

# Reading between the (binary) digits: the utilization of electronic evidence in criminal proceedings in Vietnam

By Nguyễn Thế Đức Tâm and Nguyễn Thái Khánh Bằng

## Introduction

In Vietnam, digital transformation is widely regarded as an innovative strategy for advancing industrialization and modernization.<sup>1</sup> However, alongside the benefits of integrating information technology into societal life comes an increase in the sophistication of criminal activities. Criminals exploit technological advancements not only to execute illegal acts but also to erase their digital footprints,<sup>2</sup> making it increasingly difficult for law enforcement agencies to investigate and prosecute these crimes effectively. With the growing prevalence of high-tech crimes,<sup>3</sup> the significance of electronic evidence in criminal investigations and prosecutions has become increasingly apparent.<sup>4</sup>

The 2015 Criminal Procedure Code marked a watershed moment by formally acknowledging “electronic data” as a new source of evidence,<sup>5</sup> equal in probative value to other forms of evidence in proving criminal conduct. This development bridged a longstanding gap between substantive and procedural laws, particularly in addressing crimes involving information and communication technologies. However, the incorporation of electronic evidence into the legal framework has also presented unique challenges.

This article explores the evolution and status of the Vietnamese legal framework on electronic evidence, highlighting its strengths and weaknesses from both theoretical and practical perspectives. In addition to the introduction and conclusion, the article consists of three main sections. First, the authors analyze the Vietnamese legal framework on electronic evidence, focusing on its conceptualization, admissibility, and procedural requirements under the 2015 Criminal Procedure Code. Next, the authors examine the practical use of electronic evidence in Vietnamese courts through an analysis of notable case laws, shedding light on its judicial application and the obstacles encountered. Finally, the authors offer recommendations to enhance the utilization of electronic evidence in criminal proceedings in Vietnam.

By resolving these issues, this article aims to contribute to the development of a robust legal framework for electronic evidence that aligns with international standards and addresses high-tech crimes effectively.

## Vietnamese legal framework on electronic evidence in criminal proceedings

The 2015 Criminal Procedure Code marked the inaugural legal document stipulating “electronic data” as a source of evidence in criminal cases. However, this was not the first instance where evidence from electronic data was mentioned. Before its codification in the 2015 Criminal Procedure Code, numerous debates arose regarding the use

---

<sup>1</sup> VNS. (2023). Vietnam Strives to Facilitate Digital Transformation. *Vietnam News*.

<https://vietnamnews.vn/economy/1549806/viet-nam-strives-to-facilitate-digital-transformation.html>

<sup>2</sup> An, T. X. T. (2018). Điều kiện để dữ liệu điện tử có thể sử dụng làm chứng cứ trong quá trình giải quyết vụ án hình sự [Conditions for Electronic Data to Be Used as Evidence in the Process of Resolving Criminal Cases]. <https://tkshcm.edu.vn/dieu-kien-de-du-lieu-dien-tu-co-the-su-dung-lam-chung-cu-trong-qua-trinh-giai-quyet-vu-an-hinh-su/>

<sup>3</sup> DT. (2024). Vietnam, U.S. Strengthen Cooperation in Combating High-Tech Crimes. *Public Security News*.

<https://en.cand.com.vn/public-security-forces/vietnam-u-s-strengthen-cooperation-in-combating-high-tech-crimes-i606231/>

<sup>4</sup> Thai, D. D. (2024). Proving Crimes With E-evidence Under Criminal Procedure Law. *Vietnam Law and Legal Forum*.

<https://vietnamlawmagazine.vn/proving-crimes-with-e-evidence-under-criminal-procedure-law-71418.html>

<sup>5</sup> Article 87(1)(c) of the 2015 Criminal Procedure Code. An unofficial translation is available at

<https://www.wipo.int/wipolex/en/text/585372>

of terms such as “electronic evidence,” and “digital traces,” since the preceding 2003 Criminal Procedure Code did not recognize “electronic data” as a source of evidence.<sup>6</sup>

Nonetheless, a joint circular issued in 2012 by the Ministry of Public Security, Ministry of National Defense, Ministry of Justice, Ministry of Information and Communications, the Supreme People’s Procuracy, and the Supreme People’s Court directed the application of the Criminal Code’s provisions concerning certain offenses in the information and communication technology sector, providing that “Electronic data can be considered as evidence”.<sup>7</sup> This circular exemplified the inconsistency between substantive law and procedural law in the criminal sector in Vietnam. While offenses in the information technology sector had been outlined in the 1999 Criminal Code, the subsequent 2003 Criminal Procedure Code did not address the source of evidence being electronic data – an essential source for proving the criminal conduct and the basis for handling this type of crime. Therefore, including “electronic data” as a source of evidence in the 2015 Criminal Procedure Code not only bridged the gap between substantive law and procedural law but also reflected an advancement of the Vietnamese legal system.<sup>8</sup>

## Concept of electronic evidence

The inaugural 1988 Criminal Procedure Code defined “evidence” as “factual elements, collected in accordance with the procedure outlined in this Code, that investigative agencies, the Procuracy, and the Courts utilize as the basis to ascertain the presence or absence of criminal conduct, the perpetrator, as well as other necessary circumstances for the accurate resolution of the case”.<sup>9</sup> The 2003 Criminal Procedure Code retained this definition without any modifications.<sup>10</sup> Unlike its predecessors, the 2015 Criminal Procedure Code introduced substantial alterations in defining the term “evidence” as “factual elements, collected in accordance with the procedure outlined in this Code, utilized as the basis to ascertain the presence or absence of criminal conduct, the perpetrator, and other pertinent circumstances in resolving the case”.<sup>11</sup>

Another advancement in the current Code is the separate articulation of “sources of evidence” as an independent article<sup>12</sup> rather than a minor clause within the Article on evidence.<sup>13</sup> According to the old Codes, evidence was identified through items listed in the statutory list. Although the 2003 Criminal Procedure Code provided more detailed specifications on sources of evidence as compared to the 1988 Criminal Procedure Code, these two Codes fundamentally categorized sources of evidence into four groups: (1) physical evidence, (2) testimonial statements, (3) expert conclusions, (4) records of investigation and hearings, and other documents or objects.<sup>14</sup> The list of sources of evidence from these two Codes did not mention digital environment terms such as “electronic,” “data,” and so forth.

<sup>6</sup> Phuoc, T. T. *Một số trao đổi về thu thập dữ liệu điện tử, phương tiện điện tử theo quy định của Bộ luật Tố tụng hình sự năm 2015* [Some Discussions on the Collection of Electronic Data and Electronic Devices According to the Provisions of the 2015 Criminal Procedure Code]. <http://dhannd.edu.vn/mot-so-trao-doi-ve-thu-thap-du-lieu-dien-tu-phuong-tien-dien-tu-theo-quy-dinh-cua-bo-luat-to-tung-hinh-su-nam-2015-a-2025>

<sup>7</sup> Article 5(1) of the Joint Circular no. 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC

<sup>8</sup> An, T. X. T. (2018). *Điều kiện để dữ liệu điện tử có thể sử dụng làm chứng cứ trong quá trình giải quyết vụ án hình sự* [Conditions for Electronic Data to Be Used as Evidence in the Process of Resolving Criminal Cases]. <https://tkshcm.edu.vn/dieu-kien-de-du-lieu-dien-tu-co-the-su-dung-lam-chung-cu-trong-qua-trinh-giai-quyet-vu-an-hinh-su/>

<sup>9</sup> Article 48(1) of the 1988 Criminal Procedure Code

<sup>10</sup> Article 64(1) of the 2003 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/184178>

<sup>11</sup> Article 86 of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>12</sup> Article 87 of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>13</sup> Article 48(2) of the 1988 Criminal Procedure Code

Article 64(2) of the 2003 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/184178>

<sup>14</sup> Article 48(2) of the 1988 Criminal Procedure Code

Article 64(2) of the 2003 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/184178>

Building upon provisions from the two previous Codes, the current Criminal Procedure Code has introduced modifications and expanded the list of sources of evidence, most notably adding “electronic data” as a source of evidence.<sup>15</sup> Hence, subsequent provisions in the current Code guide this new source of evidence. Some specific provisions directly referring to “electronic data” include the collection of evidence,<sup>16</sup> the definition of “electronic data”,<sup>17</sup> the collection of electronic devices and electronic data,<sup>18</sup> the seizure of electronic devices and electronic data,<sup>19</sup> and the preservation of electronic data.<sup>20</sup> Besides these provisions, other regulations concerning searches, examinations, etc., refer to “electronic data” as the object of these measures and activities.

The 2015 Criminal Procedure Code defines “electronic data” as “symbols, writings, numbers, images, sounds, or similar forms created, stored, transmitted, or received by electronic means”.<sup>21</sup> This definition is appraised for its compatibility with the concept of “data” in the 2005 Law on Electronic Transactions,<sup>22</sup> leading to the view that, theoretically, electronic data had been legally recognized and valued as a source of evidence since 2006.<sup>23</sup> However, it was not until the enactment of the 2015 Criminal Procedure Code that electronic data was formalized as one of the sources of evidence.

The recent 2023 Law on Electronic Transactions does not change the concept of “data” because it still includes symbols, letters, numbers, images, sounds, and the like.<sup>24</sup> However, the 2023 Law on Electronic Transactions elaborates that electronic data is data created, processed, and stored by electronic means.<sup>25</sup> We observe that the concepts of electronic data in the 2015 Criminal Procedure Code and the 2023 Law on Electronic Transactions have similar meanings despite some different wordings. Specifically, “transmitted or received by electronic means” (in the 2015 Criminal Procedure Code) can be understood as “processed by electronic means” (in the 2023 Law on Electronic Transactions).

While the 2015 Criminal Procedure Code does not explicitly mention “electronic evidence,” Vietnamese legal scholars continue to employ this term.<sup>26</sup> However, there are diverging views on the concept of electronic evidence. According to the Deputy Director of the Police Department for High-Tech Crime Prevention (Ministry of Public Security), electronic evidence can be understood as “evidence preserved in electronic signals in computers or other devices with digital memory related to criminal cases”.<sup>27</sup> Others argue that “electronic evidence” should refer to evidence, as stipulated in Article 86 of the 2015 Criminal Procedure Code, which is intimately related to or directly

<sup>15</sup> Article 87(1)(c) of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>16</sup> Article 88 of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>17</sup> Article 99 of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>18</sup> Article 107 of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>19</sup> Article 196 of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>20</sup> Article 199 of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>21</sup> Article 99 of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>22</sup> Article 4(5) of the 2005 Law on Electronic Transactions. An unofficial translation is available at [https://www.wto.org/english/thewto\\_e/acc\\_e/vnm\\_e/wtaccvnm43\\_leg\\_5.pdf](https://www.wto.org/english/thewto_e/acc_e/vnm_e/wtaccvnm43_leg_5.pdf)

<sup>23</sup> Dien, N. V. (2019). *Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015* [Electronic Evidence in the 2015 Criminal Procedure Code]. <https://moj.gov.vn/qt/tintuc/Pages/nguyen-cuu-trao-doi.aspx?ItemID=2455>

<sup>24</sup> Article 3(6) of the 2023 Law on Electronic Transactions

<sup>25</sup> Article 3(7) of the 2023 Law on Electronic Transactions

<sup>26</sup> Dien, N. V. (2019). *Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015* [Electronic Evidence in the 2015 Criminal Procedure Code]. <https://moj.gov.vn/qt/tintuc/Pages/nguyen-cuu-trao-doi.aspx?ItemID=2455>

Hanh, N. D. (2019). Dữ liệu điện tử và chứng cứ điện tử [Electronic Data and Electronic Evidence]. *Journal of Procuratory Science*, Special Issue 1, pp. 37-42. <https://vjol.info.vn/index.php/tks/article/view/46336/37588>

<sup>27</sup> Dien, N. V. (2019). *Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015* [Electronic Evidence in the 2015 Criminal Procedure Code]. <https://moj.gov.vn/qt/tintuc/Pages/nguyen-cuu-trao-doi.aspx?ItemID=2455>

formed from the source of electronic data.<sup>28</sup> Thus, “electronic evidence” must possess the attributes of evidence being objective, relevant, and lawful.

Although the 2015 Criminal Procedure Code has affirmed “electronic data” as a source of evidence, there remains much debate around using the term “electronic evidence” as this concept has yet to be formalized. These viewpoints primarily bifurcate into two prominent opinions: (1) considering “electronic evidence” as a subcategory of evidence;<sup>29</sup> (2) considering “electronic evidence” as a separate type of evidence with a distinct source of evidence compared to traditional evidence.<sup>30</sup>

Electronic evidence depends on electronic data because it can only be derived from electronic data. While resolving criminal cases, proceeding-conducting agencies cannot seek electronic evidence elsewhere apart from electronic data.<sup>31</sup> Hence, electronic evidence also bears the attributes of electronic data. When compared with traditional sources of evidence, electronic data possesses two prominent features:

First, electronic data is invisible to the naked eye and requires appropriate (compatible) hardware and software to convert electronic data into information perceptible to human senses. In contrast, traditional sources of evidence are easily identifiable as they exist in tangible forms that human senses can perceive.

Second, electronic data can be added, copied, edited, deleted, and restored. Electronic data exists in a digital environment. Thus, it is easily alterable and replicable multiple times. In contrast, traditional sources of evidence are unique and difficult to change.

Therefore, according to the authors, legislators should consider electronic data as an independent source of evidence due to its distinctive nature compared to traditional sources.

### Admissibility of electronic evidence

Not all electronic data can serve as a source for electronic evidence; such data must fulfill certain criteria concerning evidentiary value. The 2015 Criminal Procedure Code specifies the evidentiary value of electronic data as follows: “The evidentiary value of electronic data is determined based on the methods of initiation, storage, or transmission of electronic data, the methods ensuring and maintaining the integrity of electronic data, the identification of the creator, and other appropriate factors”.<sup>32</sup>

To be recognized as evidence, electronic data not only needs to possess all attributes of evidence (objectivity, relevance, and lawfulness) but also relies on the methods of creation, storage, transmission, and maintenance of data integrity.<sup>33</sup> Hence, electronic data should meet the following requirements to be admissible.

First, objectivity. The data must be factual, exist objectively, have a clear origin, remain unaltered, and be found and stored on computers, mobile phones, emails, USB drives, online accounts, or servers provided by internet service providers.

Second, relevance. The data must be related to criminal conduct, perpetrators, victims, consequences, etc., and be employed to ascertain pertinent circumstances in resolving the case.

<sup>28</sup> Hanh, N. D. (2019). Dữ liệu điện tử và chứng cứ điện tử [Electronic Data and Electronic Evidence]. *Journal of Procuratory Science*, Special Issue 1, pp. 37-42. <https://vjol.info.vn/index.php/tks/article/view/46336/37588>

<sup>29</sup> Hanh, N. D. (2019). Dữ liệu điện tử và chứng cứ điện tử [Electronic Data and Electronic Evidence]. *Journal of Procuratory Science*, Special Issue 1, pp. 37-42. <https://vjol.info.vn/index.php/tks/article/view/46336/37588>

<sup>30</sup> Dien, N. V. (2019). Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015 [Electronic Evidence in the 2015 Criminal Procedure Code]. <https://moj.gov.vn/qt/tintuc/Pages/nghien-cuu-trao-doi.aspx?ItemID=2455>

<sup>31</sup> Hanh, N. D. (2019). Dữ liệu điện tử và chứng cứ điện tử [Electronic Data and Electronic Evidence]. *Journal of Procuratory Science*, Special Issue 1, pp. 37-42. <https://vjol.info.vn/index.php/tks/article/view/46336/37588>

<sup>32</sup> Article 99(3) of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>33</sup> Tuyet, N. T. (2023). Một số khó khăn, vướng mắc khi chuyển hóa dữ liệu điện tử thành chứng cứ chứng minh trong các vụ án hình sự [Some Difficulties and Problems When Converting Electronic Data Into Evidence in Criminal Cases]. <https://vkstphcm.gov.vn/mot-so-kho-khan-vuong-mac-khi-chuyen-hoa-du-lieu-dien-tu-thanh-chung-cu-chung-minh-trong-cac-vu-an-hinh-su-825.html>

Third, lawfulness. The data must be collected in accordance with the regulations of the 2015 Criminal Procedure Code. Otherwise, it holds no legal value and cannot be used as the basis for resolving criminal cases,<sup>34</sup> even if the data is factual and bears traces of illegal activities. The electronic data cannot exist independently but is always associated with at least one electronic device and, thus, can be added, copied, edited, deleted, restored, and transmitted. Therefore, ensuring the legality of electronic data requires technical knowledge and skills.

Fourth, authenticity. When collecting electronic data, it is imperative to identify the person to whom the data belongs. Based on the methods of creation, electronic data is categorized into the following types: electronic data automatically generated by computers, electronic data created by the offender or the victim, and electronic data generated by authorized agencies.<sup>35</sup>

Fifth, integrity. The electronic data must preserve accuracy and consistency from creation to collection. Hence, the electronic data must remain unedited, unchanged, and free from data distortion.<sup>36</sup>

## Procedures relating to electronic data

The process of detecting, investigating, collecting, preserving, and handling electronic data has not been delineated in the 2015 Criminal Procedure Code. Aside from being mentioned in general regulations regarding evidence collection, examination, scene investigation, and evidence preservation, electronic data only has two specific legal provisions concerning the collection of electronic devices and data<sup>37</sup> and the seizure of electronic devices and data.<sup>38</sup>

Unfortunately, these two legal provisions contradict each other as the legislators seem to unify the acts of “collecting” and “seizing” electronic devices. Articles 107 and 196 of the 2015 Criminal Procedure Code have several overlapping points concerning the measures of collecting electronic devices and data, yet the titles of these articles are different. Article 107, which stipulates the collection of electronic devices and data, encompasses Article 196 concerning the seizure of electronic devices and data.<sup>39</sup> Specifically, Article 107 stipulates the collection of electronic devices and data, but its first clause states that “Electronic devices must be seized timely and fully ...”.<sup>40</sup>

The 2015 Criminal Procedure Code does not define electronic devices; however, according to Article 99, electronic devices refer to devices that create, store, transmit, or receive electronic data and serve as a repository for electronic data. Thus, the term “collecting electronic data” should be used because electronic data is a source of evidence, while electronic devices are merely items where the electronic data is collected.

Furthermore, Article 107 of the 2015 Criminal Procedure Code contains two significant shortcomings. First, Article 107(1) states, “If electronic data storing means cannot be seized, competent procedural authorities shall copy electronic data into another electronic medium for storage of evidence.” However, it does not specify the duration for storing the data or any procedure, requirements, or means for storing electronic data during backup. Article 107(1) requires electronic devices and data to be preserved like physical sources of evidence. Still, the inherent attributes of electronic devices and data, significantly different from traditional sources of evidence, necessitate distinct regulations for preserving this source of evidence. Second, Article 107(3) stipulates, “Upon receiving

<sup>34</sup> Article 87(2) of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>35</sup> Hanh, N. D. (2019). Dữ liệu điện tử và chứng cứ điện tử [Electronic Data and Electronic Evidence]. *Journal of Procuratory Science*, Special Issue 1, pp. 37-42. <https://vjol.info.vn/index.php/tks/article/view/46336/37588>

<sup>36</sup> Hieu, B. H. (2021). Bàn về một số khía cạnh của dữ liệu điện tử trong tố tụng hình sự [Discussion on Some Aspects of Electronic Data in Criminal Proceedings]. <https://baovephapluat.vn/cai-cach-tu-phap/dien-dan/ban-ve-mot-so-khia-can-qua-du-lieu-dien-tu-trong-to-tung-hinh-su-116824.html>

<sup>37</sup> Article 107 of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>38</sup> Article 196 of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>

<sup>39</sup> Minh, T. N., & Cuong, D. M. (2023). Hoàn thiện pháp luật về các biện pháp điều tra theo quy định của Bộ luật Tố tụng hình sự năm 2015 [Completing the Legal Framework on Investigative Measures According to the Provisions of the 2015 Criminal Procedure Code]. <https://kiemsat.vn/hoan-thien-phap-luat-ve-cac-bien-phap-dieu-tra-theo-quy-dinh-cua-bo-luat-to-tung-hinh-su-nam-2015-65859.html>

<sup>40</sup> Article 107(1) of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>



competent authorities' requisition for expert examination, responsible entities shall restore, search, and examine electronic data." It only mentions data restoration in case of necessary expert assessment for the collected electronic data. Still, it does not address scenarios where data restoration is performed to discover other electronic data for collection.<sup>41</sup>

The 2015 Criminal Procedure Code does not provide explicit provisions regarding the procedure for collecting electronic data, and no implementation guidance has been issued for this matter,<sup>42</sup> leading to many inadequacies in the process of collecting electronic data. In practice, prosecutors and investigators apply the provisions in Joint Circular No. 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC to address some issues regarding the procedure for collecting electronic data. Specifically, the preservation of electronic devices should comply with Article 5 of this Circular, such as not placing these devices near magnets, radio waves, or excessively hot or humid places; some devices need to be preserved in specialized bags to avoid data alteration or remote intervention after seizure.

### The use of electronic evidence in criminal proceedings in Vietnam

Electronic data was incorporated as a source of evidence to resolve the conflict between substantive law and procedural law.<sup>43</sup> While substantive law has provisions regarding cybercrimes, the stipulations from procedural law proved insufficient for substantiating these types of crimes. However, the use of electronic data as evidence in criminal proceedings over the past few years has demonstrated that this source of evidence is pivotal in proving high-tech crimes and substantiating conventional crimes. The authors choose three notable cases that exhibit the utilization of electronic data in criminal proceedings.

#### Case No. 1

The case pertains to an individual named "Vuong Quoc Th..." who was charged with obstructing the operations of computer networks, telecommunications networks, and electronic devices. Between 14 March 2021 and 16 June 2021, he launched unauthorized DDoS attacks 88 times on 23 websites belonging to different organizations. One of the targeted websites was Quy Nhon University's official site, which faced disruptions and became inaccessible due to his attacks. In Judgment No. 21/2022/HSST dated 13 May 2022, the People's Court of Binh Dinh Province fined Vuong Quoc Th 30 million VND (around 1,300 USD).<sup>44</sup>

In this case, electronic data was automatically collected through access logs. Accordingly, the attacks were identified when the websites recorded an unusually high number of events. The judgment underscores the legal consequences of cyberattacks and the efforts of Vietnamese authorities to prosecute such offenses.

#### Case No. 2

The case involves individuals named "Lau Mi L..." and "Sung Mi G..." who were charged with organizing the illegal entry of Chinese nationals into Vietnam. On 20 July 2022, they were transporting Chinese nationals when they were intercepted and asked to stop by police. Upon interrogation, they admitted to illegally transporting ten Chinese nationals into Vietnam. However, Lau Mi L did not admit that he directly participated in receiving ten Chinese nationals from the border.

The Prosecutor relied on electronic data, particularly six video files collected from Lau Mi L's mobile phone, to prove his criminal conduct. Therefore, in Judgment No. 22/2023/HS-ST dated 27 April 2023, the People's Court of Ha Giang

<sup>41</sup> Tung, P. C. (2022). *Hoàn thiện quy định về dữ liệu điện tử trong tố tụng hình sự* [Completing Regulations on Electronic Data in Criminal Proceedings]. <https://kiemsat.vn/hoan-thien-quy-dinh-ve-du-lieu-dien-tu-trong-to-tung-hinh-su-64101.html>

<sup>42</sup> Nam, N. T. (2024). Bàn về chứng cứ có nguồn là dữ liệu điện tử trong pháp luật tố tụng hình sự [Discussion on Evidence Derived from Electronic Data in Criminal Procedure Law]. *Journal of Democracy and Law*, Issue 6(1), pp. 47-50. <https://danchuphapluat.vn/ban-ve-chung-cu-co-nguon-la-du-lieu-dien-tu-trong-phap-luat-to-tung-hinh-su>

<sup>43</sup> An, T. X. T. (2018). *Điều kiện để dữ liệu điện tử có thể sử dụng làm chứng cứ trong quá trình giải quyết vụ án hình sự* [Conditions for Electronic Data to Be Used as Evidence in the Process of Resolving Criminal Cases]. <https://tkshcm.edu.vn/dieu-kien-de-du-lieu-dien-tu-co-the-su-dung-lam-chung-cu-trong-qua-trinh-giai-quyet-vu-an-hinh-su/>

<sup>44</sup> Judgment No. 21/2022/HSST of the People's Court of Binh Dinh Province. The full text of the judgment (in Vietnamese) is available at [https://congbobanan.toaan.gov.vn/5ta944850t1cvn/BA\\_Vuong\\_Quoc\\_Thinh\\_D287.pdf](https://congbobanan.toaan.gov.vn/5ta944850t1cvn/BA_Vuong_Quoc_Thinh_D287.pdf)

Province sentenced Lau Mi L to six years and Sung Mi G to five years in prison.<sup>45</sup> This case exemplifies the utilization of electronic data, not only in high-tech crimes but also in conventional crimes.

### Case No. 3

The case pertains to an individual named “Le Thi Hoai T...” and her accomplices, who were involved in illegal activities related to bank accounts. In 2021, a Vietnamese living abroad (referred to as “V”) requested Le Thi Hoai T to collect the bank accounts of several people in Vietnam for illicit purposes. Through her accomplices and other persons, Le Thi Hoai T collected details of 88 bank accounts belonging to 58 individuals.

During the investigation, authorities discovered that Le Thi Hoai T had exchanged numerous messages with specific accounts on Telegram and Facebook. Consequently, the authorities required her to personally log into her social media accounts. She was instructed to capture and print all relevant message content, with each page duly signed by her for verification. However, Telegram and Facebook did not provide user information and data, resulting in insufficient evidence to establish that the recipient accounts belonged to V.

In Judgment No. 39/2022/HS-ST dated 7 June 2022, the People’s Court of Nam Dinh Province sentenced Le Thi Hoai T to five months in prison.<sup>46</sup> This case underscores the challenges faced by investigative agencies in collecting electronic evidence, particularly in cases involving cross-border data transfers and data stored on foreign social networking platforms.

### Recommendations

To enhance the utilization of electronic evidence in criminal proceedings in Vietnam, the authors propose the following suggestions:

First, we recommend codifying the concept of “electronic evidence” within the Criminal Procedure Code and consolidating Articles 107 and 196 of the 2015 Criminal Procedure Code into a single provision titled “Collection of Electronic Data and Seizure of Electronic Devices”.<sup>47</sup>

Second, we suggest improving legal provisions regarding the collection, preservation, evaluation, and utilization of electronic data due to its distinctive features compared to traditional sources of evidence.<sup>48</sup> Various technical guidelines, notably the INTERPOL Guidelines for Digital Forensics First Responders: Best practices for search and seizure of electronic and digital evidence,<sup>49</sup> along with ISO/IEC 27037:2012 (Guidelines for the Identification, Collection, Acquisition, and Preservation of Digital Evidence),<sup>50</sup> could come in handy in advancing regulations pertaining to electronic data.

Third, we recommend supplementing legal provisions on the participation of relevant experts during the seizure of electronic devices to ensure the authenticity and integrity of the electronic data.<sup>51</sup>

<sup>45</sup> Judgment No. 22/2023/HS-ST of the People’s Court of Ha Giang Province. The full text of the judgment (in Vietnamese) is available at [https://congbobanan.toaan.gov.vn/Sta1192726t1cvn/Ban\\_an\\_ma\\_hoa\\_LG.pdf](https://congbobanan.toaan.gov.vn/Sta1192726t1cvn/Ban_an_ma_hoa_LG.pdf)

<sup>46</sup> Judgment No. 39/2022/HS-ST of the People’s Court of Nam Dinh Province. The full text of the judgment (in Vietnamese) is available at [https://congbobanan.toaan.gov.vn/Sta980915t1cvn/ban\\_an\\_dang.pdf](https://congbobanan.toaan.gov.vn/Sta980915t1cvn/ban_an_dang.pdf)

<sup>47</sup> Tung, P. C. (2022). *Hoàn thiện quy định về dữ liệu điện tử trong tố tụng hình sự* [Completing Regulations on Electronic Data in Criminal Proceedings]. <https://kiemsat.vn/hoan-thien-quy-dinh-ve-du-lieu-dien-tu-trong-to-tung-hinh-su-64101.html>

<sup>48</sup> Hanh, N. D. (2019). Dữ liệu điện tử và chứng cứ điện tử [Electronic Data and Electronic Evidence]. *Journal of Procuratory Science*, Special Issue 1, pp. 37-42. <https://vjol.info.vn/index.php/tns/article/view/46336/37588>

<sup>49</sup> INTERPOL. (2021). *INTERPOL Guidelines for Digital Forensics First Responders: Best practices for search and seizure of electronic and digital evidence*. [https://www.interpol.int/content/download/16243/file/Guidelines\\_to\\_Digital\\_Forensics\\_First\\_Responders\\_V7.pdf](https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf)

<sup>50</sup> In Vietnam, TCVN ISO/IEC 27037:2019 (published by Decision No. 2940/QĐ-BKHCN of the Minister of Science and Technology) is equivalent to ISO/IEC 27037:2012

<sup>51</sup> Tung, P. C. (2022). *Hoàn thiện quy định về dữ liệu điện tử trong tố tụng hình sự* [Completing Regulations on Electronic Data in Criminal Proceedings]. <https://kiemsat.vn/hoan-thien-quy-dinh-ve-du-lieu-dien-tu-trong-to-tung-hinh-su-64101.html>

Fourth, we suggest incorporating legal provisions on the utilization of personal data as a source of evidence in alignment with Governmental Decree No. 13/2023/ND-CP<sup>52</sup> on personal data protection. These provisions will serve as the basis to clarify the responsibilities of agencies and organizations in providing personal data as evidence in criminal proceedings.

Fifth, we recommend enhancing the information technology capabilities of proceeding-conducting persons, particularly through specialized training programs on electronic data, as well as ensuring the provision of adequate infrastructure for the examination and evaluation of electronic evidence.<sup>53</sup> The implementation of appropriate procedures for collecting, preserving, and processing electronic data heavily relies on the competence and expertise of the individuals directly responsible for these tasks.

Sixth, we suggest strengthening international cooperation, particularly information sharing, regarding electronic data in investigating, prosecuting, and adjudicating criminal cases.<sup>54</sup> Through such international collaboration, Vietnamese proceeding-conducting agencies should effectively handle electronic data, which could significantly contribute to the effective resolution of criminal cases.

## Conclusion

The utilization of electronic evidence in the investigation, prosecution, and adjudication of recent criminal cases has underscored its critical role in preventing and detecting high-tech crimes in Vietnam. Despite the recognition of “electronic data” as a source of evidence under the 2015 Criminal Procedure Code,<sup>55</sup> several shortcomings persist in both the legal framework and its practical application. These include the absence of a well-defined concept of electronic evidence, the lack of distinction between the collection and seizure of electronic devices, and the absence of practical guidance on handling electronic evidence. Furthermore, the interplay between personal data and electronic evidence remains unaddressed.

To resolve these issues, the authors propose six recommendations aimed at enhancing the Vietnamese legal framework for electronic evidence, thereby ensuring its admissibility. Strengthening the legal and practical mechanisms for electronic evidence will not only advance the Vietnamese judicial system but also improve its capacity to address high-tech crimes effectively. By bridging current gaps and incorporating international best practices, Vietnam can establish a robust foundation for the utilization of electronic evidence in criminal proceedings.

## Funding

This research is funded by the University of Economics and Law, Vietnam National University Ho Chi Minh City, Ho Chi Minh City, Vietnam.

---

<sup>52</sup> An unofficial translation is available at [https://eurochamvn.org/wp-content/uploads/2023/02/Decree-13-2023-PDPD\\_EN\\_clean.pdf](https://eurochamvn.org/wp-content/uploads/2023/02/Decree-13-2023-PDPD_EN_clean.pdf)

<sup>53</sup> Dien, N. V. (2019). *Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015 [Electronic Evidence in the 2015 Criminal Procedure Code]*. <https://moj.gov.vn/qt/tintuc/Pages/ngghien-cuu-trao-doi.aspx?ItemID=2455>

Hanh, N. D. (2019). Dữ liệu điện tử và chứng cứ điện tử [Electronic Data and Electronic Evidence]. *Journal of Procuratory Science*, Special Issue 1, pp. 37-42. <https://vjol.info.vn/index.php/tks/article/view/46336/37588>

<sup>54</sup> Hanh, N. D. (2019). Dữ liệu điện tử và chứng cứ điện tử [Electronic Data and Electronic Evidence]. *Journal of Procuratory Science*, Special Issue 1, pp. 37-42. <https://vjol.info.vn/index.php/tks/article/view/46336/37588>

<sup>55</sup> Article 87(1)(c) of the 2015 Criminal Procedure Code. An unofficial translation is available at <https://www.wipo.int/wipolex/en/text/585372>



**Nguyễn Thế Đức Tâm**

Lecturer, Faculty of Law

University of Economics and Law, Ho Chi Minh City, Vietnam

Vietnam National University, Ho Chi Minh City, Vietnam

[tamntd@uel.edu.vn](mailto:tamntd@uel.edu.vn)

ORCID iD: 0000-0003-3469-5464

**Nguyễn Thái Khánh Bằng**

LL.B. Candidate

University of Economics and Law, Ho Chi Minh City, Vietnam

Vietnam National University, Ho Chi Minh City, Vietnam

[bangntk21502@st.uel.edu.vn](mailto:bangntk21502@st.uel.edu.vn)

ORCID iD: 0009-0000-8023-0604