in FDVN Law Firm, *Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử* [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).

⁸³ Judgment No. 42/2025/HS-PT of 16 May 2025 of the People's Court of Hải Dương Province. Reproduced in FDVN Law Firm, *Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử* [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).

⁸⁴ Judgment No. 232/2020/HS-ST of 11 September 2020 of the People's Court of Thủ Đức District, Ho Chi Minh City. Reproduced in FDVN Law Firm, *Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử* [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).

⁸⁵ Judgment No. 628/2023/HS-PT of 28 December 2023 of the High People's Court in Đà Nẵng. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-su-dung-trai-phep-thong-tin-mang-may-tinh-mang-vien-thong-so-6282023hspt-313277> (accessed on 20 March 2026).

⁸⁶ Judgment No. 13/2024/HSST of 8 March 2024 of the People's Court of Y District, Ninh Bình Province. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-lam-nhuc-nguoi-khac-so-132024hsst-336963> (accessed on 20 March 2026).

⁸⁷ Judgment No. 93/2021/HSST of 27 July 2021 of the People's Court of P District, Thái Nguyên Province. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-lam-nhuc-nguoi-khac-so-932021hsst-238833> (accessed on 20 March 2026).

The same pattern appears in the two extortion prosecutions, one in which a juvenile accessed his father's iCloud account and used the images to extort the person depicted through fabricated Zalo and Facebook accounts,⁸⁸ the other in which video obtained from a former partner was used to extort the victim's sister;⁸⁹ in a gambling prosecution built on Zalo message threads recording lottery bets;⁹⁰ and in a network fraud prosecution turning on Facebook accounts and copied product images.⁹¹ None of these six judgments discusses how authorship was established or how the integrity of the material was verified.

The two prosecutions under article 117 of the Penal Code stand apart. In the first, the handsets were sealed in numbered envelopes bearing the signatures of those present and the seal of the ward police; the content of ten Facebook livestreams was printed and the accused signed every page, as he did every page of the extract of handset data; and the provincial Department of Information and Communications produced a requisitioned expert conclusion.⁹² In the second, the extraction of data from two Facebook accounts was carried out by the security investigation body together with the cyber-security unit and the People's Procuracy of the city, and four expert conclusions were obtained over three years.⁹³

The second of these judgments contains the only passage in the dataset that states an authentication standard. The appellate court recorded that the investigating body had not established when the seized material was composed, on what device, by whom it was posted, or by what method, the accused having asserted that he had lost control of the account. Those four elements are precisely the test that the CPC 2015 nowhere supplies, and the court arrived at them without any legislative warrant, simply by asking what would have to be shown before the material could be attributed to the accused. The significance of the passage lies less in its content than in its isolation. The same species of Facebook material, presenting the same attribution problem, passed unexamined in the six prosecutions described above.

⁸⁸ Judgment No. 10/2023/HS-ST of 23 March 2023 of the People's Court of Đắk Song District, Đắk Nông Province. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-cuong-doat-tai-san-so-102023hsst-285153> (accessed on 20 March 2026).

⁸⁹ Judgment No. 01/2023/HSST of 4 January 2023 of the People's Court of Kỳ Anh District, Hà Tĩnh Province. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).

⁹⁰ Judgment No. 770/2023/HS-PT of 11 October 2023 of the High People's Court in Hà Nội. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).

⁹¹ Judgment No. 108/2019/HSPT of 10 April 2019 of the High People's Court in Đà Nẵng. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-1082019hspt-ngay-10042019-ve-toi-su-dung-mang-may-tinh-mang-vien-thong-phuong-tien-dien-81995> (accessed on 20 March 2026).

⁹² Judgment No. 18/2024/HS-ST of 17 December 2024 of the People's Court of Quảng Ngãi Province. Available at: <https://congbobanan.toaan.gov.vn/3ta1707672t1cvn/> (accessed on 20 March 2026).

⁹³ Judgment No. 626/2023/HS-PT of 29 August 2023 of the High People's Court in Ho Chi Minh City. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).

4.4 Class (iii): Artefacts created by the investigation itself

A category of evidence runs through the dataset without ever being named in it. Screenshots of message threads, USB copies of camera footage, printed extracts of livestream content, transcripts and extraction reports did not exist before the investigation produced them. They are not records of the offence; they are records of the investigation's encounter with the record of the offence. Their reliability rests entirely on how they were made, which is to say on the chain of custody in its strict sense, and it cannot be tested by inspecting the artefact itself.

Three techniques for authenticating such artefacts appear in the dataset, each exactly once. The accused's signature on every page of a printed extract, in the Quang Ngai prosecution, converts the artefact into something the accused has adopted. The presence of the procuracy during extraction, in the Ho Chi Minh City prosecution, supplies an independent witness to the process. Forensic examination of the files, in the Hai Duong prosecution, tests the artefact against the possibility of alteration. Each is a serviceable answer to the problem; none is required by any provision; and in the remaining seventeen prosecutions none of the three was used. Screenshots in particular (the artefact most easily fabricated and the one on which several convictions principally rested) are nowhere examined, and no judgment records who made them, when, or from what display.

4.5 Two cases at the boundary

Two prosecutions in the dataset mark the limits of the concept and are instructive for that reason. The first concerned the installation of VoIP GSM gateway devices to route international telecommunications traffic outside the licensed network, causing losses to state revenue exceeding 3.5 billion Vietnamese dong.⁹⁴ The proof consisted of the seized devices, an expert conclusion of the Ministry of Information and Communications on their function, and a determination that they bore no conformity marking. No electronic data were tendered. The case concerns electronic means within the meaning of the 2023 Law on Electronic Transactions, not electronic data within the meaning of article 99 of the CPC 2015, and it illustrates why the distinction between the two terms has practical consequences rather than merely terminological ones.

The second is the converse. A patrol conducted an administrative check on a person suspected of online gambling; he stated that he was using his telephone to view customers' winnings and losses; the handset was seized and a record of the administrative check drawn up.⁹⁵ The scale of his participation was then established from his statements. The judgment records no extraction from the seized handset and no examination of its contents. A device known to contain the operative record of the offence was taken into custody and, so far as the judgment discloses, never interrogated. The case is a reminder that the deficiencies traced in Part 3 are not only about how electronic data are handled once collected, but also about the absence of any requirement that they be collected at all.

⁹⁴ Judgment No. 406/2019/HSPT of 18 July 2019 of the High People's Court in Hà Nội. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-4062019hspt-ngay-18072019-ve-toi-su-dung-mang-may-tinh-mang-vien-thong-phuong-tien-dien-135351> (accessed on 20 March 2026).

⁹⁵ Judgment No. 268A/2022/HSST of 21 November 2022 of the People's Court of Hai Bà Trưng District, Hà Nội City. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-danh-bac-cuoc-so-lo-de-qua-mang-internet-so-268a2022hsst-320770> (accessed on 20 March 2026).

4.6 Observations on the judgment data

A systematic review of twenty cases yielded four findings across all four functional groups and revealed the current state of electronic evidence practice in Vietnamese criminal proceedings.

The first finding concerns the distribution of evidentiary care rather than its absence. Documentation of provenance does occur in the dataset, and where it occurs it is thorough. In the two prosecutions under article 117 of the Penal Code the handsets were sealed in numbered envelopes bearing the signatures of those present and the seal of the ward police; the printed extracts of livestream content and of handset data were signed by the accused on every page; the extraction of account data was carried out by the security investigation body together with the cyber-security unit and the People's Procuracy; and expert conclusions were obtained, four of them in one case. In a public-order case the eleven video files were sent for forensic examination, which reported no trace of cutting or alteration. In a traffic case the court expressly declared the USB holding the extracted camera data to be electronic evidence to be retained on the file. In the gambling prosecution concerning a commercial platform the court recorded that the server data had been seized in accordance with criminal procedure.

What is striking is where this care is absent. The same species of Facebook material that was sealed, signed, verified by the procuracy and examined by experts in the article 117 cases enters the file without a single line on its origin in the prosecutions for humiliating another person, for extortion and for gambling. Screenshots, printed message threads and USB copies, items of class (iii), which exist only because the investigation made them, are examined in one case out of the twenty. The variable that predicts evidentiary rigour in this dataset is therefore not the fragility of the data but the gravity and sensitivity of the charge. The practical consequence is that the assurance of integrity a defendant receives depends on the offence with which he is charged rather than on how readily the evidence against him could have been altered.

One judgment shows that the missing standard is nevertheless within reach of the courts as the law stands. On appeal in the article 117 case decided in Ho Chi Minh City the court recorded that the investigating body had not established when the seized material had been composed, on what device, by whom it had been posted, or by what method, the accused having asserted that he had lost control of the account. That formulation states, in four elements, precisely the authentication test that the CPC 2015 does not contain: time of creation, generating device, author, and method of publication. It was reached without any legislative amendment. Its isolation across twenty judgments is the measure of the problem: the standard exists in Vietnamese judicial reasoning, but only sporadically, and nothing in the Code requires courts to apply it.

The second finding is that authenticity is primarily established through confessions and oral testimony rather than through expert examination. In the majority of the twenty cases the defendant either pleaded guilty to the acts recorded in the electronic evidence or did not challenge its authenticity, and the courts appeared to consider the absence of such a challenge sufficient to establish the admissibility of the evidence. The evidential significance of this finding is that the Vietnamese system currently lacks a default requirement for independent expert examination of electronic evidence a requirement that would be triggered regardless of whether the defendant chooses to challenge the evidence.

The third finding concerns the recurring problem of cross-border access to data. At least four of the twenty cases involved electronic data stored on servers operated by foreign companies (primarily Meta Platforms (Facebook, Instagram, Messenger), and Telegram), with the judgments giving no explanation of how, or through what channel, access to that data was sought or obtained. In three of these cases, the

courts proceeded on evidence gathered by requesting the defendants to provide their own account data without any assessment of whether this method of collection was procedurally valid or whether the resulting evidence could be considered sufficient and not manipulated. This finding underscores the urgency of Vietnam's need for effective judicial assistance mechanisms and more importantly, for the kind of framework for direct cooperation with foreign service providers that the Second Additional Protocol to the Budapest Convention is designed to establish.

The fourth finding concerns the spread of electronic evidence across offence categories. The dataset covers fifteen categories of offence, and electronic data appear as the principal proof or as significant corroboration in prosecutions for theft, for road traffic offences, for disturbing public order and for abuse of trust, as well as in the prosecutions for computer and telecommunications offences with which the subject is conventionally associated. The dataset does not permit any statement about change over time, and none is made here: a purposive sample of twenty judgments selected for variation cannot establish a trend, and the published record itself begins only in 2017. What the dataset does establish is a point about the scope of the problem rather than its history. The procedural deficiencies identified in Part 3 are not confined to a specialised class of technological offences; they affect ordinary criminal adjudication, which is what makes their correction a matter for the Code rather than for specialist guidance.

5. Comparative perspectives on the deficiencies identified

Part 3 identified three deficiencies in the Vietnamese framework: admissibility criteria stated without any machinery for establishing them, no integrated chain of custody for electronic data, and no procedural power directed at data held abroad. Part 4 showed how each of these presents itself in adjudication. This Part asks how other systems have addressed the same three problems, and what of their answers can be carried across.

The comparators are not chosen for general similarity of legal system. Singapore and Malaysia are selected because they share Vietnam's exposure to transnational platforms holding the relevant data offshore, operate investigative bodies of comparable scale, and decisively resolved the authentication problem by statutory amendment rather than by incremental judicial development. A solution reached by legislation in a codified system is capable of being adopted by another codified system; a solution built from case law is not, at least not directly. The Budapest Convention with its Second Additional Protocol, the European Union instruments and the United Nations Convention against Cybercrime are examined because they address the cross-border problem, and because Vietnam has now assumed obligations under the last of them.

5.1 Authentication: From proof in each case to presumption

Article 99(3) of the CPC 2015 requires the evidentiary value of electronic data to be assessed by reference to the manner of its creation, storage and transmission, the manner in which its integrity was maintained, and the manner in which its originator is identified. These are the right questions. What the provision does not do is say who must answer them, by what means, or what follows if they are not answered. A Vietnamese court confronted with a server log has the criteria and no instrument.

Malaysia addressed the same difficulty in 1993 by inserting sections 90A to 90C into the Evidence Act 1950.⁹⁶ Section 90A(1) makes a document produced by a

⁹⁶ PARLIAMENT OF MALAYSIA. Evidence Act 1950 (Malaysia, Act 56) inserted by the Evidence (Amendment) (No. 2) Act 1993, Kuala Lumpur, 1993, ss. 90A, 90B and 90C. Available at:

computer admissible provided it was produced “in the course of its ordinary use”, and admissible whether or not tendered by its maker. Section 90A(2) allows that condition to be proved by a certificate signed by the person responsible for the management of the operation of the computer, or for the conduct of the activities for which the computer was used. Section 90A(4) attaches to that certificate a presumption that the computer was in good working order and operating properly in all respects. Section 90B governs the weight to be given to the document, and section 90C gives the two preceding sections precedence over any inconsistent provision of any other written law. The scheme therefore identifies a person who vouches for the machine, and converts that person’s statement into a presumption.

Malaysian case law has since loosened the scheme, and the direction of travel is instructive. In *Gnanasegaran* the Court of Appeal held that a certificate is not required in every case: the condition in section 90A(1) may equally be proved by oral evidence from a person familiar with the computer’s use, and section 90A was enacted, in the words of Mahadev Shankar JCA, to bring the best evidence rule up to date with the realities of the electronic age.⁹⁷ The Federal Court in *Ahmad Najib bin Aris* confirmed that a closed-circuit television recording is a document produced by a computer for these purposes,⁹⁸ a holding of direct relevance to the camera cases in Part 4. The criticism made of the Malaysian position is that the deeming provision in section 90A(6) has progressively absorbed the certificate requirement, so that the machinery which was to secure reliability now largely presumes it.

Singapore went further in 2012. The previous scheme, which required affirmative proof of reliability by a certificate explaining why the output could be trusted, was replaced by three rebuttable presumptions in section 116A of the Evidence Act 1893.⁹⁹ The first is that where a device or process is of a kind that, properly used, ordinarily produces or accurately communicates an electronic record, the court presumes that it did so on the occasion in question. The second is that a record made in the ordinary course of business by a person who is not a party to the proceedings, and whose making the proponent did not control, is presumed authentic. The third is that a record created by a party adverse in interest, and used against that party, is presumed authentic. Each presumption yields to evidence sufficient to raise a doubt, and section 116A(6) allows a record-keeping system to be certified as an “approved process” by a Certifying Authority appointed by the Ministry of Law. The drafting has been described judicially as clumsy,¹⁰⁰ but the structure is clear: the proponent is relieved of proving what is ordinarily true, and the opponent is given a defined route to displace the presumption.

A recent decision marks the limit of the technique and is the most useful part of the comparison for Vietnamese purposes. The Court of Appeal held that section 116A(1) presumes only that the record accurately reflects what the device produced or communicated; it does not presume that any analysis the device performed is

https://ccid.rmp.gov.my/Laws/Act_56_-_Evidence_Act_1950.pdf (accessed on 20 March 2026).

⁹⁷ MALAYSIAN COURT OF APPEAL. *Gnanasegaran a/l Pararajasingam v Public Prosecutor* [1997] 3 MLJ 1; [1997] 4 CLJ 6 (Court of Appeal, Malaysia).

⁹⁸ MALAYSIAN FEDERAL COURT. *Ahmad Najib bin Aris v Public Prosecutor* [2009] 2 MLJ 613. Available at: <https://supremetoday.ai/doc/judgement/MYS00000056376> (accessed on 01 March 2026).

⁹⁹ PARLIAMENT OF SINGAPORE. Evidence Act 1893 (Singapore, 2020 Rev Ed), inserted by the Evidence (Amendment) Act 2012, Singapore, 2020, s 116A. Available at: <https://sso.agc.gov.sg/Act/EA1893> (accessed on 10 March 2026).

¹⁰⁰ SINGAPORE HIGH COURT. *Telemedia Pacific Group Ltd v Credit Agricole (Suisse) SA (Yeh Mao-Yuan, third party)* [2015] 1 SLR 338; [2014] SGHC 235, at [248] and [250]. Available at: https://www.elitigation.sg/gd/s/2014_SGHC_235 (accessed on 10 March 2026).

correct.¹⁰¹ The distinction is exactly the one that Part 4 found the Vietnamese courts failing to draw when they treated an expert conclusion on the capability of a device as though it also established the integrity of the logs the device generated. A presumption about the fidelity of a record is not a presumption about the soundness of an inference drawn from it.

Outside the two core comparators, a third system is worth noting on this narrower point of authentication technique. The United States reaches a comparable result by a different route, through the self-authentication rules of the Federal Rules of Evidence: rule 902(13) for records generated by an electronic process or system, and rule 902(14) for data copied from an electronic device or file where the copy is authenticated by a process of digital identification, in practice a hash value, certified by a qualified person.¹⁰² Rule 902(14) is significant here because it is the point at which a technical act (the computation and recording of a hash) is given a defined legal consequence.

The lesson for Vietnam is not that any of these schemes should be transplanted. It is that each of them does two things Article 99(3) does not: it names the person who vouches, and it attaches a stated legal consequence to a stated technical act. That is the form the recommendation in Part 6 takes. A provision establishing a rebuttable presumption of integrity where a hash value was computed and recorded at the moment of seizure, displaceable by evidence raising a doubt, would give Vietnamese courts an instrument they presently lack, without importing the common-law model of a threshold ruling on admissibility before evidence is received, a model which does not fit a system in which the court evaluates the file as a whole.

5.2 Chain of custody: Standards that Vietnam has adopted but not required

The technical content of a chain of custody is not contested internationally. ISO/IEC 27037:2012 sets out the identification, collection, acquisition and preservation of digital evidence as documented procedures each step of which can be independently inspected and verified,¹⁰³ and the guidance issued for first responders in the United Kingdom and by INTERPOL translates the standard into operational practice.¹⁰⁴ Vietnam has already adopted the standard as TCVN ISO/IEC 27037:2019. What it has not done is give it normative force in criminal procedure. The gap is therefore not one of knowledge or of access to technical material, and it cannot be closed by further study; it is a gap in legal obligation, and it can be closed by an implementing instrument without waiting for amendment of the Code.

Three requirements would carry most of the weight, and each corresponds to a failure identified in Part 4. A hash value computed and recorded at the moment of seizure would supply the objective basis for integrity that the twenty judgments sought instead in the accused's admissions. Forensic imaging in place of selective copying would address the class of artefacts examined in section 4.4, whose reliability

¹⁰¹ COURT OF APPEAL OF THE REPUBLIC OF SINGAPORE. *GIL v Public Prosecutor* ([2025] SGCA 21) [2025] SGCA 21. Available at: https://www.elitigation.sg/gd/s/2025_SGCA_21 (accessed on 10 April 2026).

¹⁰² UNITED STATES CONGRESS. Federal Rules of Evidence, Washington DC, 1975 (Pub. L. 93-595, as amended), Rules 902(13) and 902(14). Available at: https://www.law.cornell.edu/rules/fre/rule_901 and https://www.law.cornell.edu/rules/fre/rule_902 (accessed on 05 March 2026).

¹⁰³ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27037:2012, Guidelines for the Identification, Collection, Acquisition and Preservation of Digital Evidence, International Organization for Standardization, Geneva, 2012. Ibid.

¹⁰⁴ INTERPOL. Guidelines for digital forensics first responders: Best practices for search and seizure of electronic and digital evidence, Lyon, 2021. Available at: https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf (accessed on 05 March 2026).

presently depends on an undocumented act of the investigation. An access log recording who handled the data, when and with what tool would supply what the appellate court in the Ho Chi Minh City prosecution found to be missing when it observed that the investigating body had not established when the material was composed, on what device, by whom it was posted or by what method.

5.3 Cross-border access: From aspiration to obligation

The Budapest Convention equips States Parties with a defined set of procedural powers over electronic data: expedited preservation of stored data, production orders, search and seizure of stored computer data, and real-time collection, each subject to the conditions and safeguards required by article 15.¹⁰⁵ The Second Additional Protocol adds mechanisms that operate directly between a State and a service provider in another State: direct requests for subscriber information, and arrangements for giving effect to orders issued by another Party, both accompanied by data protection safeguards.¹⁰⁶ The European Union has built a comparable structure by pairing a Regulation on European production and preservation orders with a Directive requiring providers to designate an establishment or legal representative to receive them;¹⁰⁷ the Regulation without the Directive would have had no addressee, which is a point of drafting technique worth noting for any Vietnamese equivalent.

For Vietnam the question is no longer whether to draw on these models. Chapter IV of the United Nations Convention against Cybercrime requires States Parties to establish, in domestic law, the same family of procedural powers over electronic data, together with corresponding conditions and safeguards, and Chapter V provides the cooperation framework.¹⁰⁸ Vietnam ratified the Convention in April 2026. The CPC 2015 contains none of these powers: there is no preservation order, no production order addressed to a service provider, and no procedure for a request to a foreign provider. Part 4 found four prosecutions in which the relevant data were held on servers operated abroad, and in three of them the courts proceeded on material the accused had been directed to produce from his own account. The judgments do not explain how the data held by foreign service providers were obtained or authenticated in those cases. Creating the alternative is now an implementation obligation, and the interval before the Convention enters into force is the period in which it must be discharged.

5.4 Pairing power with condition

A feature common to all four instruments deserves separate notice because it bears directly on the analysis in section 3.4. In each of them a power to reach electronic data is created together with the conditions under which it may be exercised: article 15 of the Budapest Convention, article 14 of the Second Additional Protocol, the issuing conditions and review mechanism of the European Regulation,

¹⁰⁵ COUNCIL OF EUROPE. Convention on cybercrime (Budapest Convention), ETS No. 185, Budapest. 2001. Available at: <https://www.coe.int/en/web/cybercrime/convention-on-cybercrime> (accessed on 25 March 2026).

¹⁰⁶ COUNCIL OF EUROPE. Second additional protocol to the convention on cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), opened for signature in Strasbourg on 12 May 2022. Ibid.

¹⁰⁷ OFFICIAL JOURNAL OF THE EUROPEAN UNION. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings (OJ L 191, 28.7.2023). Ibid.

¹⁰⁸ UNITED NATIONS. United Nations Convention against Cybercrime, Hanoi, 2025. Chapters IV and V. Available at: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html> (accessed on 20 March 2026).

and the conditions and safeguards provisions of the Hanoi Convention. None of them creates an unconditioned power.

The CPC 2015 does the opposite in a specific and remediable way. It attaches conditions to the narrower powers (procuratorial approval for the seizure of postal and telecommunications items, and approval, offence limits and time limits for the covert collection of electronic data) while leaving the broader power, the overt extraction of the entire contents of a device under Articles 107 and 196, without approval, scope or time limit. Measured against the comparators, the deficiency is not that Vietnamese law lacks a tradition of conditioning investigative powers. It plainly has one. The deficiency is that the condition was attached to the measure the legislature perceived as intrusive in 2015, and the perception has not been revised. Table 4 sets the position under the CPC 2015 alongside that of Singapore, Malaysia and the three international instruments examined in this Part, across the five dimensions on which the foregoing comparison has turned.

Table 4. Treatment of electronic evidence across the comparators.

System	Status of electronic data	Mechanism for authentication	Chain of custody	Cross-border access	Conditions attached to the power
Vietnam	Independent source of evidence, art. 87(1)(c) CPC 2015; not an exhibit	Art. 99(3) states criteria; no presumption, no certificate, no responsible person identified	No integrated requirement; sealing of the device only	No preservation order, no production order, no provider procedure	Approval required for postal seizure and covert collection; none for overt extraction under arts. 107 and 196
Singapore	Electronic record within the Evidence Act 1893	s 116A: three rebuttable presumptions; s 116A(6) approved process certified by a Certifying Authority	Practice-based, not statutory	Mutual legal assistance	Presumption displaced by evidence sufficient to raise a doubt
Malaysia	Document produced by a computer, ss 90A–90C Evidence Act 1950	s 90A(2) certificate by the person responsible for the computer; s 90A(4) presumption of proper working order; s 90A(6) deeming provision	Practice-based, not statutory	Mutual legal assistance	Certificate optional in practice after Gnanasegaran; weight governed by s 90B
Budapest Convention and Second Additional Protocol	Stored computer data and traffic data	Left to domestic law	Left to domestic law	Arts. 16–21; Protocol arts. 7 and 8 for direct requests to providers	Art. 15 conditions and safeguards; Protocol art. 14 data protection safeguards
European Union	Electronic evidence in criminal proceedings	Left to national law	Left to national law	Regulation (EU) 2023/1543 production and preservation orders; Directive (EU)	Issuing conditions and review mechanism within the Regulation

System	Status of electronic data	Mechanism for authentication	Chain of custody	Cross-border access	Conditions attached to the power
				2023/1544 designated establishments	
United Nations Convention against Cybercrime	Electronic data	Left to domestic law	Left to domestic law	Chapter IV domestic procedural powers; Chapter V cooperation	Conditions and safeguards required alongside each power

Two columns of Table 4 are worth reading together. In the authentication column Vietnam is the only system that states criteria without supplying an instrument for satisfying them; every other system either creates a presumption or nominates a person who vouches, and most do both. In the final column Vietnam is the only system in which a power to reach electronic data exists without any attached condition, and it is not the case that Vietnamese law is unfamiliar with conditioning such powers, since it conditions two narrower ones. The two observations point to the same conclusion, and it is a conclusion about drafting rather than about legal culture: the CPC 2015 legislated for the electronic device and left the electronic datum to be governed by provisions written for physical things.

A question arises at this point which the comparison itself cannot answer: whether a Vietnamese court, confronted with the gap identified in Part 3, may close it by reference to the standards described above. The answer is largely negative, and the reasons are worth stating because they determine the form the recommendations in Part 6 must take. Under the Law on Treaties 2016 a treaty to which Vietnam is a party prevails over a domestic legal instrument other than the Constitution where the two conflict, and a treaty provision that is sufficiently clear and detailed may be applied directly

¹⁰⁹ Vietnam is now a party to the United Nations Convention against Cybercrime. But the obligations in Chapter IV are obligations to legislate: they require States Parties to establish procedural powers in domestic law, and a provision of that character cannot be applied by a court in place of the legislation it calls for.

The difficulty is compounded by the structure of Vietnamese evidence law itself. Article 87(2) of the CPC 2015 denies legal value to material not collected in accordance with the order and procedures prescribed by that Code.¹¹⁰ The exclusionary rule is thus keyed to domestic procedure, and where domestic procedure prescribes nothing there is nothing for the rule to bite on. A court cannot exclude an extraction for want of a hash value, because no provision requires a hash value; nor can it treat compliance with ISO/IEC 27037 as a condition of admissibility, because the standard has been adopted as a technical standard and not as a rule of procedure. The gap is not one that judicial interpretation is equipped to close.

Two things nevertheless remain open to the courts, and the dataset shows both being done. The first is to require reasoning: the appellate court in the Ho Chi Minh City prosecution asked when the material was composed, on what device, by whom it was posted and by what method, and found the investigation had not answered. Nothing prevented that, and nothing prevents its repetition. The second is guidance. A resolution of the Council of Judges of the Supreme People's Court, or a joint circular of the kind that has been used before in this field, could require those four questions

¹⁰⁹ VIETNAMESE NATIONAL ASSEMBLY. Law on Treaties 2016, Hanoi, 2016. Art. 6(1). Ibid.

¹¹⁰ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Art. 87(2). Available at: <https://www.wipo.int/wipolex/en/text/585372> (accessed on 20 April 2026).

to be addressed whenever electronic evidence is relied on, and could prescribe hash verification and forensic imaging as the ordinary means of answering them. That instrument would not amend the Code and would not create an exclusionary consequence, but it would convert an isolated instance of good practice into an expectation. It is on that basis that the recommendations below are arranged in three tiers.

6. Recommendations

The six recommendations that follow are arranged by the type of legal instrument required and the timeframe necessary for their implementation. The first tier can be implemented by subordinate instrument without amending the Code and could take effect within the current legislative cycle. The second requires amendment of the CPC 2015. The third depends on treaty implementation and on bilateral negotiation, and will run over a longer period. The sequence matters: the first tier is not a provisional substitute for the second but the prerequisite for its effectiveness, since a statutory chain of custody without established technical practice would produce records rather than reliability.

6.1 Consolidating and completing Articles 107 and 196 (second tier: Amendment of the code)

The first task is not definitional. A statutory definition of “electronic evidence” would merely restate the existing terms of Article 86 without providing actionable guidance on what investigator must do or what a court must require. As argued in section 3.1, the distinctiveness of electronic evidence lies in procedure rather than in taxonomy, and the reform should follow this reality. What is required is that Articles 107 and 196 be merged into a single provision, provisionally entitled “Collection of electronic data and seizure of electronic means”, which separates the procedural stages of seizure, collection, copying and preservation, and prescribes the record to be drawn up at each. The structural conflict between the two articles analysed in section 3.3 is the source of the uncertainty described there, and consolidation is the condition of every other reform proposed below, since a requirement cannot be attached to a stage that the Code does not distinguish.

The consolidated provision should also close the two gaps identified in section 3.3: it should prescribe a time limit, a method and a means of verification for copying under what is presently Article 107(2), and it should provide for the recovery of deleted data before collection, which the present Article 107(3) does not reach.¹¹¹

6.2 A mandatory chain of custody and hash verification (first tier: Subordinate instrument)

A specific provision should require that every seized electronic device and every item of electronic data collected be accompanied by a continuous record identifying each person who held the device or the data, the time and place of each transfer, the condition of the device or data at each transfer, and the measures taken to prevent alteration or contamination. Because this requirement is technical rather than structural it does not depend on amendment of the Code and could be issued as an implementing circular or as a resolution of the Council of Judges, which is why it is placed in the first tier. It should be anchored in ISO/IEC 27037:2012, adopted in Vietnam as TCVN ISO/IEC 27037:2019, and in the INTERPOL guidance for first responders, neither of which the Vietnamese procedural framework has yet absorbed.

¹¹¹ VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Art. 107(3). Available at: <https://www.wipo.int/wipolex/en/text/585372> (accessed on 20 April 2026).

The mandatory use of hash value verification (a standard forensic technique for establishing the integrity of digital data) should be required specifically for all evidence stored electronically. That would give courts an objective and verifiable basis for assessing the integrity of evidence independently of investigator testimony or defendant confession. The instrument should also designate the competent authority responsible for authorising and supervising this process, whether the investigating body itself under prosecutorial oversight or a specialised digital-forensic unit for complex seizures, and should specify the consequence of non-compliance: evidence collected or preserved without the required chain-of-custody record should be treated as inadmissible, or at minimum as carrying diminished probative weight, unless the prosecution otherwise establishes its integrity.

6.3 A framework for cross-border access to data (third tier: Treaty implementation)

The problem of data held on servers operated by foreign providers, present in at least four of the twenty judgments, requires a legislative and diplomatic response rather than a procedural one alone. These four judgments illustrate an absence of judicial explanation as to how such data were obtained; on their own, they do not establish that existing cooperation mechanisms have failed in practice. The case for reform rests instead on the normative gaps in the CPC 2015 and on the obligations Vietnam assumed in ratifying the United Nations Convention against Cybercrime, addressed below. In the short term Vietnam should accelerate bilateral mutual legal assistance arrangements with the jurisdictions in which the principal platforms are established, chiefly the United States and Ireland, addressing specifically the disclosure of electronic evidence in criminal proceedings and incorporating the procedural safeguards and time limits of the Second Additional Protocol to the Budapest Convention. In the medium term the decisive step is the implementation in domestic law of the powers required by Chapter IV of the United Nations Convention against Cybercrime, to which Vietnam is already a party: expedited preservation, production orders addressed to service providers, and a procedure for requests to providers established abroad.

Accession to the Budapest Convention should be assessed separately and on a narrower ground. What that Convention adds, through Articles 7 and 8 of its Second Additional Protocol, is a mechanism operating directly between a requesting State and a provider in another State, and a means of giving effect to orders issued by another Party. That is a degree of directness the Hanoi Convention does not achieve. Whether it justifies accession is a question that extends beyond legal calculation, and this article does not attempt to answer it.

6.4 Conditions on the use of personal data as criminal evidence (second tier: Amendment of the Code)

The exemption in Article 19(1) of the Law on Personal Data Protection 2025 removes consent as an obstacle to criminal investigation but supplies no conditions. The reform required is therefore not a further exemption but a set of statutory conditions attached to the existing one, establishing when the collection, processing and retention of personal data for criminal evidentiary purposes is lawful and prescribing the procedural safeguards applicable to it. At a minimum that framework should address the categories of personal data that may be collected as criminal evidence without the data subject's consent; the period for which such data may be retained; the mechanisms of judicial oversight over data-collection decisions; the data subject's right to challenge the use of their personal data as evidence in criminal proceedings; and a supervision mechanism for investigative processing, giving effect in criminal procedure to the duty imposed by Article 19(2) of the Law.

6.5 Technical capacity and mandatory expert involvement (first and second tiers)

Implementing the chain of custody requirement and raising the general standard of practice will require sustained investment in the technical capacity of investigating, prosecuting and adjudicating bodies: specialised training in digital forensics for the units that regularly handle electronic evidence, and a working knowledge of the principles of integrity and of the applicable procedural requirements among criminal justice practitioners generally. This belongs to the first tier because it can begin at once and because the instruments in section 6.2 will not operate without it.

The CPC 2015 needs to be amended to mandate the involvement of a qualified forensic expert in the seizure of complex electronic devices and data storage systems, a reform that would address the recurring gap noted in the case analysis above: the judgments examined do not indicate whether a forensic expert was involved in assessing the integrity of the data or what measures were taken to safeguard it. This is consistent with international best practice; both the INTERPOL Guidelines and the ISO/IEC 27037 standard anticipate the involvement of forensic experts in the process of collecting evidence, and not only in the subsequent examination of evidence already collected. That involvement should be mandatory whenever the device or data storage system requires specialised extraction methods, involves encrypted or remotely stored data, or where the authenticity of the data is contested, rather than being left to the discretion of the investigating officer in each case.

6.6 Institutional framework for international cooperation (third tier)

Vietnam should develop a framework for international cooperation directed specifically at the demands of digital investigation, supplementing the general regime of mutual legal assistance. It should address not only the formal mechanisms for requesting and transmitting electronic evidence in individual proceedings, but also the institutional relationships between investigating bodies, between procuracies and between courts on which cooperation in complex multi-jurisdictional investigations depends.

In this area, Vietnam would benefit from its engagement with the UNODC cybercrime program and from its participation in the law enforcement cooperation network maintained by the Budapest Convention framework. These international relationships not only provide access to official legal documents but also to the accumulated practical experience of countries that have developed and perfected their digital forensic capabilities for a significantly longer period than Vietnam.

6.7 Difficulties of implementation

The recommendations above would meet resistance of four kinds, and a proposal that does not acknowledge them is of limited use to the bodies that would have to act on them. The first is cost. Forensic imaging and hash verification at the point of seizure require write blockers, imaging equipment and trained operators at district level, not only in the specialised units of the Ministry of Public Security. The equipment is not expensive by the standards of criminal justice budgets; the training and the maintenance of competence are.

The second is the absence of an operational standard. TCVN ISO/IEC 27037:2019 states principles; it does not prescribe which tools are acceptable, how a hash is to be recorded in a Vietnamese procedural document, or what an investigator should do when a device cannot be imaged. Until a technical standard of that kind exists, a statutory requirement would be applied unevenly and would in practice mean whatever each investigating body took it to mean.

The third is the risk that a chain of custody becomes a paper exercise. The dataset already contains an instance of documentation performing an evidentiary function

well (the accused's signature on each page of the printed extract) and instances of documentation performing none. A requirement to keep a record will produce records; whether it produces reliability depends on whether anything turns on the record when the evidence is challenged, which in turn depends on the courts asking the four questions identified in section 4.3.

The fourth is institutional capacity in forensic examination. Making expert examination of electronic data mandatory, as section 6.5 proposes, would increase demand on a small number of facilities concentrated in the Ministry of Public Security and its provincial technical units. Meeting that demand would require either a substantial expansion of those facilities or the accreditation of examiners outside them, and the second raises questions of independence and of standards that would themselves need to be settled by regulation.

7. Conclusion

This article analyzes the legal framework and judicial practice regarding electronic evidence in Vietnamese criminal proceedings, drawing three main conclusions. First, the CPC 2015 possesses a solid conceptual structure but suffers from serious shortcomings. It contains no codified chain-of-custody requirement for electronic data, and across the twenty reviewed judgments, no court articulated any basis for establishing data authenticity or integrity beyond the defendant's admissions and the apparent consistency of the records with other evidence. Second, electronic evidence appears across the full range of offence categories and at every tier of court represented in the dataset, in prosecutions for theft, road traffic offences and disturbing public order as much as in prosecutions for computer and telecommunications offences. The deficiencies of the framework are therefore not confined to a specialised class of case; they affect ordinary criminal adjudication. Third, the Law on Personal Data Protection 2025 exempts criminal investigation from the consent requirement while leaving the conditions of that exemption to a procedural law that does not supply them. Articles 107 and 196 of the CPC 2015 permit the extraction of private data without approval, without a defined scope and without a time limit, while the Code requires procuratorial approval for the seizure of physical correspondence and for the covert collection of electronic data. That asymmetry, rather than any conflict between the two regimes, is what requires legislative attention. The article proposes six reforms, arranged in three tiers according to the instrument each requires: a chain of custody with hash verification and investment in technical capacity, both achievable by subordinate instrument; the consolidation of Articles 107 and 196 and the attachment of conditions to the use of personal data as evidence, both requiring amendment of the Code; and a framework for cross-border access together with an institutional basis for cooperation, both dependent on implementation of the obligations Vietnam assumed on ratifying the United Nations Convention against Cybercrime. A limitation of the study is that it relies only on published judgments, excluding the investigation and prosecution phases. Future research should combine judgment analysis with surveys of investigative practices particularly the relationship between personal data protection and the use of evidence in criminal proceedings.

8. References

- BACHMAIER WINTER, L. and QUERALT, J. *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge: Cambridge University Press. 2018. Available at: <https://doi.org/10.1017/9781009049771> (accessed on 25 March 2026).
- BÙI HẢI HIẾU. *On some aspects of electronic data in criminal procedure*. Protection of Law newspaper (Kiểm sát), 2021. Available at: <https://baovephapluat.vn/cai-cach-tu-phap/dien-dan/ban-ve-mot-so-khia-can-h-cua-du-lieu-dien-tu-trong-to-tung-hinh-su-116824.html> (accessed on 20 March 2026).

- CAO ANH ĐỨC and NGÔ THỊ BÍCH THU. "Measures for collecting, transforming and using electronic evidence in high-tech crime cases". *Journal of Procuracy*, 2020. Available at: <https://kiemsat.vn/bien-phap-thu-thap-chuyen-hoa-su-dung-chung-cu-dien-tu-trong-vu-an-su-dung-cong-nghe-cao-62958.html> (accessed on 15 March 2026).
- CASEY, E. *Digital evidence and computer crime: Forensic science, computers and the internet*, 3rd ed. Waltham (MA): Academic Press, 2011, pp. 7-12. Available at: <https://archive.org/details/digitalevidenc0003case> (accessed on 25 March 2026).
- COUNCIL OF EUROPE. Convention on cybercrime (Budapest Convention), ETS No. 185, Budapest. 2001. Available at: <https://www.coe.int/en/web/cybercrime/convention-on-cybercrime> (accessed on 25 March 2026).
- COUNCIL OF EUROPE. Second additional protocol to the convention on cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), opened for signature in Strasbourg on 12 May 2022. Available at: <https://www.coe.int/en/web/cybercrime/second-additional-protocol> (accessed on 19 April 2026).
- COURT OF APPEAL OF THE REPUBLIC OF SINGAPORE. GIL v Public Prosecutor ([2025] SGCA 21) [2025] SGCA 21. Available at: https://www.elitigation.sg/gd/s/2025_SGCA_21 (accessed on 10 April 2026).
- DINH THE HUNG. "The legal framework of electronic evidence in vietnamese criminal procedure: From the budapest convention to domestic legislation". *Access to Justice in Eastern Europe*, vol. 8, no. 4, 2025, pp. 301-339. Available at: <https://doi.org/10.33327/AJEE-18-8.4-a000142> (accessed on 05 March 2026).
- DUONG QUYNH HOA. "Electronic evidence and electronic evidence storage using Blockchain technology: China's experience and implications for Vietnam". *Vietnam Journal of Social Sciences*. 2024. Available at: <https://vjol.info.vn/khxbvn/article/view/108622> (accessed on 05 March 2026).
- GIOVA, G. "Improving chain of custody in forensic investigation of electronic digital systems". *International Journal of Computer Science and Network Security (IJCSNS)*, v. 11, n. 1, 2011, pp. 1-9. Available at: http://paper.ijcsns.org/07_book/201101/20110101.pdf (accessed on 25 April 2026).
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27037:2012, Guidelines for the Identification, Collection, Acquisition and Preservation of Digital Evidence, International Organization for Standardization, Geneva, 2012. Available at: <https://www.iso.org/standard/44381.html> (accessed on 20 April 2026).
- INTERPOL. Guidelines for digital forensics first responders: Best practices for search and seizure of electronic and digital evidence, Lyon, 2021. Available at: https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf (accessed on 05 March 2026).
- Judgment No. 01/2023/HSST of 4 January 2023 of the People's Court of Kỳ Anh District, Hà Tĩnh Province. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).
- Judgment No. 10/2023/HS-ST of 23 March 2023 of the People's Court of Đắk Song District, Đắk Nông Province. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-cuong-doat-tai-san-so-102023hsst-285153> (accessed on 20 March 2026).
- Judgment No. 108/2019/HSPT of 10 April 2019 of the High People's Court in Đà Nẵng. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-1082019hspt-ngay-10042019-ve-toi-su-dung-mang-may-tinh-mang-vien-thong-phuong-tien-dien-81995> (accessed on 20 March 2026).
- Judgment No. 13/2024/HSST of 8 March 2024 of the People's Court of Y District, Ninh Bình Province. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-lam-nhuc-nguoi-khac-so-132024hsst-336963> (accessed on 20 March 2026).
- Judgment No. 141/2020/HS-PT of 5 March 2020 of the People's Court of Ho Chi Minh City. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-1412020hspt-ngay-05032020-ve-toi-su-dung-mang-may-tinh-phuong-tien-dien-tu-thuc-hien-ha-156002> (accessed on 20 March 2026).

- Judgment No. 18/2024/HS-ST of 17 December 2024 of the People's Court of Quảng Ngãi Province. Available at: <https://congbobanan.toaan.gov.vn/3ta1707672t1cvn/> (accessed on 20 March 2026).
- Judgment No. 232/2020/HS-ST of 11 September 2020 of the People's Court of Thủ Đức District, Ho Chi Minh City. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).
- Judgment No. 268/2024/HS-PT of 20 June 2024 of the High People's Court in Đà Nẵng. Available at: <https://congbobanan.toaan.gov.vn/2ta1528785t1cvn/chi-tiet-ban-an> (accessed on 20 March 2026).
- Judgment No. 268A/2022/HSST of 21 November 2022 of the People's Court of Hai Bà Trưng District, Hà Nội City. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-danh-bac-cuoc-so-lo-de-qua-mang-internet-so-268a2022hsst-320770> (accessed on 20 March 2026).
- Judgment No. 406/2019/HSPT of 18 July 2019 of the High People's Court in Hà Nội. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-4062019hspt-ngay-18072019-ve-toi-su-dung-mang-may-tinh-mang-vien-thong-phuong-tien-dien-135351> (accessed on 20 March 2026).
- Judgment No. 42/2025/HS-PT of 16 May 2025 of the People's Court of Hải Dương Province. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).
- Judgment No. 45/2022/HS-ST of 31 March 2022 of the People's Court of Bình Thạnh District, Ho Chi Minh City. Available at: https://cdn.thuvienphapluat.vn/uploads/danluat/FileAttack/BA/313899/45_2022_HS-ST_HCM.pdf (accessed on 20 March 2026).
- Judgment No. 55/2022/HS-ST of 14 September 2022 of the People's Court of Hoàng Hóa District, Thanh Hóa Province. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).
- Judgment No. 56/2017/HSST of 28 September 2017 of the People's Court of Kiến Xương District, Thái Bình Province. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).
- Judgment No. 626/2023/HS-PT of 29 August 2023 of the High People's Court in Ho Chi Minh City. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).
- Judgment No. 628/2023/HS-PT of 28 December 2023 of the High People's Court in Đà Nẵng. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-su-dung-trai-phep-thong-tin-mang-may-tinh-mang-vien-thong-so-6282023hspt-313277> (accessed on 20 March 2026).
- Judgment No. 770/2023/HS-PT of 11 October 2023 of the High People's Court in Hà Nội. Reproduced in FDVN Law Firm, Tổng hợp 20 bản án hình sự có sử dụng chứng cứ điện tử [Compilation of twenty criminal judgments using electronic evidence], available at: <https://fdvn.vn/wp-content/uploads/2025/07/luu-ban-nhap-tu-dong-5-47.pdf> (accessed on 20 March 2026).
- Judgment No. 790/2023/HS-PT of 29 September 2023 of the High People's Court in Ho Chi Minh City. Available at: <https://congbobanan.toaan.gov.vn/3ta1348649t1cvn/> (accessed on 20 March 2026).
- Judgment No. 85/2021/HS-ST of 21 June 2021 of the People's Court of Hải Phòng City. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-to-chuc-danh-bac-so-852021hsst-220986> (accessed on 20 March 2026).

- Judgment No. 93/2021/HSST of 27 July 2021 of the People's Court of P District, Thái Nguyên Province. Available at: <https://thuvienphapluat.vn/banan/ban-an/ban-an-ve-toi-lam-nhuc-nguoi-khac-so-932021hsst-238833> (accessed on 20 March 2026).
- KALANCHIA, I., BOZHYK, V., MUZYCHENKO, O. and VATSIYK, V. "Digital evidence in comparative criminal procedure: International experience and the practice of judicial review". *TPM - Testing, Psychometrics, Methodology in Applied Psychology*, v. 32, n. S2, 2025, pp. 34-46. Available at: <https://tpmap.org/submission/index.php/tpm/article/view/150> (accessed on 15 April 2026).
- LE NGUYEN THANH. "Electronic evidence collection in Vietnamese criminal proceedings". *Vietnamese Journal of Legal Science*, vol. 3, no. 175, 2024, pp. 51-62. Available at: <https://doi.org/10.70236/tckhplvn.70> (accessed on 20 April 2026).
- MALAYSIAN COURT OF APPEAL. Gnanasegaran a/l Pararajasingam v Public Prosecutor [1997] 3 MLJ 1; [1997] 4 CLJ 6 (Court of Appeal, Malaysia).
- MALAYSIAN FEDERAL COURT. Ahmad Najib bin Aris v Public Prosecutor [2009] 2 MLJ 613. Available at: <https://supremetoday.ai/doc/judgement/MYS00000056376> (accessed on 01 March 2026).
- Narasimhan, p. And kala, n. "Ensuring the integrity of digital evidence: The role of the chain of custody in digital forensics". *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, v. 10, n. 6, 2024, pp. 2438-2450. Available at: <https://doi.org/10.32628/CSEIT2410612443> (accessed on 25 April 2026).
- NGÔ XUÂN KHANG. "Identifying legal bottlenecks on electronic data and recommendations for improvement". *People's Court Journal*, 2023. Available at: <https://tapchitoaan.vn/nhan-dien-cac-diem-nghen-phap-ly-ve-du-lieu-dien-tu-va-kien-nghi-hoan-thien15042.html> (accessed on 05 March 2026).
- NGUYỄN ĐỨC HẠNH. "Electronic data and electronic evidence". *Journal of Procuratorial Science, Special Issue 1, 2019*, pp. 37-42. Available at: <https://vjol.info.vn/tks/article/view/46336/37588> (accessed on 05 March 2026).
- NGUYỄN ĐỨC HẠNH. "Provisions on electronic evidence in procedural law and the Law on Electronic Transactions". *People's Court Journal*. 2021. Available at: <https://tapchitoaan.vn/quy-dinh-ve-chung-cu-dien-tu-trong-phap-luat-to-tung-va-luat-giao-dich-dien-tu8114.html> (accessed on 05 March 2026).
- NGUYỄN PHI HÙNG. "Collection of electronic evidence in criminal procedure: Some shortcomings and recommendations for improvement". *Journal of Democracy and Law*, 2021. Available at: <https://danchuphapluat.vn/thu-thap-chung-cu-dien-tu-trong-to-tung-hinh-su-mot-so-bat-cap-va-kien-nghi-hoan-thien-8648-8648.html> (accessed on 25 April 2026).
- NGUYEN THANH MINH CHANH. "Authentication of electronic evidence derived from digital transactions and communications". *Futurity Proceedings, n. 5, 2025*, pp. 302-309 (*International Conference on Economic Sciences and Management in the Changing World*). Available at: <https://doi.org/10.5281/zenodo.17926441> (accessed on 20 March 2026).
- NGUYỄN VĂN ĐIỀN. "Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015" [Electronic evidence in the 2015 Criminal Procedure Code]. Ministry of Justice, 17 June 2019. Available at: <https://moj.gov.vn/qt/tintuc/Pages/nghien-cuu-trao-doi.aspx?ItemID=2455> (accessed on 25 March 2026).
- OFFICIAL JOURNAL OF THE EUROPEAN UNION. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings (OJ L 191, 28.7.2023). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1543> (accessed on 25 March 2026).
- PARLIAMENT OF MALAYSIA. Evidence Act 1950 (Malaysia, Act 56) inserted by the Evidence (Amendment) (No. 2) Act 1993, Kuala Lumpur, 1993, ss. 90A, 90B and 90C. Available at: https://ccid.rmp.gov.my/Laws/Act_56_-_Evidence_Act_1950.pdf (accessed on 20 March 2026).
- PARLIAMENT OF SINGAPORE. Evidence Act 1893 (Singapore, 2020 Rev Ed), inserted by the Evidence (Amendment) Act 2012, Singapore, 2020, s 116A. Available at: <https://sso.agc.gov.sg/Act/EA1893> (accessed on 10 March 2026).
- PHẠM CÔNG TÙNG, "Improving the provisions on electronic data in criminal procedure", Protection of Law newspaper (Kiểm sát), 2022. Available at: <https://kiemsat.vn/hoan>

- thien-quy-dinh-ve-du-lieu-dien-tu-trong-to-tung-hinh-su-64101.html (accessed on 05 March 2026).
- PHẠM MINH ĐỒ, "Improving criminal law on high-tech crimes in the context of digital transformation in Vietnam". *Legal Affairs Journal*, 2023. Available at: <https://phaply.net.vn/hoan-thien-phap-luat-hinh-su-ve-toi-pham-cong-nghe-cao-trong-boi-can-chuyen-doi-so-tai-viet-nam-a260189.html> (accessed on 20 March 2026).
- SINGAPORE HIGH COURT. *Telemedia Pacific Group Ltd v Credit Agricole (Suisse) SA (Yeh Mao-Yuan, third party)* [2015] 1 SLR 338; [2014] SGHC 235, at [248] and [250]. Available at: https://www.elitigation.sg/gd/s/2014_SGHC_235 (accessed on 10 March 2026).
- THE GOVERNMENT OF VIETNAM. Decree No. 127/2017/ND-CP of 16 November 2017 of the Government detailing the sealing and unsealing of exhibits, Hanoi, 2017. Available at: <https://vanban.chinhphu.vn/default.aspx?pageid=27160&docid=192054> (accessed on 20 April 2026).
- THE GOVERNMENT OF VIETNAM. Decree No. 356/2025/ND-CP of 31 December 2025 detailing certain articles of and measures implementing the Law on Personal Data Protection, Hanoi, 2025, (Article 42(1)). Available at: <https://vanban.chinhphu.vn/?pageid=27160&docid=216387> (accessed on 05 Jun 2026).
- TRẦN NGỌC MINH & ĐẶNG MINH CƯỜNG. "Improving the law on investigative measures under the criminal procedure code 2015". *Protection of Law newspaper (Kiểm sát)*, 2023. Available at: <https://kiemsat.vn/hoan-thien-phap-luat-ve-cac-bien-phap-dieu-tra-theo-quy-dinh-cua-bo-luat-to-tung-hinh-su-nam-2015-65859.html> (accessed on 05 March 2026).
- TRƯỜNG THÀNH THẢO NGUYỄN. "Digital evidence in criminal procedure: Legal challenges and solutions in Vietnam". *Journal of Science and Technology (Binh Duong University)*, vol. 8, no. 1, 2025. Available at: <https://jst.bdu.edu.vn/index.php/jst/article/view/297> (accessed on 05 March 2026).
- UK PARLIAMENT. Police and Criminal Evidence Act 1984 (PACE), London, 1984, Code B. Available at: <https://www.gov.uk/government/publications/pace-code-b-2023> (accessed on 05 March 2026).
- UNITED NATIONS. United Nations Convention against Cybercrime, Hanoi, 2025. Available at: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html> (accessed on 20 March 2026).
- UNITED STATES CONGRESS. Federal Rules of Evidence, Washington DC, 1975 (Pub. L. 93-595, as amended), Rules 901-902. Available at: https://www.law.cornell.edu/rules/fre/rule_901 and https://www.law.cornell.edu/rules/fre/rule_902 (accessed on 05 March 2026).
- Vietnam's Ministry of Public Security – Vietnam's Ministry of National Defence – Vietnam's Ministry of Justice – Vietnam's Ministry of Information and Communications – Vietnam's Supreme People's Procuracy – Vietnam's Supreme People's Court. Joint Circular No. 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC guiding the application of the provisions of the Penal Code on certain offences in the field of information technology and telecommunications, Hanoi, 2012. Available at: <https://congbao.chinhphu.vn/vanban/thong-tu-lien-tich-so-10-2012-tslt-bca-bqp-btp-btttt-vksndtc-tandtc-16819.htm> (accessed on 20 April 2026).
- VIETNAMESE NATIONAL ASSEMBLY. Criminal Procedure Code 2015 (as amended by Law No. 99/2025/QH15), Hanoi, 2015. Available at: <https://www.wipo.int/wipolex/en/text/585372> (accessed on 20 April 2026).
- VIETNAMESE NATIONAL ASSEMBLY. Law on Electronic Transactions 2005, Hanoi, 2005, Art. 4(5). Available at: https://www.wto.org/english/thewto_e/acc_e/vnm_e/wtaccvnm43_leg_5.pdf (accessed on 20 March 2026).
- VIETNAMESE NATIONAL ASSEMBLY. Law on Electronic Transactions 2023 (Law No. 20/2023/QH15), Hanoi, 2023. Available at: <https://thuvienphapluat.vn/vanban/EN/Thuong-mai/Law-20-2023-QH15-Electronic-Transactions/577937/tieng-anh.aspx> (accessed on 02 Jun 2026).
- VIETNAMESE NATIONAL ASSEMBLY. Law on Personal Data Protection 2025, Hanoi, 2025. Available at: <https://english.luatvietnam.vn/dan-su/law-on-personal-data-protection-law-no-91-2025-qb15-405135-d1.html> (accessed on 05 Jun 2026).

- VIETNAMESE NATIONAL ASSEMBLY. Law on Treaties 2016, Hanoi, 2016, art. 6(1). Available at: <https://vanban.chinhphu.vn/?pageid=27160&docid=184571> (accessed on 20 April 2026).
- VIETNAMESE NATIONAL ASSEMBLY. The 2013 Constitution of the Socialist Republic of Vietnam, Hanoi, 2013, Art. 14(2) and 21. Available at: <https://www.wipo.int/wipolex/en/legislation/details/21482> (accessed on 20 April 2026).
- VNS. *Vietnam strives to facilitate digital transformation*. Vietnam News, 2023. Available at: <https://vietnamnews.vn/economy/1549806/viet-nam-strives-to-facilitate-digital-transformation.html> (accessed on 15 March 2026).