Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

Research Article

THE LEGAL FRAMEWORK OF ELECTRONIC EVIDENCE IN VIETNAMESE CRIMINAL PROCEDURE: FROM THE BUDAPEST CONVENTION TO DOMESTIC LEGISLATION

Dinh The Hung

DOI:
https://doi.org/10.33327/AJEE-18-8.4-a000142

Date of submission: 10 Aug 2025
Date of acceptance: 08 Oct 2025
Publication: 18 Nov 2025

Disclaimer:
The author declares that the opinion and views expressed in this manuscript are free of any impact of any organizations.

ABSTRACT

Background: *Electronic evidence constitutes a critical and sensitive subject addressed in international instruments on crime prevention, most notably the Budapest Convention on Cybercrime, and the Treaty on Cybercrime – UN (the Hanoi Convention), which was newly signed in Hanoi, Vietnam, in October 2025. The legal treatment of electronic evidence has emerged as one of the most vigorously debated topics within academic circles, particularly in discussions concerning the domestic incorporation of international treaty obligations.*

Vietnam's Criminal Procedure Code of 2015 represents a significant development by formally recognising electronic data as a legitimate form of evidence, equivalent in probative value to other traditional sources. As electronic evidence is becoming increasingly prevalent across a wide spectrum of criminal offences, this recognition is timely. However, with the rise of cybercrime, Vietnam's current legal framework falls short of European standards, particularly in terms of conceptual clarity,

procedural safeguards for the collection and evaluation of electronic evidence, protection of human rights, and adherence to adversarial principles.

Accordingly, this article aims to clarify the theoretical and legal framework for electronic evidence under European standards, compare it with Vietnam's approach, and identify the theoretical and legal gaps that must be addressed—such as the need for clearer definitions, stronger procedural guarantees in evidence collection and assessment, human rights protections, and the reinforcement of adversarial principles.

Methods: *To conduct a comparative analysis of electronic evidence within Vietnam's criminal procedure law and international legal frameworks, the study draws on methodologies rooted in comparative legal studies. The analysis focuses on the comparative examination of international and domestic legal provisions concerning electronic evidence. Accordingly, the author makes extensive use of comparative legal methods, including normative comparison and functional comparison, to identify both similarities and differences between Vietnam's regulations on sources of evidence in criminal procedure and those found in international instruments and the legal systems of other jurisdictions.*

Results and conclusions*: The article concludes that Vietnam's legal provisions and practical implementation regarding electronic evidence must draw upon international experience in several key respects: the accurate conceptualisation of electronic evidence, the development of standardised procedures for its collection, and the refinement of legal mechanisms governing the duty to produce evidence, forensic examination, and the application of special investigative measures. Such reforms are essential to ensure the authenticity and legality of electronic evidence while safeguarding human rights within the criminal justice process.*

1 INTRODUCTION

Statistical data, academic literature, and practical experience in combating cybercrime worldwide have demonstrated that cybercrime is a transnational issue of global concern. Policymakers widely agree that cybercrime constitutes a core priority requiring immediate action at the EU level, ranging from public-private cooperation to the exchange of best practices among stakeholders.[1]

1 See amongst others: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security (COM (2015) 185 final, 28 April 2015) 13, 19-20 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0185> accessed 10 August 2025; Commission Services, 'Improving Cross-Border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way Forward' (*European Commission*, 22 May 2017) <https://home-affairs.ec.europa.eu/system/files/2017-05/20170522_non-paper_electronic_evidence_en.pdf> accessed 10 August 2025.

Unlike traditional crimes, which typically leave physical traces in the material world, cybercrimes occur not only in the physical realm but also within cyberspace. Naturally, the traces left behind in this environment are called digital traces.[2] In other words, although communication in cyberspace is mediated through electronic devices, it remains a form of interaction that inevitably generates traces, thus giving rise to electronic evidence.[3]

Due to the unique modus operandi of cybercriminals and the inherent characteristics of the digital environment, the traces they leave differ significantly from conventional forms of evidence and are now recognised as electronic evidence. Electronic evidence has already begun to reshape and will continue to transform the criminal procedure frameworks of national jurisdictions. While procedural systems may vary across countries, they must nonetheless adhere to universal standards governing evidence, particularly the principles of integrity, authenticity and legality in the treatment of electronic evidence.

Vietnam's Criminal Procedure Law is currently under pressure to reform to keep pace with the rapid advancement of science and technology and the evolving nature of cybercrime. Since 2015, Vietnam has undertaken procedural reforms to adapt to technological developments, notably by establishing a general legal framework to regulate criminal investigations in the digital era. This includes the formal recognition of electronic data as a legitimate source of evidence, the introduction of basic procedures for the collection and processing of electronic evidence, and the authorisation of various digital investigative techniques under existing legal mandates (e.g., computer searches, data access, electronic surveillance). However, in practice, these procedures remain largely indistinguishable from those applied to traditional forms of evidence. Compounding this issue is the limited technical expertise among law enforcement personnel and the lack of specialised training in digital forensics. These deficiencies have led to scepticism regarding the authenticity and legality of electronic evidence, as well as concerns over the protection of human rights in criminal proceedings.

This situation underscores Vietnam's pressing need to assimilate the successes and advancements of international legal frameworks, particularly the standards in the European Treaty Series (ETS) and the legal systems of countries within its sphere of influence, to enhance its domestic legislation. The Budapest Convention,[4] for instance, is widely regarded as having transcended its European origins, with several signatory and ratifying states outside the Council of Europe, including the United States, Japan, and

2 Bart Custers and Lonneke Stevens, 'The Use of Data as Evidence in Dutch Criminal Courts' (2021) 29(1) European Journal of Crime, Criminal Law and Criminal Justice 25. doi:10.1163/15718174-bja10015.

3 Ken Zatyko and John Bay, 'The Digital Forensics Cyber Exchange Principle' (*Villanova University, College of Liberal Arts and Sciences*, 22 April 2013) <http://www.csc.villanova.edu/~dprice/9010sp14/extra_handouts/The_Digital_Forensics_Cyber_Exchange_Principle_-_2013-04-22.pdf> accessed 10 August 2025.

4 Convention on Cybercrime (Budapest Convention) (23 November 2001) ETS 185.

Australia.[5] Although Vietnam is not yet a member of the Convention, it has engaged in cooperative efforts with countries operating under its influence in the transnational fight against cybercrime, particularly in the field of electronic evidence investigation. Furthermore, research indicates that Europe ranks highest in the adequacy of national laws governing cybercrime investigations: approximately 70% of surveyed European countries reported that their investigative powers are sufficient, 25% deemed them partially sufficient, and 5% considered them insufficient.[6]

Compared to European standards, Vietnam's legal framework still contains several gaps that need to be addressed, including: (i) the conceptualisation of electronic evidence and electronic data; (ii) the procedural gaps in the digital investigation workflow; (iii) obligations and mechanisms for cooperation with service provider; (iv) standards for assessing admissibility and technological reliability; (v) protection of human rights and judicial oversight; and (vi) digital forensic capacity and the integrity of the chain of custody. To address these issues, this article will examine the theoretical framework for electronic evidence, compare European standards with Vietnamese law, and identify areas where legal and conceptual development is needed.

A comparative study of electronic evidence in Vietnam may offer valuable insights for other legal jurisdictions and contribute practical experience to countries in the process of integrating international and foreign legal standards on this issue. This research is particularly relevant given the forthcoming signing of an international convention on cybercrime in Hanoi, as well as the growing imperative for international cooperation to combat cybercrime.

2 METHODOLOGY AND RESEARCH METHODS

The study adopts a comparative law approach to examine and address the issue of electronic evidence within the context of Vietnamese law and European legal systems. For a meaningful comparison, it is essential to establish a common analytical basis; without such a foundation, identifying similarities and differences or formulating recommendations for legal harmonisation and adoption would be impossible. Comparative analysis also requires a thorough understanding of the legal systems under examination—namely, the Budapest

5 Deliverable 3.2 of the E-CRIME project (Grant Agreement Number 607775): E-CRIME Deliverable 3.2 final report on countermeasure including policy and enforcement responses, March 2015 for more information on cybercrimes and the Cybercrime Convention. See: 'Economic Impacts of Cybercrime (E-CRIME, Grant agreement ID 607775)' (*European Commission*, 27 May 2024) <https://cordis.europa.eu/project/id/607775/reporting> accessed 10 August 2025.

6 Jeanne Pia Mifsud Bonnici, Melania Tudorica and Joseph A Cannataci, 'The European Legal Framework on Electronic Evidence' in Maria Angela Biasiotti and others, *Handling and Exchanging Electronic Evidence Across Europe* (Springer 2018) 189. doi:10.1007/978-3-319-74872-6_11.

Convention and the legal frameworks of selected European countries—while the comparative system is represented by Vietnam's legal regime.

The objective of this comparison is to identify similarities and differences between Vietnam's national law and those of other jurisdictions worldwide. The comparative content focuses on core issues related to electronic evidence, including procedures for its collection and preservation, as well as the protection of human rights in criminal proceedings.

To assess the compatibility between European legal systems and Vietnamese law regarding electronic evidence, the analysis begins by identifying key similarities between the two frameworks. Establishing such similarities is a prerequisite for assessing the extent to which Vietnam's criminal procedure law can assimilate European legal standards. The similarities highlighted include the underlying models of criminal procedure and the theory of evidence, both of which exert significant influence on the regulation of electronic evidence in each system. Vietnam shares notable parallels with European law in both foundational aspects.

This study also employs the theory of legal transplantation to identify international best practices that Vietnam should consider adopting. Legal transplantation refers to the horizontal transfer of laws and legal institutions from one country to another, or the vertical transfer from international organisations to national jurisdictions. Such transplantation may occur through imposition or voluntary adoption and may encompass an entire legal system, specific statutes, selected legal principles, or doctrinal frameworks.[7] Scholars have examined the foundations, influencing factors, modalities, and processes involved in legal transplantation. Vietnam currently possesses the necessary political and legal foundations to incorporate international norms on electronic evidence into its domestic legal system. Moreover, the country has acceded to international conventions on transnational and cybercrime. However, once a state becomes a signatory and ratifies such conventions, the legislative obligations arising therefrom must be implemented in ways that reflect the specific conditions and characteristics of each jurisdiction.[8]

The study employs the method of legal analysis, focusing on studies related to electronic evidence and the relevant provisions of international law, national laws of selected European countries, and Vietnam's Criminal Procedure Law. The comparative method is applied to identify similarities and differences between these two legal systems. The comparative framework centers on the current international legal regime, with particular reference to the ETS; the Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and the disclosure of electronic evidence of the European Council;[9]

7 John Gillespie, 'Towards a Discursive Analysis of Legal Transfers into Developing East Asia' (2008) 40(3) NYU Journal of International Law and Politics 657.

8 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (A/Res/39/46, 10 December 1984) [1996] UNTS 1465/85, art 11.

9 Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (12 May 2022) CETS 224.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (repealing Council Framework Decision 2008/977/JHA),[10] and Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.[11]

The analysis also considers the legal frameworks of several European and Eastern European countries, including the Netherlands, Poland, Ukraine, and Germany. Vietnam's current legal framework is examined through the Criminal Procedure Code of 2015[12] and the Law on Electronic Data.[13]

This study proceeds on the assumption that the legal framework for electronic evidence established by the European Convention on Cybercrime has significantly advanced beyond that of Vietnam. In contrast, Vietnam's current legal provisions on this matter still exhibit notable gaps in meeting those international standards. Consequently, Vietnam's legal system stands to benefit from the experiences and best practices of European jurisdictions in developing a more robust and coherent legal framework for electronic evidence.

3 THEORETICAL FRAMEWORK ON ELECTRONIC EVIDENCE

To compare European and Vietnamese standards on electronic evidence in criminal procedure, a theoretical framework on electronic evidence is required as a point of reference. Such a framework should cover its core elements, namely: terminology and definitions; the characteristic features of electronic evidence; the fundamental principles governing electronic evidence; the processes for collection; and the criteria for the assessment and admissibility of electronic evidence. The following sections examine these issues in greater detail.

10 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

11 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 Regarding the European Investigation Order in Criminal Matters [2014] OJ L 130/1.

12 Law of Vietnam No 101/2015/QH13 'Criminal Procedure Code' (27 November 2015) <https://vanban.chinhphu.vn/default.aspx?pageid=27160&docid=183217> accessed 10 August 2025. [in Vietnamese]

13 Law of Vietnam No 60/2024/QH15 'On Data' (30 November 2024) <https://chinhphu.vn/?pageid=27160&docid=212488&classid=1&typegroupid=3> accessed 10 August 2025. [in Vietnamese]

3.1. Concept of Electronic Evidence

The emergence of electronic evidence poses one of the greatest challenges to the traditional doctrine of evidence. Unlike physical evidence, which is tangible, electronic evidence consists of information that is generated, transmitted, or stored by electronic means. Accordingly, the first issue that needs to be addressed concerns the terminology and concept of electronic evidence. The definition of electronic evidence depends on both the general theory of evidence and its specific characteristics. The following section examines these two aspects and, on that basis, proposes a definition of electronic evidence.

Currently, two distinct approaches to terminology are in use: *electronic evidence* và *digital evidence*. One prevailing viewpoint asserts that the term electronic evidence "better reflects the cybernetic aspect of information transmission, processing and preservation in view of the processes of information transformation using a binary code," and that "devices and machines processing and saving digital information should be called electronic.[14]

From a theoretical perspective, the concept of digital evidence remains a subject of vigorous debate in both European countries and Vietnam. Such debate is entirely justified, as the term "digital evidence" appears frequently in legal texts, yet its precise meaning requires further theoretical clarification. Electronic evidence and evidence collected via information and communication technology also introduce new work practices and tools, necessitating a coherent and supportive normative framework. When seeking to achieve such a framework, it is first necessary to determine what should be considered electronic evidence.[15] To date, there is no evidence to suggest that the absence of a unified definition of electronic evidence has hindered cooperation among Member States in the collection, preservation, and use of such evidence. However, a standardised definition could facilitate the exchange of electronic evidence, an indispensable component of international cooperation, and is regarded as a useful starting point for engaging with electronic evidence frameworks.[16] A shared understanding of the concept of electronic evidence, therefore, constitutes a foundational element, alongside other components such as procedures for collection, preservation, and evaluation, within a common legal framework governing electronic evidence.

14 N Zozulia, 'Electronic or Digital Evidence: Improving Amendments in Procedural Legislation' (*Ukrainian Law*, 8 May 2018) <https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva> accessed 10 August 2025. [in Ukrainian]; Galina Avdeeva and Elzbieta Żywucka-Kozlowska, 'Problems of Using Digital Evidence in Criminal Justice of Ukraine and the USA' (2923) 1(30) Theory and Practice of Forensic Science and Criminalistics 131. doi:10.32353/khrife.1.2023.07 [in Ukrainian].

15 Elena Alina Onțanu, Normalising the Use of Electronic Evidence: Bringing Technology Use into a familiar Normative Path in Civil Procedure' (2022) 12(3) Oñati Socio-Legal Series 582. doi:10.35295/osls.Iisl/0000-0000-0000-1304.

16 Mifsud Bonnici, Tudorica and Cannataci (n 6).

To date, no universally accepted definition of electronic evidence exists,[17] and a clear distinction remains between theoretical perspectives and codified law on the subject. This research indicates that, in theory, there are two main conceptual approaches. The first approach equates electronic evidence with the data itself—such as subscriber data, traffic data, or content data—stored within electronic systems. The second approach views electronic evidence as the information contained in electronic data, while the data itself serves merely as a repository. This perspective reflects a fundamental principle: data becomes evidence only when it meets the legal thresholds of relevance, authenticity, and admissibility.

The first equates electronic evidence with the medium that carries it, namely, electronic or computer data. Specifically, electronic evidence is understood to include subscriber data, traffic data, or content stored electronically by service providers,[18] as well as any digital data through which a crime may be proven or the relationship between the offender, the offence, and the victim may be established. Digital data is defined as a collection of numerical representations derived from various documents, encompassing text, graphics, maps, audio, and drawings.[19] This view is also reflected in the following definitions: "Electronic evidence is factual data presented in digital (discrete) form, recorded on any type of medium, and accessible to humans after being processed by a computer"[20] or "electronic evidence is any data resulting from the output of an analogue device and/or a digital device of potential value that are generated, processed, stored, or transmitted using any electronic device."[21] Another perspective defines electronic evidence as *any evidence with potential probative value that is manipulated, generated, stored, or transmitted by any electronic device.*[22]

The second school of thought draws a clear distinction between electronic evidence as "information" and the medium that contains it: electronic data. This perspective holds that electronic Evidence is any information generated, stored or transmitted using electronic devices that may be relied upon in court.[23] Meanwhile, legal and forensic communities in

17 Sergi Vazquez Maymir, 'Anchoring the Need to Revise Cross-Border Access to eEvidence' (2019) 9(3) Internet Policy Review 1. doi:10.14763/2020.3.1495

18 Adam Juszczak and Elisa Sason, 'The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence' (2023) 2 Eucrim 182.

19 Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn, Academic Press 2011).

20 Dmytro M Tsekhan, 'Digital Evidence: Concept, Features and Place in the Evidence System' (2013) 5 Scientific Bulletin of the International Humanities University, Series: Jurisprudence 256. [in Ukrainian]

21 Maria Angela Biasiotti and others, 'Opportunities and Challenges for Electronic Evidence' in Maria Angela Biasiotti and others (eds), *Handling and Exchanging Electronic Evidence Across Europe* (Springer 2018) 3. doi:10.1007/978-3-319-74872-6_1.

22 Mifsud Bonnici, Tudorica and Cannataci (n 6).

23 EVIDENCE, *Project "European Informatics Data Exchange Framework for Courts and Evidence": D2.1 - EVIDENCE Semantic Structure (Grant Agreement No 608185)* (EU 2015) 18 <https://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d2-1-410.pdf> accessed 10 August 2025.

Poland tend to align with international theoretical understandings of "digital evidence", which is defined as any information with evidentiary value derived from electronically processed binary data (data in digital form).[24] In Ukraine, the Draft Law "Amendments to the Criminal Procedure Code of Ukraine" (Registration No. 4004 dated September 1, 2020)[25] proposes a definition of electronic evidence as information in electronic (digital) form that contains data capable of serving as proof of facts or circumstances established during criminal proceedings.[26]

Europe has an alternative approach to electronic evidence. This approach includes both digitised physical or traditional evidence, such as a digital photograph of a murder weapon and evidence that is originally created in digital form by any digital device (a computer or computer-like equipment). All such forms of evidence are classified as "electronic evidence" because, upon completion of the evidentiary process, they can be labelled as electronic regardless of their original source.[27]

As regards positive law, this research indicates that there is no formal definition of electronic evidence in the statutory laws of European countries, with the exception of Croatia. The Budapest Convention does not provide a definition of electronic evidence; instead, it refers to the concept of electronic data and outlines procedures for the collection, preservation, and processing of such evidence. The only existing definition of electronic evidence within the European legal framework appears in the recently updated guidelines of the Council of Europe. There, digital (or electronic) evidence is defined as: "any information created, stored, or transmitted in digital form that may subsequently be required to prove or disprove a disputed fact in legal proceedings."[28]

Thus, while some countries have adapted their legal frameworks to accommodate electronic evidence, others continue to rely on traditional criminal law provisions and apply them to digital contexts.[29] Evidentiary rules vary significantly, even among countries that share similar legal traditions.[30]

24 Piotr Lewulis, 'Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law' (2022) 33(1) Criminal Law Forum 39. doi:10.1007/s10609-021-09430-4.

25 Draft Law of Ukraine No 4004 'On Amendments to the Criminal Procedure Code of Ukraine to Increase the Efficiency of Combating Cybercrime and the Use of Electronic Evidence' (1 September 2020) <https://itd.rada.gov.ua/billinfo/Bills/Card/3765> accessed 10 August 2025. [in Ukrainian]

26 Roman Blahuta, Anatolii Movchan and Maksym Movchan, 'Use of Electronic Evidence in Criminal Proceedings in Ukraine' (International Conference on Social Science, Psychology and Legal Regulation (SPL 2021), Kyiv, Ukraine, 22-24 December 2021) 196. doi:10.2991/assehr.k.211218.032.

27 Mifsud Bonnici, Tudorica and Cannataci (n 6).

28 Nigel Jones and others, *Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges* (version 2.1, Council of Europe 2020) 12 <https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4> accessed 10 August 2025.

29 Mifsud Bonnici, Tudorica and Cannataci (n 6).

30 UNODC, *Comprehensive Study on Cybercrime: Draft* (UN 2013) 158 <https://www.unodc.org/e4j/data/_university_uni_/draft_comprehensive_study_on_cybercrime.html?lng=en> accessed 10 August 2025.

In Vietnam, there is currently no statutory definition of electronic evidence; however, theoretical discourse reveals two prevailing schools of thought, similar to those found in European jurisdictions. The first school equates electronic evidence with electronic data, treating them as one, while the other believes that all evidence is fundamentally similar in nature, differing only in its source, namely, digital data. One perspective asserts that: "Electronic data may be considered evidence or referred to as electronic evidence if it is collected in accordance with the procedures and formalities prescribed by law."[31] A more widely accepted view defines electronic evidence as: "Information stored in the form of electronic signals within computers or digital memory devices that is relevant to a criminal case."[32]

The legal framework governing electronic evidence in Vietnam is embedded within the general framework of evidentiary law, which is itself grounded in the evidentiary theory previously outlined. Thus, the Vietnamese Criminal Procedure Code does not explicitly recognise electronic evidence as a distinct category. This omission stems from Vietnam's legal tradition, rooted in socialist jurisprudence, which clearly distinguishes between evidence and its sources. Under this theory, objective, factual events that constitute a criminal offence must be recorded and reflected in evidence sources as defined by criminal procedural law.[33] According to the Vietnamese Criminal Procedure Code, evidence is defined as factual information relevant to a criminal case that is collected lawfully.[34] A source of evidence is defined as "a place or medium from which the authorities or officials may obtain evidence in a criminal case."[35] It is essential not to conflate evidence with its source, as not all information contained within a source qualifies as evidence unless it meets the criteria of truthfulness, relevance, and lawful collection. Each source of evidence reflects the lifecycle of evidentiary material, from its formation, existence, and potential disappearance. Based on this understanding, the law prescribes specific characteristics for each type of evidentiary source, along with distinct procedures for collecting and evaluating evidence derived from them. Thus, evidence is understood as "information", while the source of evidence refers to the medium that contains such information.

Vietnam's Criminal Procedure Code identifies seven categories of evidentiary sources, with the recent addition of a significant new source: electronic data. Electronic data constitutes the source of evidence, whereas the information contained within that data is considered the evidence itself. This aligns with the view that "data is merely the input,

31 Le Tan Quan, 'Difficulties in Determining the Properties of Electronic Evidence' (2024) 15 Tạp chí Kiểm sát 10. [in Vietnamese]

32 Tran Văn Hòa, 'The Issue of Electronic Traces and Evidence in the Amended Criminal Procedure Code' (2014) 12 Tạp chí Khoa học và Chiến lược. [in Vietnamese]

33 Nguyen Ngoc Chi and Le Lan Chi (eds), *Criminal Procedure Law Textbook* (Hanoi National University Press 2018) 222. [in Vietnamese]

34 Law of Vietnam No 101/2015/QH13 (n 12) art 86.

35 Tran Quang Tiep, *Evidence Regulation in Vietnamese Criminal Procedure Law* (National Political Publishing House 2011) 47. [in Vietnamese]

while 'evidence' is the outcome of a verified reasoning process",[36] and that "data only becomes evidence when placed within a legal context and meets thresholds of relevance, authenticity, and reliability."[37]

In both scholarship and policy, various definitions of electronic evidence have been proposed. Nevertheless, regardless of how it is conceptualised, electronic evidence invariably possesses the following distinctive features:

First, unlike physical evidence—where alterations to its structure are difficult to conceal and typically leave traces—electronic evidence can be easily copied, disseminated, modified, updated, or deleted (with deletion in an electronic environment not necessarily meaning permanent erasure, as data may still be recoverable)[38]. This characteristic not only increases the risk of loss but also poses a major challenge to ensuring integrity and authenticity. Research has demonstrated that electronic data can be altered without leaving clear traces; therefore, the application of digital forensic mechanisms is indispensable in modern criminal proceedings.[39]

Second, electronic evidence is inherently technology-dependent. It cannot exist independently; rather, it is generated through electronic devices and application software. Electronic data requires interpretation in order to be displayed in a readable format. Users cannot create or manipulate electronic data without the appropriate hardware and software.[40] Consequently, the collection, preservation, and presentation of this type of evidence demand the support of technical tools, digital forensic experts, as well as adherence to international standards.

*Third***,** electronic evidence may possess a cross-border character in terms of storage and retrieval: network data, logs, and backups are often distributed across multiple systems and jurisdictions, giving rise to challenges regarding access rights, international cooperation, and the protection of personal data during investigation.[41]

36 Alex Biedermann and Kyriakos N Kotsoglou, 'Digital Evidence Exceptionalism? A Review and Discussion of Conceptual Hurdles in Digital Evidence Transformation' (2020) 2 Forensic Science International: Synergy 262. doi:10.1016/j.fsisyn.2020.08.004.

37 Michal Gebicki, 'Cross-border Acquisition of Digital Data in Criminal Proceedings: State of Play and Measures Taken by the European Union and the Council of Europe' (2024) 1(29) Teisės apžvalga 3. doi:10.7220/2029-4239.29.1.

38 Stephen Mason and Daniel Seng (eds), *Electronic Evidence* (University of London Press 2017). doi:10.14296/517.9781911507079.

39 Brian D Carrier and Eugene H Spafford, 'An Event-Based Digital Forensic Investigation Framework' (DFRWS 2004 Digital Forensic Research Conference, USA, Baltimore, MD, 11-13 August 2004).

40 Bich Thao Nguyen, 'Improving Vietnam's Electronic Evidence Law in the Industry 4.0 Era: Experience from China' (2024) 16(1) Revista de Direito 1. doi:10.32361/2024160117322.

41 Wei Wang and Thomas E Daniels, 'Building Evidence Graphs for Network Forensics Analysis' (21st Annual Computer Security Applications Conference ACSAC 2005). doi:10.1109/CSAC.2005.14.

Finally, although electronic evidence has significant probative value, it is highly susceptible to dispute if the chain of custody or the collection process is not clearly documented and verifiable. Courts require proof of origin and integrity before admitting electronic data as evidence.[42]

The next part of the discussion concerns the concept of electronic data in European and Vietnamese law. Clarifying this concept is essential for determining the scope of data that may contain evidence and, therefore, needs to be seized. The Budapest Convention does not use the term electronic data but instead refers to computer data. According to the Convention, computer data is any representation of facts, information, or concepts in a form suitable for processing by a computer system.[43] This definition is based on the ISO data standard, and the notion of "suitable for processing" is defined as follows: data is put in a form that can be processed directly by the computer system. To make clear that the data in this Convention must be understood as data in electronic or other directly processable form, the notion "computer data" is introduced.[44] Within the scope of computer data, the Convention categorises data into three main groups: (i) Stored data, (ii) Traffic data, and (iii) Content data.

In the criminal procedure laws of European countries today, the concept of electronic data is widely used. Vietnamese criminal procedure law also adopts the term electronic data, which is defined as symbols, text, numbers, images, sounds, or similar forms that are created, stored, transmitted, or received via electronic means.[45] Unlike traditional forms of evidence, the value of electronic evidence is assessed not only based on conventional criteria such as objectivity, relevance, and legality, but also on additional factors. These include the methods used to ensure and maintain the integrity of the electronic message, the identification of the message's originator, and other relevant contextual elements.[46]

However, this study aligns with the view that, in addition to computer data as defined at the time of the Convention's adoption, new categories of data have since emerged—namely, electronic data and digital data. Electronic data means data recorded by an electronic device. From the category of electronic data, two further categories may be distinguished: data recorded in digital form (digital data) or in analogue form (analogue data). The criterion distinguishing them is not the type of device with which they are recorded or reproduced, but the nature of the signal carrying the information.[47] Recently, the Council of Europe and

42 Orin S Kerr, 'Searches and Seizures in a Digital World' (2005) 119(2) Harvard Law Review 531.

43 Convention on Cybercrime (n 4) art 1.

44 Council of Europe, 'Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence' (12 May 2022) CETS 224.

45 Law of Vietnam No 101/2015/QH13 (n 12) art 99.

46 Nguyen Ngoc Khanh, 'Source of Evidence is Electronic Data in Criminal Proceedings in Vietnam and Some Countries in the World' (Master's thesis, Vietnam National University 2024). [in Vietnamese]

47 Piotr Lewulis, *Dowody cyfrowe: teoria i praktyka kryminalistyczna w polskim postępowaniu karnym* (Wydawnictwo Uniwersytetu Warszawskiego 2021) 32.

the European Parliament issued a Directive on electronic evidence, which introduces a new category of data: "data requested for the sole purpose of identifying the user". This category is defined as "IP addresses and, where necessary, the relevant source ports and time stamp, namely the date and time, or technical equivalents of those identifiers and related information, where requested by law enforcement authorities or by judicial authorities for the sole purpose of identifying the user in a specific criminal investigation."[48]

3.2. Fundamental Principles Governing Electronic Evidence

Given the characteristics of electronic evidence outlined above, the field of digital forensics has identified several fundamental principles as follows:

*First, the principle of integrity***.** Unlike physical evidence, which leaves discernible traces when altered, electronic data may be modified without producing any visible signs. Therefore, without an appropriate preservation process, the probative value of electronic evidence will inevitably be called into question.[49] This principle is regarded as a prerequisite for electronic evidence to attain legal validity. It requires that information contained in digital data be considered lawful evidence only where the competent procedural authorities can demonstrate that, from the moment of collection until its presentation before the court, the content has remained intact, without alteration or loss. In other words, electronic data has probative value only if its integrity is preserved throughout the entire evidentiary process.

This principle entails full documentation of who accessed the data, when, how, and which technical steps were taken. Maintaining such transparent records enables the court and the parties concerned to verify that the data has not been tampered with outside of lawful procedures.[50] Accordingly, courts are called upon to emphasise technical standards and scientific processes to ensure the integrity of electronic evidence.

Second, the principle of authenticity requires proof that electronic data is indeed what it purports to be, originating from the claimed source, preserved, and unchanged from the moment of collection until its presentation in court.[51] In U.S. legal practice, authentication is closely tied to the chain of custody, which demonstrates that the evidence has been maintained in its original state. Authenticity is therefore inseparably linked with integrity.[52]

48 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 and for the Execution of Custodial Sentences Following Criminal Proceedings [2023] OJ L 191/118.

49 Casey (n 19).

50 Carrier and Spafford (n 39).

51 Richard Kissel (ed), *Glossary of Key Information Security Terms* (Diane Publishing 2011).

52 Sean E Goodison, Robert C Davis and Brian A Jackson, 'Digital Evidence and the US Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence' (*RAND*, 20 April 2015) <https://www.rand.org/pubs/research_reports/RR890.html> accessed 10 August 2025.

This principle entails two core requirements: (i) no action by law enforcement authorities, their personnel, or authorised agents may alter the data in any way that could undermine its reliability before the court; and (ii) where direct access to the original data is necessary, the individual concerned must possess adequate competence and be able to account for the meaning and consequences of their actions.

In practice, this principle is operationalised through a rigorous process of collecting, preserving, examining, and analysing data sources containing electronic evidence.

Third, the principle of legality. This principle requires that every operation involving electronic data—search, seizure, copying, analysis, or presentation—must have a clear legal basis, be carried out by a competent authority, and comply with the procedures and limits prescribed by law (for example, a search warrant, valid voluntary consent, or exigent circumstances). In the digital environment, this requirement is even more stringent, as operations are often conducted on a large scale (such as an entire hard drive or cloud storage) and can easily exceed the permissible scope if minimisation measures and precise descriptions of the search objects are not applied.

To ensure legality, when searching a computer or data repository, the warrant must specifically describe the target and scope (e.g., file types, time frames, or keywords) to avoid "general searches." In practice, the process typically involves creating a forensically sound image of the data and then filtering it in a laboratory setting, thereby ensuring both legality and privacy protection.

This reflects the classic analytical framework governing the search and seizure of digital data. The principle also requires that the collection of electronic evidence respect the criteria of authority, scope, and proportionality. In addition, standardised procedures for collecting electronic evidence must be observed, including codified technical standards. Where legal grounds are absent, the scope of the warrant is exceeded, or procedural requirements are breached, the evidence may be excluded or assigned diminished probative weight by the court. Such violations may also undermine the admissibility of derivative findings under the *fruit-of-the-poisonous-tree* doctrine.

In addition, electronic evidence must also comply with principles such as verifiability. The steps of collecting and analysing electronic data must be capable of replication and independent verification. Wang and Daniels proposed the "evidence graph" model, which reconstructs the logic of the collection and analysis process so that other experts may review and confirm the results.[53]

Finally, the principle of fairness and privacy. This principle emphasises that the use of electronic evidence must strike a balance between the demands of criminal prosecution and the protection of individual privacy, particularly in cross-border data contexts.[54]

53 Wang and Daniels (n 41).

54 Mark Pollitt, 'A History of Digital Forensics' (6th IFIP WG 11.9 International Conference on Digital Forensics (DF), Hong Kong, China, Jan 2010) 3. doi:10.1007/978-3-642-15506-2_1.

4 EUROPEAN AND VIETNAMESE LEGAL FRAMEWORKS FOR ELECTRONIC EVIDENCE

European law approaches electronic evidence through the standardisation of procedural tools, the protection of human rights, and the strengthening of international cooperation. The cornerstone of this approach is the Budapest Convention on Cybercrime (2001), complemented by the legal framework of the European Union (EU) and the case law of the European Court of Human Rights (ECtHR). Thus, the European model establishes a dual standard: it seeks to enhance the effectiveness of investigating high-tech crime through modern procedural instruments, while at the same time emphasising the protection of human rights and adversarial guarantees. These aspects are elaborated on below.

4.1. The European Regulatory Framework on Electronic Evidence

European legislation contains no statutory definition of electronic evidence, with the sole exception of Croatia. The Budapest Convention likewise does not define electronic evidence; rather, it refers to electronic data and regulates procedures for its collection, preservation, and handling. The only explicit definition of electronic evidence appears in the recently updated guidelines of the Council of Europe, where digital (or electronic, as it is sometimes called) evidence is defined as "any information that is created, stored or transmitted in digital form which may be relied upon in court or needs to be preserved as potential evidence in legal proceedings." [55]

Accordingly, while some states have adapted their laws to address electronic evidence, others continue to rely on traditional rules of criminal law and apply them to digital contexts.[56] Rules of evidence thus vary considerably, even among countries with similar legal traditions.[57]

4.2. Shared Procedural Aspects of Investigating and Using Electronic Evidence

As argued above, this study maintains that there is no distinct category of "electronic evidence" existing separately from traditional forms. All evidence is, at its core, information, and must satisfy the essential attributes of evidence: authenticity, relevance, and legality. The difference lies only in the manner of creation, existence, transformation, and form of such information.

In the context of today's information technology, new types of information—digital traces left by offenders in cyberspace—have emerged. These traces are stored in electronic data and exhibit characteristics that differ significantly from physical sources of evidence.

55 Jones and others (n 28).

56 Mifsud Bonnici, Tudorica and Cannataci (n 6).

57 UNODC (n 30) 158.

Accordingly, for such information to qualify as evidence and be admitted before a court, its preservation, collection, and use must be governed by a legal framework that prescribes specific procedures and methods.

Developing such a framework has therefore become a matter of central importance for all states, including European countries and Vietnam. The following section thus turns to examine the points of convergence between these two jurisdictions.

4.2.1. European Legal Framework

To date, the most direct and comprehensive legal framework governing procedures for the investigation and prosecution of cybercrime, including the critical issue of electronic evidence, while ensuring respect for human rights and the rule of law, is the Budapest Convention.[58] Under this Convention, electronic evidence may be collected, preserved, used, and exchanged in the same manner as in criminal investigations concerning both cybercrime and traditional offences, while simultaneously safeguarding human rights and the principles of the rule of law. The Convention has been extensively commented upon and elaborated through various legal instruments, which provide practical guidance for the handling of electronic evidence, such as:

Regarding investigative procedures for identifying electronic evidence: Electronic evidence is a special category of evidence, and its collection must ensure integrity, authenticity, and legality in order to be admissible in court. This requires specialised procedures beyond those used for traditional forms of evidence. Accordingly, the Budapest Convention recommends that member states enact legislation and adopt measures to establish the necessary powers and procedures for conducting criminal investigations and prosecutions related to offences covered by the Convention, as well as other crimes committed through computer systems and the collection of electronic evidence.[59]

These specialised procedures for investigating electronic evidence are further reflected in the application of special investigative measures, which include:

First, expedited preservation of stored computer data và partial disclosure of traffic data.[60] Preservation is an intrusive measure because it restricts the data owner's rights. The second characteristic is that preservation is merely a temporary measure designed to maintain the existing state of data for a maximum period of 90 days, subject to extension. Further legal authorisation is required for access and disclosure, accompanied by a confidentiality obligation to prevent compromising the investigation.[61] Preservation of data differs from data storage, as it ensures the data remains unaffected by external factors that could alter or

58 Convention on Cybercrime (n 4) arts 11–21.
59 ibid, art 14.
60 ibid, arts 16, 17.
61 Council of Europe (n 44) para 156.

degrade its quality or condition, and prevents unauthorised disclosure. The preservation process emphasises maintaining data integrity and serves solely for criminal investigation or prosecution, without any other intent. Data protection begins upon issuance of an order by a competent authority, and at the time of preservation, the information has not yet been disclosed to law enforcement agencies. To proceed, a subsequent step of data disclosure must be carried out under strict procedural safeguards. Specific rules governing the prompt provision of traffic data are crucial for the continuation of criminal investigations while awaiting authorisation for full disclosure. Article 17, paragraph 1(a), permits the collection of traffic data regardless of whether one or multiple service providers are involved. Article 17, paragraph 2(b), requires the entity subject to the preservation order to disclose to competent authorities a sufficient volume of traffic data to enable the tracking of communications and identification of the perpetrator.

Second, production order.[62] This measure may compel an individual or a service provider to submit specific stored information that they possess or control, including subscriber information under their custody. Subscriber information encompasses the type of communication service used, technical specifications, duration of service, and other data obtained by the provider through contractual or service agreements with the user (such as identity, address, contact details, payment information…).

Third, search and seizure of stored computer data.[63] This represents the next step in the process of investigating electronic evidence. It authorises law enforcement agencies to search computers or other data storage devices. This includes access to data stored on other networked or otherwise accessible computers from the device being searched. Additionally, it permits seizure, duplication, preservation, deletion, or disabling of access to such data. This is a highly technical operation aimed at ensuring the integrity of electronic evidence; thus, it may involve the participation of specialised experts at the request of law enforcement authorities.

Fourth, real-time collection of traffic data and Interception of content data.[64] These provisions authorise competent authorities to intercept communications /or request assistance from service providers, or directly collect traffic and content data. Such measures involve the interception of personal communications and pose a significant intrusion into the rights to privacy and freedom of communication. Therefore, they should be applied only in cases involving serious offences. Article 21 permits domestic legislation to determine which offences qualify for such measures. This classification is mandatory for the collection of content data, whereas traffic data collection remains optional. A State Party may choose to limit the collection of traffic data to a defined set

62 Convention on Cybercrime (n 4) art 18.

63 ibid, art 19.

64 ibid, arts 20, 21.

of criminal offences. However, this list must not be narrower than the list of serious offences for which the interception of content data is permitted.

The aforementioned measures provide sufficient legal basis and effective methods for the collection of electronic evidence. When implementing these measures, competent authorities must adhere to core requirements: ensuring the integrity, authenticity, and legality of electronic evidence; safeguarding human rights and freedoms; and upholding the principle of proportionality.[65] Article 15 of the Convention establishes a range of safeguards to ensure the legality of investigative procedures. These include judicial oversight or other forms of independent supervision, justification for the application of such measures, and limitations on the scope and duration of the powers or procedures involved.

In addition, the Council of Europe has issued the Electronic Evidence Guide (EEG) for law enforcement agencies and judicial authorities. [66] The EEG provides detailed guidance on on-site search and seizure procedures, methods for collecting evidence from the internet, and techniques for obtaining evidence from third parties. It also offers instructions on analysing electronic evidence and on preparing and presenting (or using) it in court proceedings. Recently, the Council and the European Parliament adopted Regulation (EU) 2023/1543 concerning the European Production Order and the European Preservation Order for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings.[67]

Regarding the criteria for assessing the admissibility and integrity of electronic evidence, such evidence is presented before the court, which is responsible for its evaluation. Courts in Europe typically assess such evidence in accordance with the principles and standards applied to traditional evidence, while also taking into account its unique characteristics of electronic evidence. This involves consideration of specific criteria, including: (i) the legality of investigative measures under Article 15 of the Budapest Convention, and (ii) the reliability of the technical procedures employed (such as interception methods, data backup, preservation techniques), often with the involvement of expert professionals.

For example, under France's Electronic Documents Law of 2000, a document in electronic form is admissible as evidence if it possesses the attributes of evidence and satisfies conditions such as lawful creation, integrity, reliability, and compliance with authentication and identification requirements. Germany's Code of Criminal Procedure[68] devotes Chapter 4, comprising six articles, to regulating the procedures, forms, and rules for collecting and authenticating electronic data. These provisions aim to ensure legality, reasonableness,

65 Council of Europe (n 44).
66 Jones and others (n 28).
67 Regulation (EU) 2023/1543 (n 48).
68 German Code of Criminal Procedure 'Strafprozeßordnung – StPO' (7 April 1987) <https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html> accessed 10 August 2025.

authenticity, reliability, and demonstrable integrity, thereby allowing such data to be accepted as electronic evidence.

Regarding the protection of human rights in the collection of electronic evidence, the European legal framework requires that the collection and use of electronic evidence must adhere to principles derived from Article 8 of the European Convention on Human Rights (ECHR), which guarantees the right to respect for private life, family, and correspondence. The European Court of Human Rights (ECtHR) has developed a set of standards to safeguard these rights:

1. *L*egality: All measures involving the collection of electronic data must be grounded in clear, transparent, and foreseeable legal provisions. The law must specify the scope of data collection, the authority responsible, procedural requirements, and time limitations.[69]

2. Necessity and proportionality: Data collection is permissible only when strictly necessary for a legitimate purpose (such as combating serious crime), and must be conducted in the least intrusive manner possible to achieve that objective.[70]

3. Independent judicial authorisation: Access to electronic data (including subscriber information and traffic data) must be authorised by an independent judicial body (a court), rather than solely by prosecutorial or investigative authorities.[71]

4. Data minimisation: Investigative agencies are permitted to collect only data directly relevant to the case. They are also obligated to delete any data outside the scope of the investigation to protect the privacy rights of third parties.[72]

The Convention thus sets forth only the fundamental principles. It consistently prioritises the autonomy of individual states in determining how to implement its provisions. Domestic legislation establishes both the conditions under which investigative powers may be exercised and the safeguards to protect against their misuse.[73] This approach has led to considerable diversity in the legal frameworks of member states, including those in Eastern Europe.

69 *Klass and Others v Germany* App no 5029/71 (ECtHR, 6 September 1978) <https://hudoc.echr.coe.int/eng?i=001-57510> accessed 10 August 2025.

70 *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) <https://hudoc.echr.coe.int/fre?i=001-159324> accessed 10 August 2025.

71 *Benedik v Slovenia* App no 62357/14 (ECtHR, 24 April 2018) <https://hudoc.echr.coe.int/fre?i=001-182455> accessed 10 August 2025.

72 *S and Marper v the United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) <https://hudoc.echr.coe.int/fre?i=001-90051> accessed 10 August 2025.

73 Francesco Calderoni, 'The European Legal Framework on Cybercrime: Striving for an Effective Implementation' (2010) 54(5) Crime, Law and Social Change 339. doi:10.1007/s10611-010-9261-6.

In this context, an overview of the legal frameworks of selected countries, such as Poland, the Netherlands, and Ukraine, helps clarify the potential basis for Vietnam's potential adoption. Notably, these countries do not possess a separate legal framework specifically governing the collection of electronic evidence; rather, such activities are regulated under the general provisions applicable to traditional evidence. For instance, in Poland, the collection of electronic evidence is conducted in the same manner as physical evidence, involving steps such as search, seizure, and visual examination.[74] Nonetheless, certain specific provisions do exist for electronic evidence.[75] Article 236a of the Polish Criminal Procedure Code, introduced in 2003,[76] provides for the corresponding application of procedural rules to individuals who possess or use devices containing electronic data or IT systems. This includes data stored on such devices, systems, or data storage media owned or used by them, including correspondence sent via email. The law does not prescribe specific techniques or methods for collecting physical evidence; instead, it delegates such tasks to experts in relevant forensic disciplines.[77] As a result, current guidelines on the handling of digital evidence remain non-binding in a formal legal sense.

Meanwhile, in the Netherlands, the collection of evidence is regulated under criminal procedure law, with several specialised measures in place. Many digital investigative methods are based on existing legal powers; for example, a seized computer may be searched in the same manner as a seized diary or firearm found in a residence.[78] In addition, new digital investigative techniques have been formally codified. The collection of electronic evidence in the Netherlands is also governed by the General Data Protection Regulation (GDPR).[79] The Police Data Act (Wet politiegegevens, Wpg)[80] regulates the use of personal data by police authorities, while the Judicial and Prosecution Data Act (Wet

74 Polish Criminal Procedure Code 'Kodeks postępowania karnego' (6 June 1997) ch 23, art 207 <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970890555> accessed 10 August 2025.

75 Piotr Lewulis, 'Digital Forensic Standards and Digital Evidence in Polish Criminal Proceedings: An Updated Definition of Digital Evidence in Forensic Science' (2021) 13(4) International Journal of Electronic Security and Digital Forensics 403. doi:10.1504/IJESDF.2021.10034988.

76 Law of Poland 'On Amending the Act – Code of Criminal Procedure, the Act – Provisions introducing the Code of Criminal Procedure, the Act on Crown Witnesses, and the Act on the Protection of Classified Information' (10 January 2003) [2003] DzU 17/155, art 1, para 79.

77 Lewulis (n 24).

78 Bert-Jaap Koops and Jan-Jaap Oerlemans, 'Formeel strafrecht en ICT ' in Bert-Jaap Koops and Jan-Jaap Oerlemans (eds), *Strafrecht en ICT* (Monografieën recht en informatietechnologie, SDU 2019) 117.

79 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

80 Wet politiegegevens (Wpg) (21 July 2007) <https://wetten.overheid.nl/BWBR0022463/2025-07-01> accessed 10 August 2025.

justitiële en strafvorderlijke gegevens, Wjsg)[81] governs the use of personal data by prosecutorial and judicial bodies.

Meanwhile, in Ukraine, electronic evidence appears to be more specifically regulated. The Ukrainian Criminal Procedure Code[82] addresses the collection of subscriber information and subscriber identification (Articles 162, 248, 263, and 268), with certain concepts referencing the Telecommunications Law, for example, the term "subscription". Special provisions concerning search and seizure, as outlined in Article 19 of the Budapest Convention, are incorporated into Ukraine's general regulations on seizure procedures and the involvement of experts and specialists in criminal proceedings.

Ukraine has implemented Articles 20 and 21 of the Budapest Convention, which pertain to the real-time collection of traffic data and the interception of content data under a similar regulatory framework. Article 39(4) of the Telecommunications Law obliges telecommunications operators to bear the costs of "installing and maintaining the technical means necessary for search and investigative authorities, as well as cybersecurity monitoring bodies in Ukraine, to carry out their functions. Operators must also, within the scope of their authority, facilitate search and investigative activities, ensure operational oversight, and prevent the disclosure of organisational and tactical methods employed." [83] Additionally, the law requires operators to protect these technical systems against unauthorised access.

In terms of procedural implementation, Articles 258 to 266 of Ukraine's Criminal Procedure Code provide the legal basis for certain covert investigative actions (surveillance), including interference with individuals' private communications. Within the context of Articles 20 and 21 of the Budapest Convention, the relevant activity primarily involves the "collection of information from telecommunications traffic networks" (Article 263 of the Criminal Procedure Code).

4.2.2. Vietnam's Framework on Investigation of Electronic Evidence

The investigation of electronic evidence in Vietnam is currently governed under the general framework applicable to traditional evidence. According to the 2015 Criminal Procedure Code (CPC),[84] only three articles directly address electronic evidence. Specifically, Article 97 defines electronic data and electronic devices; Article 223 outlines special investigative measures; and Article 107 regulates the process of investigating electronic evidence, which includes the

81 Wet justitiële en strafvorderlijke gegevens (Wjsg) (7 November 2002) <https://wetten.overheid.nl/BWBR0014194/2025-07-01> accessed 10 August 2025.

82 Criminal Procedural Code of Ukraine No 4651-VI (13 April 2012) <https://zakon.rada.gov.ua/go/4651-17> accessed 10 August 2025. [in Ukrainian]

83 Law of Ukraine No 1280-IV 'On Telecommunications' (18 November 2003) <https://zakon.rada.gov.ua/laws/show/1280-15> accessed 10 August 2025. [in Ukrainian]

84 Law of Vietnam No 101/2015/QH13 (n 12).

following steps: seizure, backup, preservation, recovery, and forensic examination. Accordingly, the procedural authorities are required to carry out the following steps:

1. Identification of the source and scope of evidence: This includes devices (phones, computers, cameras), accounts/services (email, social media, cloud platforms), system logs, and data in transmission. Investigators must then plan and conduct searches based on procedural documents such as search warrants, seizure orders, or special investigative measures.
2. Preservation of the on-site status quo: This involves accurately documenting the condition of the device or account, capturing screenshots, recording system configurations and running applications, and sealing the storage medium (if seized).
3. Seizure or backup when physical seizure is not feasible: This includes confiscating the device and related accessories. If the device is fixed or cannot be removed, data must be backed up to a storage medium (e.g., a hard drive or a USB drive) and treated as physical evidence. Technical experts may be invited to assist.
4. Full documentation of extraction/interception/backup from networks or transmission channels (e.g., logs from service providers, servers, or cloud services), which must be included in the case file (Article 107 CPC).
5. Sealing and preservation as physical evidence: Immediate sealing after seizure, unsealing according to legal procedures, and maintaining a chain of custody.
6. Forensic duplication and integrity verification: Creating forensic images or copies, generating hash values for comparison; all recovery, decryption, and examination must be performed on the copy, not the original.
7. Examination, recovery, and decryption: Conducted under an official forensic order; results must be converted into readable, audible, or viewable formats for use in proceedings.
8. Evaluation and use as evidence: Assessment of legality, origin, integrity, and ability to identify the creator; evidence must be presented with the original storage medium or a valid copy.
9. Covert collection channel (if conditions are met): After prosecution is initiated, authorities may request the application of special procedural measures for "covert collection of electronic data," subject to strict compliance with conditions, jurisdiction, duration, and document management.

From the above observation and analysis of Vietnamese law and European law, the following similarities have been identified:

First, while the concept of electronic evidence is not explicitly defined in law, both legal theory and statutory frameworks recognise electronic evidence as information, and the medium that carries such information is electronic data, which is also referred to in Vietnam

as a source of evidence. Although electronic data is not yet classified as a distinct evidentiary source, electronic evidence nonetheless satisfies the general requirements of admissible evidence: authenticity, relevance, and legality. Moreover, electronic evidence possesses unique characteristics arising from its digital environment, the nature of the tools used to commit crimes, and its transnational dimension.

Second, the legal framework governing evidence is grounded in the core principles of criminal procedure law, which apply uniformly to physical evidence, testimonial evidence, and electronic evidence. This approach is consistent with the traditions of continental European legal systems.

Third, based on these distinctive features, both the Budapest Convention and Vietnamese law have developed a legal framework for electronic evidence. This framework includes: identifying electronic data as the source of electronic evidence; establishing procedures for detecting, collecting, preserving, and presenting electronic evidence in court; and ensuring the admissibility and integrity of digital evidence extracted from electronic devices in criminal proceedings.

5 LEGAL GAPS IN ELECTRONIC EVIDENCE REGULATION IN VIETNAM COMPARED TO THE BUDAPEST CONVENTION

The differences in the legal framework governing electronic evidence across regions of the world are shaped by multiple factors, including the underlying theories of evidence adopted in each region and the prevailing model of criminal procedure. Therefore, before assessing the legal gaps in Vietnam's regulation of electronic evidence vis-à-vis European standards, a general account of the theoretical foundations of evidence law and the criminal procedure model in Vietnam is provided.

On the theory of evidence and proof. At present, the regulation of evidence is comprehensively contained within Vietnam's Criminal Procedure Code. The history of legal thought has witnessed several major theories of evidence, including the formal theory of evidence, the doctrine of free evaluation of evidence, the Anglo-Saxon evidentiary tradition, and the former Soviet evidentiary doctrine. As with other aspects of criminal procedure, the Vietnamese law of evidence has been profoundly shaped by the Soviet evidentiary doctrine, the main tenets of which are:

(i) evidence must be authentic, requiring that the information contained therein correspond to what has occurred in objective reality, with its reliability depending largely on the competence, ethics, and professionalism of the investigative authorities;

(ii) evidence must be lawful, requiring that it be collected in strict compliance with statutory procedures, with any violation of this standard rendering the evidence inadmissible; and

(iii) evidence must be probative, meaning it must be capable of proving the facts that require determination in the criminal case.

Taken as a whole, the current Vietnamese evidentiary doctrine is closely aligned with the theory of free evaluation of evidence based on the inner conviction of the judge, which is widely accepted in many European jurisdictions. This can be illustrated by a specific case adjudicated by a Vietnamese court.

In this case, a police investigator was accused of accepting a bribe in exchange for exonerating a suspect involved in repatriating citizens to Vietnam during the COVID-19 pandemic. Numerous pieces of evidence were presented against the defendant, including witness testimonies. A particularly significant piece of evidence was a surveillance camera recording showing the investigator receiving a suitcase from an individual at the entrance of his office. This image aligned with the testimonies of the alleged bribe-giver and other witnesses regarding the time and location of the transaction. However, during the trial, the investigator claimed that the suitcase contained bottles of wine, not money.

The central question became whether the suitcase held cash or wine. Despite the ambiguity, the court concluded that the investigator had accepted money and was guilty of bribery. This decision sparked considerable debate,[85] as the evidence appeared insufficient to dispel reasonable doubt. The judge's inner conviction was reportedly based on the reasoning: "No one gifts wine in a suitcase."

In adjudicating cases of this nature, judges in European legal systems typically apply the principle of proof beyond a reasonable doubt. This evidentiary standard requires that the prosecution's burden of proof reach a threshold sufficient to overcome the legal presumption of innocence, including, but not limited to, adherence to the principle of in *dubio pro reo*, whereby any unresolved doubt must be interpreted in favour of the accused. Where this threshold is not met, the adjudicator is obliged to acquit, as the presumption of innocence remains legally intact.

In the case under discussion, the central issue of reasonable doubt pertains to the nature of the item allegedly received: was it money or wine? This constitutes a material uncertainty that the prosecution and the court must resolve to lawfully convict. If the prosecution fails to establish that the item in question was money, then, in accordance with the spirit of the presumption of innocence, the doubt must be construed in favour of the defendant-i.e., the item should be considered wine. Nonetheless, the court appears to have rendered a guilty verdict for bribery without a sufficient evidentiary basis to overcome this doubt. This has

85 Xuan Nha, 'The Suitcase is Not the Only Evidence to Charge the Former Head of the Ministry of Public Security's Investigation Security Agency' *Báo điện tử Bảo vệ pháp luật* (Hanoi, 24 July 2023) <https://baovephapluat.vn/phap-dinh/cau-chuyen-phap-luat/chiec-vali-khong-phai-chung-cu-duy-nhat-de-buoc-toi-cuu-truong-phong-thuoc-co-quan-an-ninh-dieu-tra-bo-cong-an-143192.html> accessed 10 August 2025. [in Vietnamese]

generated ongoing legal and scholarly debate regarding the legitimacy of the conviction and the proper application of evidentiary standards in light of the presumption of innocence.[86]

Any comparative analysis of criminal procedure must begin with an examination of the underlying procedural model. The criminal procedure model determines how truth is established in a criminal case, including the treatment of evidence. Vietnamese criminal law belongs to the legal tradition of former communist countries, similar to those in Eastern Europe. The influence of communist ideology on the legal systems of these nations has been widely studied.[87]

Nonetheless, Vietnam's legal system is also considered to be shaped by the civil law tradition, owing to its history as a French colony for nearly a century.[88] Also, Vietnamese law shares notable similarities with China, which, despite its nationalist orientation, has relied on civil law principles to construct its criminal procedure framework. While substantive laws and procedural mechanisms may differ across jurisdictions, all legal systems share a fundamental objective: to ascertain the truth and apply legal principles to factual circumstances.

As a universal rule, human beings, regardless of nationality, strive to achieve a just outcome.[89] Vietnam's criminal procedure model remains fundamentally inquisitorial, shaped by the civil law tradition, enabling it to absorb elements from the procedural frameworks of continental European countries. Nonetheless, adversarial features have been gradually incorporated. The system does not reject adversarial principles; in fact, alongside foundational norms such as the presumption of innocence and the right to defence, the principle of adversarial proceedings has recently been formally recognised in Vietnam's Criminal Procedure Code.

A defining characteristic of Vietnam's current criminal procedure model is that it is not structured around distinct functional roles, such as prosecution, defence, and trial, but rather operates through a clearly delineated sequence of procedural stages: initiation, investigation, prosecution, and trial. This structure reflects the state's monopoly over criminal proceedings, wherein public resources are concentrated on detecting and adjudicating criminal offences, primarily through specialised state agencies.[90] While differences remain, Vietnam's reformed criminal procedure model now closely resembles the inquisitorial systems found in several Eastern European countries.

86 ibid.

87 Joseph M Snee, SJ and A Kenneth Pye, 'Due Process in Criminal Procedure: A Comparison of Two Systems' (1960) 21(4) Ohio State Law journal 467.

88 LL Nemes, 'Hungarian Law of Criminal Procedure In the Light of the Mindzenti Trial' (1957) 17 Jurist 157.

89 Joseph M Snee and Kenneth A Pye, *Status of Forces Agreements and Criminal Jurisdiction* (Literary Licensing LLC 2013).

90 Nguyen Thi Thuy, 'Vietnam's Criminal Procedure Model and the Possibility of Applying the Adversarial Procedure Model' (PhD thesis, Vietnam National University 2014) 54. [in Vietnamese]

The following discussion examines the legal gaps in Vietnam's regulation of electronic evidence in comparison with European standards.

Regarding the investigation of electronic evidence, Vietnam still lacks several procedural components compared to the standards set by the Budapest Convention and European countries. Specifically, there is an absence of detailed legal provisions governing the necessary procedures for handling electronic evidence; no clear regulations or protocols exist for the seizure, preservation, and restoration of electronic data to ensure its safety, integrity, and evidentiary value; and there are no specialised rules for the management and use of this unique category of evidence. For example, searches of computers and electronic devices currently follow general search procedures, without dedicated protocols tailored to digital environments. The three articles in the Vietnamese Criminal Procedure Code that directly address electronic evidence are insufficient to establish a comprehensive legal framework. At present, specific procedures and technical measures are only outlined in internal operational guidelines issued by investigative and prosecutorial agencies. Under the principle of due process, evidence obtained through such unofficial procedures may not meet the standard of legality, as the investigative measures are not grounded in statutory law.

Moreover, several critical aspects of electronic evidence investigation are either omitted or only superficially addressed in Vietnam's criminal procedure law, including interception of content data and issuance of production orders. These remain classified as operational techniques rather than codified legal procedures.

The investigation of electronic evidence is closely tied to the entities that possess such data, including service providers. However, Vietnam's Criminal Procedure Code overlooks this category of actors and treats them in the same manner as traditional evidence holders, merely stating that "procedural authorities may request agencies or organisations to submit evidence". A recent high-profile case in Vietnam highlights this legal shortcoming: the Rikvip/Tip.Club online gambling ring, led by Phan Sào Nam and Nguyễn Văn Dư□ng, adjudicated by the People's Court of Phú Th□ Province,[91] stands as one of the most prominent examples of electronic evidence usage in criminal investigation and prosecution. The online card game system operated from 2014 to 2017, attracting millions of user accounts and generating illicit revenues estimated in the trillions of Vietnamese đ□ng. During the investigation, authorities conducted searches and seizures of servers, system data, and transaction logs. The electronic data collected included user information, login records, and financial flows through agents and intermediary payment gateways. Investigators extracted data from the servers and cross-referenced it with financial transactions and witness statements, thereby reconstructing actual revenue figures and identifying the specific roles of the defendants. The court admitted these digital records as electronic evidence to substantiate charges of "organising gambling" and "money laundering."

91 Case No 68/2020/HS-ST [2020] People's Court of Phu Tho Province.

This case highlights a notable strength of Vietnamese law: its recognition of electronic data as admissible evidence, as stipulated in Article 87 of the 2015 Criminal Procedure Code. However, it also reveals critical gaps in the legal framework. Specifically, Vietnam has yet to establish a mechanism for issuing preservation orders to freeze data before it can be deleted, and lacks a production order system to compel service providers to promptly supply data in standardised technical formats. Compared to CETS standards,[92] Vietnam is missing two essential legal instruments, thus increasing the risk of data loss and significantly hampering international cooperation in cybercrime investigations. Specifically, ETS clearly defines the rights and obligations of these entities through instruments such as the Production Order, which allows law enforcement authorities in one EU member state to request electronic data from service providers established or represented in another member state and compel its transfer.[93] Additionally, law enforcement agencies may issue a Preservation Order requiring service providers to retain electronic data for future production, thereby preventing its deletion or overwriting.

Regarding the authenticity of electronic evidence, comparative practice offers further insight. In Poland, electronic evidence is understood in two distinct senses. In the broad sense (sensu largo), digitally-originated data is entered into the case file in printed or summarised form and is primarily assessed based on its content. In this context, there is little to no technical processing aimed at verifying or preserving the data's integrity. In the narrow, technical sense (sensu stricto), data is collected, preserved, and analysed according to standardised forensic procedures. Its evidentiary value depends significantly on the ability to demonstrate its integrity, origin, and chain of custody.[94] This dual-layered approach reflects the practical operations of Polish courts and aligns with international legal trends that permit certain data to be self-authenticating, provided it meets requirements regarding origin and procedural handling. It enables courts to determine when full technical forensic analysis is necessary and when printed data from a reliable source may be reasonably accepted as evidence.

In contrast, due to limitations in technical capacity and in the expertise of investigators, prosecutors, and judges, electronic evidence in Vietnam is currently understood primarily in the broad sense. The most common and significant method of converting electronic evidence in Vietnam today involves printing all retrieved data onto paper. Police officers then prepare a written record documenting the seizure of all printed materials extracted from the suspect's hard drive or digital device.

The following case illustrates this legal gap. The Nhật Cư□ng Mobile case, adjudicated by the Hanoi People's Court in 2022, serves as a notable example of the decisive role electronic evidence plays in economic and corruption-related proceedings. Investigative

92 Convention on Cybercrime (n 4) arts 16–21.

93 Thomas Wahl, 'E-evidence Regulation and Directive Published' (2023) 2 Eucrim 165.

94 Lewulis (n 75).

authorities collected and extracted electronic data from the company's internal enterprise resource planning (ERP) system, including sales records, illegal import orders, financial transactions, and electronic accounting documents. Based on this data, the prosecution reconstructed 2,502 import orders involving 254,364 smuggled products with a total value exceeding 3,000 billion VND, and identified illicit profits amounting to over 221 billion VND. The court recognised these extracted data records as electronic evidence with direct probative value in establishing acts of smuggling, money laundering, and violations of accounting regulations.[95]

However, from a comparative legal perspective, this case highlights notable gaps in Vietnam's legal framework. Under European standards—specifically Article 18 of the Budapest Convention—requests for corporate data must be executed through a formal production order, which clearly defines the authority issuing the request, the scope of data, applicable time limits, and format requirements. Vietnam's 2015 Criminal Procedure Code has yet to establish a corresponding legal mechanism. As a result, the collection of electronic evidence in the Nhật Cư□ng case relied primarily on manual procedures such as searches, seizures, and data extraction. This approach poses challenges for data standardisation and diminishes the adversarial value of the evidence during trial proceedings.

The need for specialists in computer science and information technology has become increasingly urgent for courts confronted with technologically advanced crime. Such specialists assist investigators in prosecuting offenders by analysing and deploying data processing systems and software tools. Their expertise and effectiveness play a crucial role in enabling investigators to access, organise, and interpret electronic evidence.[96] For example, in Italy, Article 244 (2) of the Code of Criminal Procedure (Codice di Procedura Penale) stipulates that in identifying digital evidence, the legislator must ensure that inspections and searches are carried out using "technical measures capable of ensuring preservation and preventing alteration of the original data."[97]

Currently, Vietnam's criminal procedure law does not distinguish between the process of collecting evidence through investigation, digital forensic procedures, and digital investigative workflows. Digital forensics is a discipline that applies computer science in conjunction with investigative techniques to meet legal requirements. When authorised by competent authorities, digital forensics involves the collection and analysis of electronic evidence, the establishment of a chain of custody, the preparation of expert reports, and the presentation of findings using legally sanctioned tools.[98] Digital forensics ensures the

95 Case No 144/2021/HS-ST [2022] People's Court of Hanoi.

96 Fredesvinda Insa, 'The Admissibility of Electronic Evidence in Court (AEEC): Fighting Against High-Tech Crime–Results of a European Study' (2007) 1(4) Journal of Digital Forensic Practice 285. doi:10.1080/15567280701418049.

97 Codice di procedura penale No 447 (22 September 1988) <https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-di-procedura-penale> accessed 10 August 2025.

98 Le (n 31).

authenticity and integrity of electronic evidence. However, in Vietnam, digital forensics currently plays only a limited role as a post-investigation assessment tool. To guarantee the authenticity and integrity of electronic evidence, it must be integrated throughout the entire investigative process. The absence of digital forensic involvement and a dedicated procedural framework raises concerns about the reliability and integrity of electronic evidence. A proper digital investigation process requires operational precision at each stage; standardisation of procedural sequences; coordinated, synchronised, and efficient collaboration among investigative units; and systematic documentation of investigative activities to support the chain of custody and enable retrospective verification. Despite its importance, digital investigation in Vietnam remains classified as an internal operational technique rather than a formally codified legal procedure.

Regarding the evaluation of electronic evidence, Vietnam's Criminal Procedure Code does not yet provide specific criteria. Instead, it refers to standards found in the Law on Electronic Transactions, which include: (1) the reliability of the method used to create, store, and transmit the data; (2) the method used to ensure and maintain data integrity; and (3) the method used to identify the originator and related factors. By contrast, internationally accepted standards for evaluating electronic evidence typically include: (1) whether the technology has been tested; (2) whether it has undergone rigorous evaluation; (3) whether known error rates are associated with the technology; (4) whether operational control standards exist and are maintained; and (5) whether the technology is widely accepted by the scientific community.

The reliability of electronic evidence must be assessed on the basis of sound technological criteria.[99] The absence of such standards in Vietnam has led to uncertainty in judicial evaluations. In one criminal case, although both the victim and the defendant admitted that an email contained fraudulent content, the email's authenticity could not be verified through a proper electronic evidence investigation. Accepting the email risked violating evidentiary standards; rejecting it risked overlooking a criminal act.

In another case involving assault and damage to two motorcycles, the case file included printed images depicting one young man holding a hammer and a knife, and two others holding a metal chair in a threatening manner. The court nevertheless relied solely on these printed images to convict the defendants without verifying their authenticity through a digital forensic process.

A further illustration is the case involving Mr Cao Toan My and beauty queen Truong Ho Phuong Nga. Mr My accused Ms Nga of appropriating VND 16.5 billion through a fraudulent real estate contract that was never executed. She was prosecuted for "fraudulent appropriation of property". However, during trial proceedings, the defendant testified that the VND 16.5 billion was not payment for a house, but rather part of a seven-year "intimate

99 Zatyko and Bay (n 3).

relationship agreement" with Mr My. The defence submitted emails and electronic messages to support this claim. Yet the evidence consisted only of printed email copies that had not been verified by the service provider, leading to intense disputes over their authenticity and integrity. This case highlights a critical gap in Vietnamese law regarding the verification of electronic evidence: electronic communications provided by parties lacked forensic authentication and were not obtained through formal production orders. As a result, the evidentiary process failed to meet international standards for reliability and adversarial fairness. To address these deficiencies, Vietnam requires clear legal provisions governing the authenticity, integrity, and legality of electronic evidence, aligned with international norms, including the Budapest Convention and European Union standards.[100]

Vietnam's criminal procedure remains inquisitorial, with case files compiled by investigative and prosecutorial authorities from the moment a case is initiated. The court conducts its trial based primarily on this dossier, following the principle *Quod non est in acta, non est in mundo* (what is not in the record does not exist).[101] As a result, adversarial proceedings for evaluating electronic evidence remain limited. In practice, electronic evidence derived from digital data is primarily presented as printed copies produced by investigative authorities, which raises concerns about its authenticity. The lack of adversarial scrutiny is further reflected in the disadvantaged position of defence counsel, who face significant restrictions in their rights and ability to collect electronic evidence. As a result, the determination of factual truth in criminal cases relies almost entirely on evidence submitted by the prosecution. For example, under Vietnam's Criminal Procedure Code, any documents or objects obtained by the accused, defence counsel, or any other parties must be handed over to the investigative authority and only become evidence if that authority accepts them into the case file.

Protection of Human Rights remains a significant challenge for countries seeking to domesticate the Budapest Convention. The investigation of electronic evidence carries a high risk of infringing upon the right to privacy. European countries have established numerous safeguards to protect human rights, whereas Vietnam currently lacks a robust mechanism to ensure such protection during electronic evidence investigations. In Vietnam, the process is notably favourable to law enforcement authorities, as service providers are required to supply electronic evidence without any statutory limitations, especially during pre-prosecution surveillance activities conducted by police. However, this raises serious concerns from a human rights perspective. Investigative measures involving electronic evidence inherently restrict individual rights, and the authority to approve such measures should rest with the judiciary. Yet, as previously discussed, in Vietnam, the

100 Gia Minh, 'Temporarily Suspend Investigation of Miss Phuong Nga Case' (*Tuoi Tre Online*, 10 August 2017) <https://tuoitre.vn/tam-dinh-chi-dieu-tra-vu-an-hoa-hau-phuong-nga-1366696.htm> accessed 20 September 2025. [in Vietnamese]

101 Đào Trí Úc, 'Principles of Criminal Procedure Vienam' (2011) 27(1) Tạp chí Khoa học ĐHQGHN, Luật học 10. [in Vietnamese]

approval for searches and seizures is granted by the prosecution, not the court. This raises doubts about the legitimacy, reasonableness, and legality of such actions, and fuels fears of arbitrary violations of fundamental human rights.

These concerns were evident in the Rikvip/Tip.Club case.[102] First, mass data seizure without relevance filtering occurred: during the server data extraction process, investigative authorities seized comprehensive user information, including personal data from millions of accounts unrelated to the alleged criminal conduct. The 2015 Criminal Procedure Code lacks clear provisions regarding the scope, retention period, or deletion of data beyond the investigative remit, thereby creating risks of abuse and privacy violations. Second, judicial oversight was absent. Data seizure and extraction were conducted based on decisions by investigative bodies and Procuracy approvals, without an independent court-issued warrant. This stands in contrast to European legal practice, where any access to personal data requires judicial authorisation to ensure legality, necessity, and proportionality. Third, defence rights and adversarial principle were limited. Electronic evidence was primarily printed and included in the case file. Dence lawyers were not granted access to forensic copies for independent verification, undermining their ability to challenge the evidence and weakening the adversarial balance in proceedings.

Regarding international cooperation, cybercrime is inherently transnational, with digital traces often extending beyond national borders. As a result, international cooperation in the investigation of electronic evidence is critically important, yet remains complex and sensitive for many countries, including Vietnam. At present, Vietnam has not fully engaged in bilateral or multilateral cooperation frameworks on this issue, resulting in difficulties when investigating cross-border electronic evidence due to legal conflicts.

In the aforementioned fraud case involving beauty queen Phư?ng Nga, the defendant presented an email sent via Gmail to support her claim. The alleged sender denied having written the email. The court requested the investigative agency to verify the ownership of the Gmail account. The agency sought assistance from Interpol, as the Gmail server is located in the United States. However, the request was denied due to U.S. privacy laws, which prohibit service providers from disclosing account ownership information. This example illustrates the necessity for Vietnam to engage promptly with, and align its domestic legislation to, established international cooperation frameworks, so that cross-border requests for the collection and verification of electronic evidence do not fall into institutional deadlock, the consequences of which would significantly weaken the State's ability to address cybercrime in an effective and proportionate manner.

102 Case No 68/2020/HS-ST [2020] People's Court of Phu Tho Province.

6 CONCLUSIONS

The acknowledgement of electronic data as a source of evidence in Vietnam's 2015 Criminal Procedure Code marks a significant advancement in the country's adaptation to the rise of high-tech crime. However, when compared to international standards, particularly the Budapest Convention, the current legal framework still exhibits substantial gaps, including the absence of standardised procedures, insufficient human rights safeguards, ineffective mechanisms for international cooperation, and a lack of digital forensic standardisation. Based on comparative legal analysis, several reform directions emerge:

First, the process of investigating electronic evidence should be codified through a national standard procedure covering detection, documentation, seizure, preservation, and forensic examination of electronic data. This should include mandatory chain-of-custody protocols and standardised tools. Vietnam should incorporate procedural instruments recognised under the Budapest Convention, such as preservation orders, production orders, and search-and-seizure mechanisms.

Second, human rights protections and judicial oversight must be strengthened. The authority to approve intrusive electronic-data-collection measures should be transferred from the procuracy to the judiciary, reinforcing checks and balances and ensuring proportionality and necessity. The principle of data minimisation should be codified, along with mandatory deletion of data beyond the scope of investigation.

Third, the adversarial principle should be reinforced. Defence counsel must be guaranteed access to forensic copies of electronic evidence for independent verification. Courts must ensure that electronic data is presented in readable, audible, or viewable formats rather than solely as printed documents.

Fourth, service provider obligations must be clarified. Telecommunications, internet, and social media companies should be subject to regulations governing data retention, provision, and authentication of electronic data, accompanied by liability and compensation mechanisms for non-compliance.

Fifth, international cooperation should be expanded. Vietnam should expedite accession to the Budapest Convention and prepare to participate in the forthcoming United Nations Convention on Cybercrime. These instruments will provide a legal basis for cross-border data requests and help overcome conflicts of law.

Sixth, digital forensic capacity must be standardised. Minimum competency requirements for digital forensic examiners should be established, independent forensic centres should be developed, and collaboration with international forensic laboratories should be promoted.

In conclusion, electronic evidence has become an inevitable component of modern criminal proceedings. Reforming Vietnam's legal framework in accordance with the recommendations above will not only enhance investigative efficiency but also preserve the

balance between crime control and human-rights protection. Such reforms will bring Vietnam closer to international standards—particularly those of the Budapest Convention and European legal systems—thereby strengthening the legitimacy, transparency, and fairness of the criminal justice system.

REFERENCES

1. Avdeeva G and Żywucka-Kozlowska E, 'Problems of Using Digital Evidence in Criminal Justice of Ukraine and the USA' (2923) 1(30) Theory and Practice of Forensic Science and Criminalistics 126. doi:10.32353/khrife.1.2023.07
2. Biasiotti MA and others, 'Opportunities and Challenges for Electronic Evidence' in Biasiotti MA and others (eds), *Handling and Exchanging Electronic Evidence Across Europe* (Springer 2018) 3. doi:10.1007/978-3-319-74872-6_1
3. Biedermann A and Kotsoglou KN, 'Digital Evidence Exceptionalism? A Review and Discussion of Conceptual Hurdles in Digital Evidence Transformation' (2020) 2 Forensic Science International: Synergy 262. doi:10.1016/j.fsisyn.2020.08.004
4. Blahuta R, Movchan A and Movchan M, 'Use of Electronic Evidence in Criminal Proceedings in Ukraine' (International Conference on Social Science, Psychology and Legal Regulation (SPL 2021) Kyiv, Ukraine, 22-24 December 2021) 196. doi:10.2991/assehr.k.211218.032
5. Calderoni F, 'The European Legal Framework on Cybercrime: Striving for an Effective Implementation' (2010) 54(5) Crime, Law and Social Change 339. doi:10.1007/s10611-010-9261-6
6. Carrier BD and Spafford EH, 'An Event-Based Digital Forensic Investigation Framework' (DFRWS 2004 Digital Forensic Research Conference, USA, Baltimore, MD, 11-13 August 2004)
7. Casey E, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn, Academic Press 2011)
8. Custers B and Stevens L, 'The Use of Data as Evidence in Dutch Criminal Courts' (2021) 29(1) European Journal of Crime, Criminal Law and Criminal Justice 25. doi:10.1163/15718174-bja10015
9. Dao TU, 'Principles of Criminal Procedure Vienam' (2011) 27(1) Tạp chí Khoa học ĐHQGHN, Luật học 10. [in Vietnamese]
10. Gebicki M, 'Cross-border Acquisition of Digital Data in Criminal Proceedings: State of Play and Measures Taken by the European Union and the Council of Europe' (2024) 1(29) Teisės apžvalga 3. doi:10.7220/2029-4239.29.1

11. Gia M, 'Temporarily Suspend Investigation of Miss Phuong Nga Case' (*Tuoi Tre Online*, 10 August 2017) <https://tuoitre.vn/tam-dinh-chi-dieu-tra-vu-an-hoa-hau-phuong-nga-1366696.htm> accessed 20 September 2025. [in Vietnamese]
12. Gillespie J, 'Towards a Discursive Analysis of Legal Transfers into Developing East Asia' (2008) 40(3) NYU Journal of International Law and Politics 657.
13. Goodison SE, Davis RC and Jackson BA, 'Digital Evidence and the US Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence' (*RAND*, 20 April 2015) <https://www.rand.org/pubs/research_reports/RR890.html> accessed 10 August 2025
14. Insa F, 'The Admissibility of Electronic Evidence in Court (AEEC): Fighting Against High-Tech Crime–Results of a European Study' (2007) 1(4) Journal of Digital Forensic Practice 285. doi:10.1080/15567280701418049
15. Jones N and others, *Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges* (version 2.1, Council of Europe 2020) <https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4> accessed 10 August 2025.
16. Juszczak A and Sason E, 'The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence' (2023) 2 Eucrim 182.
17. Kerr OS, 'Searches and Seizures in a Digital World' (2005) 119(2) Harvard Law Review 531.
18. Kissel R (ed), *Glossary of Key Information Security Terms* (Diane Publishing 2011)
19. Koops BJ and Oerlemans JJ, 'Formeel strafrecht en ICT' in Koops BJ and Oerlemans JJ (eds), *Strafrecht en ICT* (Monografieën recht en informatietechnologie, SDU 2019) 117
20. Le TQ, 'Difficulties in Determining the Properties of Electronic Evidence' (2024) 15 Tạp chí Kiểm sát 10. [in Vietnamese]
21. Lewulis P, 'Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law' (2022) 33(1) Criminal Law Forum 39. doi:10.1007/s10609-021-09430-4
22. Lewulis P, 'Digital Forensic Standards and Digital Evidence in Polish Criminal Proceedings: An Updated Definition of Digital Evidence in Forensic Science' (2021) 13(4) International Journal of Electronic Security and Digital Forensics 403. doi:10.1504/IJESDF.2021.10034988
23. Lewulis P, *Dowody cyfrowe: teoria i praktyka kryminalistyczna w polskim postępowaniu karnym* (Wydawnictwo Uniwersytetu Warszawskiego 2021)
24. Mason S and Seng D (eds), *Electronic Evidence* (University of London Press 2017). doi:10.14296/517.9781911507079

25. Mifsud Bonnici JP, Tudorica M and Cannataci JA, 'The European Legal Framework on Electronic Evidence' in Maria Angela Biasiotti and others, *Handling and Exchanging Electronic Evidence Across Europe* (Springer 2018) 189. doi:10.1007/978-3-319-74872-6_11

26. Nemes LL, 'Hungarian Law of Criminal Procedure In the Light of the Mindzenti Trial' (1957) 17 Jurist 157

27. Nguyen BT, 'Improving Vietnam's Electronic Evidence Law in the Industry 4.0 Era: Experience from China' (2024) 16(1) Revista de Direito 1. doi:10.32361/2024160117322

28. Nguyen NC and Le LC (eds), *Criminal Procedure Law Textbook* (Hanoi National University Press 2018) [in Vietnamese]

29. Nguyen NK, 'Source of Evidence is Electronic Data in Criminal Proceedings in Vietnam and Some Countries in the World' (Master's thesis, Vietnam National University 2024) [in Vietnamese]

30. Nguyen TT, 'Vietnam's Criminal Procedure Model and the Possibility of Applying the Adversarial Procedure Model' (PhD thesis, Vietnam National University 2014) [in Vietnamese]

31. Onțanu EA, Normalising the Use of Electronic Evidence: Bringing Technology Use into a familiar Normative Path in Civil Procedure' (2022) 12(3) Oñati Socio-Legal Series 582. doi:10.35295/osls.Iisl/0000-0000-0000-1304

32. Pollitt M, 'A History of Digital Forensics' (6th IFIP WG 11.9 International Conference on Digital Forensics (DF), Hong Kong, China, Jan 2010) 3. doi:10.1007/978-3-642-15506-2_1

33. Snee JM and Pye AK, 'Due Process in Criminal Procedure: A Comparison of Two Systems' (1960) 21(4) Ohio State Law journal 467

34. Snee JM and Pye AK, *Status of Forces Agreements and Criminal Jurisdiction* (Literary Licensing LLC 2013)

35. Tran QT, *Evidence Regulation in Vietnamese Criminal Procedure Law* (National Political Publishing House 2011) [in Vietnamese]

36. Tran VH, 'The Issue of Electronic Traces and Evidence in the Amended Criminal Procedure Code' (2014) 12 Tạp chí Khoa học và Chiến lược. [in Vietnamese]

37. Tsekhan DM, 'Digital Evidence: Concept, Features and Place in the Evidence System' (2013) 5 Scientific Bulletin of the International Humanities University, Series: Jurisprudence 256. [in Ukrainian]

38. Vazquez Maymir S, 'Anchoring the Need to Revise Cross-Border Access to eEvidence' (2019) 9(3) Internet Policy Review 1. doi:10.14763/2020.3.1495

39. Wahl T, 'E-evidence Regulation and Directive Published' (2023) 2 Eucrim 165

40. Wang W and Daniels TE, 'Building Evidence Graphs for Network Forensics Analysis' (21st Annual Computer Security Applications Conference ACSAC 2005). doi:10.1109/CSAC.2005.14

41. Xuan N, 'The Suitcase is Not the Only Evidence to Charge the Former Head of the Ministry of Public Security's Investigation Security Agency' *Báo điện tử Bảo vệ pháp luật* (Hanoi, 24 July 2023) <https://baovephapluat.vn/phap-dinh/cau-chuyen-phap-luat/chiec-vali-khong-phai-chung-cu-duy-nhat-de-buoc-toi-cuu-truong-phong-thuoc-co-quan-an-ninh-dieu-tra-bo-cong-an-143192.html> accessed 10 August 2025. [in Vietnamese]

42. Zatyko K and Bay J, 'The Digital Forensics Cyber Exchange Principle' (*Villanova University, College of Liberal Arts and Sciences*, 22 April 2013) <http://www.csc.villanova.edu/~dprice/9010sp14/extra_handouts/The_Digital_Forensics_Cyber_Exchange_Principle_-_2013-04-22.pdf> accessed 5 August 2025

43. Zozulia N, 'Electronic or Digital Evidence: Improving Amendments in Procedural Legislation' (*Ukrainian Law*, 8 May 2018) <https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva> accessed 10 August 2025. [in Ukrainian]

AUTHORS INFORMATION

Dinh The Hung
PhD (Law), Faculty of Law, Hanoi Open University, Vietnam
dthung4@hou.edu.vn
https://orcid.org/0009-0001-6700-1353
Corresponding author, solely responsible for the manuscript preparing.

Competing interests: No competing interests were disclosed.

Disclaimer: The author declares that the opinion and views expressed in this manuscript are free of any impact of any organizations.

RIGHTS AND PERMISSIONS

EDITORS

ABOUT THIS ARTICLE

Cite this article
Dinh TH, 'The Legal Framework of Electronic Evidence in Vietnamese Criminal Procedure: From the Budapest Convention to Domestic Legislation' (2025) 8(4) Access to Justice in Eastern Europe 301-39 <https://doi.org/10.33327/AJEE-18-8.4-a000142>

DOI: https://doi.org/10.33327/AJEE-18-8.4-a000142

Summary: 1. Introduction. – 2. Methodology and Research Methods. – 3. Theoretical Framework on Electronic Evidence. – *3.1. Concept of Electronic Evidence.* – *3.2. Fundamental Principles Governing Electronic Evidence*. – 4. European and Vietnamese Legal Frameworks for Electronic Evidence. – 4.*1. The European Regulatory Framework on Electronic Evidence. – 4.2. Shared Procedural Aspects of Investigating and Using Electronic Evidence. – 4.2.1. European Legal Framework. – 4.2.2. Vietnam's Framework on Investigation of Electronic Evidence*. – 5. Legal Gaps in Electronic Evidence Regulation in Vietnam Compared to the Budapest Convention. – 6. Conclusions.

Keywords: *Cybercrime, Electronic Evidence, Criminal Proceedings, Electronic Data, Legality of Electronic Evidence, Authenticity*

DETAILS FOR PUBLICATION

Date of submission: 10 Aug 2025
Date of acceptance: 08 Oct 2025
Publication: 18 Nov 2025
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 2 reports
Number of revision rounds: 2 rounds with major revisions

Technical tools were used in the editorial process:
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

AI DISCLOSURE STATEMENT

The author declares that no artificial intelligence tools were used in the writing, translation, or editing of this manuscript. The research and the content of the article represent the authors' own original work.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ПРАВОВЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ В'ЄТНАМУ: ВІД БУДАПЕШТСЬКОЇ КОНВЕНЦІЇ ДО НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА

Дінь Тхе Хунг

АНОТАЦІЯ

Вступ. *Електронні докази є критично важливою та делікатною темою, що розглядається в міжнародних документах щодо запобігання злочинам, зокрема в Будапештській конвенції та Договорі Організації Об'єднаних Націй про кіберзлочинність (Ханойська конвенція), що був нещодавно підписаний у Ханої, В'єтнам, у жовтні 2025 року. Правове регулювання електронних доказів стало однією з найбільш обговорюваних тем в академічних колах, особливо в дискусіях щодо інкорпорації зобов'язань за міжнародними договорами всередині країни.*

Кримінально-процесуальний кодекс В'єтнаму 2015 року зробив значний крок вперед, офіційно визнавши електронні дані як законну форму доказів, еквівалентну за доказовою силою іншим традиційним джерелам доказів. Оскільки електронні докази стають дедалі поширенішими в спектрі кримінальних правопорушень, це визнання є своєчасним. Однак, зі зростанням кіберзлочинності, чинне законодавство В'єтнаму виявляє значні обмеження порівняно з європейськими стандартами, особливо, що стосується концептуальної ясності, процесуальних гарантій збору та оцінки електронних доказів, захисту прав людини та забезпечення дотримання принципів змагальності.

Таким чином, ця стаття має на меті уточнити теоретичну та правову базу для електронних доказів згідно з європейськими стандартами, порівняти її з підходом В'єтнаму та визначити теоретичні та правові прогалини, які необхідно усунути, такі як: потреба в чіткіших визначеннях, сильніших процесуальних гарантіях збору та оцінки доказів, потреба в захисті прав людини та посиленні принципів змагальності.

Методи. *Для проведення порівняльного аналізу електронних доказів у рамках кримінально-процесуального права В'єтнаму та міжнародно-правового регулювання*

автор статті використовує методологію, що ґрунтуються на порівняльно-правових дослідженнях. Аналіз зосереджений на порівняльному вивченні міжнародних та національних правових положень щодо електронних доказів. Відповідно, автор широко використовує порівняльно-правові методи, зокрема нормативне порівняння та функціональне порівняння, для виявлення як подібностей, так і відмінностей між нормативними актами В'єтнаму щодо джерел доказів у кримінальному процесі та тими, що містяться в міжнародних документах та правових системах інших юрисдикцій.

Результати та висновки. *У статті було зроблено висновок, що правові положення В'єтнаму та їх практичне впровадження щодо електронних доказів повинні ґрунтуватися на міжнародному досвіді у кількох ключових аспектах: точна концептуалізація електронних доказів, розробка стандартизованих процедур їх збору та вдосконалення правових механізмів, що регулюють обов'язок подання доказів, судово-медичну експертизу та застосування спеціальних слідчих заходів. Такі реформи є важливими для забезпечення автентичності та законності електронних доказів, одночасно захищаючи права людини в рамках кримінального судочинства.*

Ключові слова: *кіберзлочинність, електронні докази, кримінальне провадження, електронні дані, законність електронних доказів, автентичність.*