**УДК 343.1**

Фам Ньы Хан
Академия народной безопасности
Кафедра фундаментальной и профессиональной науки
Вьетнам, Ханой
nik.fam.89@mail.ru
Pham Nhu Han
People's Security Academy
Department of fundamental and professional science
Vietnam, Hanoi

# УГОЛОВНОЕ СУДОПРОИЗВОДСТВО ВО ВЬЕТНАМЕ, КАКИЕ ТИПЫ ЭЛЕКТРОННЫХ ДАННЫХ ЯВЛЯЮТСЯ ДОКАЗАТЕЛЬСТВАМИ?

**Аннотация:** в соответствии с Уголовно-процессуальным кодексом 2015 года (далее - УПК 2015) доказательствами считаются электронные данные. Одним из значительных изменений, внесенных в УПК 2015 г., является включение «электронных данных» в качестве нового источника доказательств в главу о доказательствах. Это совершенно новая проблема, которая теперь официально признана правовой системой в качестве источника доказательств, который может быть использован для разрешения уголовных дел. В данной статье рассматриваются некоторые аспекты проблемы доказательств в виде электронных данных, а также сбор и применение доказательств в виде электронных данных в уголовных процессах.

**Ключевые слова:** преступление, расследование, доказательство, электронные данные, уголовный процесс, уголовное дело.

# VIETNAM'S CRIMINAL PROCEEDINGS , WHAT KINDS OF ELECTRONIC DATA IS CONSIDERED EVIDENCE?

**Abstract:** Evidence is defined as electronic data under the Criminal Procedure Code 2015 (further - CPrC 2015). One of the significant changes made to the CPrC in 2015 is the inclusion of «electronic data» as a new source of evidence in the chapter on evidence. This is a brand-new problem that is now formally acknowledged by the legal system as a source of evidence that may be utilized to resolve criminal cases. The article that follows examines a few aspects of the problem of evidence as electronic data, as well as the gathering and application of evidence as electronic data in criminal trials.

**Keywords:** crime, investigation, evidence, electronic data, criminal process, criminal case.

### 1.What types of electronic data are accepted as proof?

Evidence is a way to establish criminals and offenders and is used to ascertain other factors required for the proper resolution of criminal cases, therefore it is implied that it goes hand in hand with the effort to reduce crime. Evidence serves as both a tool for establishing the objective truth of the matter and a record of how that truth was discovered.

In criminal procedures, the investigating, prosecuting, and adjudicating authorities are only able to ascertain the facts of the case via evidence, which provides a foundation for deciding whether a crime has been committed. If a crime has been committed, and if it has, whether to pursue the appropriate legal action. In order to correctly resolve a criminal case, evidence is a way to support certain facts and phenomena while simultaneously rejecting and refuting events and phenomena that did not really take place or unimportant.

The CPrC 2015 specifies in Article 87 that one of the sources of evidence is: electronic data, demonstrating that, in the present, the source of evidence is electronic data, which plays an increasingly essential part in the process of proving the case. We must first define what constitutes evidence in order to establish the idea of evidence as electronic data [2, c.45]. Article 86 of the CPrC 2015 states that evidence is what is

actual, gathered in accordance with the order and methods specified by this Code, and utilized as a foundation for deciding whether or not a violation has been committed, the offender, and other crucial details that may affect how the case is resolved.

Thus, independent of its source, evidence has fundamental characteristics and features - this does not preclude electronic evidence. However, defining this idea is a little more difficult and confusing, since proof, according to the conventional perspective, must be tangible information that individuals can control, keep, and seize. However, this is not the case with electronic evidence.

Electronic data differs from the conventional paradigm even in the way that evidence is formed. Dialectical materialism holds that every crime committed in reality is detectable and verifiable by people. In accordance with the dialectical materialism theory, which holds that everything has the ability to reflect, human actions, including criminal ones, leave a trace in the real world. The physical evidence of a crime can take the form of fingerprints left at the scene, tools used in the crime, or the offender's handwriting [3, c.80]. It can also be stored in the memory of the victim or another person. This is not the case with electronic evidence because the formation (reflection), existence, and information-carrying mechanisms of electronic evidence are distinct from those of traditional evidence. Electronic evidence is also understood differently.

Dr. Tran Van Hoa, deputy director of the high-tech crime prevention police department, mentioned that «electronic evidence are evidence stored in the form of electronic signals in computers or in devices with digital memory related to criminal cases» [4, c.69]. The International Criminal Police Organization (Interpol) defines electronic evidence as information and data that have significance for pharmacological investigations stored or transferred by a computer, computer network, or any other digital electronic device. Establishing, seizing, and restoring electronic evidence must be done quickly yet cautiously; it calls for great precision and meticulousness.

Electronic data is defined as symbols, words, numbers, pictures, sounds, or similar forms generated, preserved, transmitted, or received by electronic means, according to Article 99 of the CrPC 2015. Electronic data is gathered from electronic sources such as transmission lines, computer networks, telecommunications networks, and electronic vehicles. Similar to this, the 2015 Civil Procedure Code established in Article 95 that there must be a content linked to identifying the source of any electronic data message proof. As proof that electronic data is present in the CrPC 2015, it may be claimed that electronic data messages include identical information.

Thus, there is evidence that information linked to criminal cases is stored as electronic signals in computers or other devices with digital memory. Three qualities must be present in this information: objectivity, relevancy, and legality [5, c.207]. The following conditions must be met before «electronic data» may be used as evidence to support a claim and establish its veracity: the data must be accurate and objective, and it must have been lawfully gathered for the purposes of the claim and the evidence.

Furthermore, since «electronic data» is kept in computers and digital devices, it must fulfill three additional unique criteria in order to constitute legal evidence, including: «objectivity» «: «as is» - there is no outside intervention in the data to be changed or deleted, and it must be «verifiable.»

In terms of application. Today, no person, organization, or company can separate computers and computer networks in the age of information technology and communication growth. As a result, high-tech user’s illegal activities are becoming more popular, and their crimes are becoming more complex. As a result, recognizing evidence from electronic data is a step forward in our country's criminal procedures by exploring actions to show the crime process is more reliant on electronic evidence.

**2. Gathering and using electronic data as evidence in criminal proceedings**

Collecting evidence in a criminal case is the process through which investigators and legislators locate, recognize, seize, and preserve evidence using

acceptable procedures, tactics, and means. Not in violation of the law. Thus, the following actions are included in the content of evidence collecting activities: detection, recognition, seizure, and preservation of evidence.

According to Article 107 of the CPrC 2015, electronic media and data collection must be done in a timely and thorough manner, correctly reflect the circumstances, and be sealed right away after seizure. in accordance with the Law's rules. If the electronic data storage device cannot be seized, the agency authorized to handle the case must back up the relevant electronic data to the device, keep it as evidence, and simultaneously ask the agency to handle the case. Related businesses, agencies, and people must answer to the law for storing and maintaining the integrity of electronic data that has been backed up by qualified procedure-conducting organizations [6].

When electronic data is collected, blocked, or backed up from electronic means, computer networks, telecommunications networks, or transmission lines, the proper authority must make a record and put it in the file's case before hand.

Individual and organizations will have to restore, search, and evaluate electronic data when they get the decision to ask the competent authority to assess how to run the proceedings. Electronic data can only be recovered, searched, and evaluated on a copy; the results of the recovery, search, and evaluation must be turned to read, hear, or see.

Evidence shows that electronic data differs from other evidence in both the substance that it contains and the manner of identification, therefore this activity was carried out efficiently and had the intended impact in addition to adhering to the rules. Apply the basic guidelines for gathering, storing, preserving, restoring, analyzing, searching, and evaluating evidence to the letter while gathering, storing, restoring, analyzing, searching, and inspecting evidence. More has to be understood about topics like: not changing data saved on computers or in digital devices; The gathering and recovery of electronic evidence must be done by qualified specialists when they have access to original material that has been stored [7, c.106].

Additionally, the proper procedure must be followed while capturing data; must use verifiable, globally acknowledged hardware and software; must gather evidence to support the data recovery procedure; To achieve the same outcomes as those put out in court, it may be necessary to repeat the procedure.

Two criminal procedural standards must be adhered to while gathering electronic vehicles and data:

The legality must first be gathered and kept in compliance with the law: according to the criminal process for a search, a seizure, a record, photography, a drawing, and the preservation of electronic data to guarantee the legal value of electronic data and the requirements for using electronic data as evidence.

Second, authenticity is ensured prior to, during, and after data seizure, and data stored onto electronic vehicles during data seizure cannot be influenced by outside forces. updated data. There are enough reasons to support the claim that electronic data and evidence are valid, objective, true, and undamaged.

Therefore, the judicial agency's efforts such as gathering, maintaining, restoring, decoding, analysis, search, and evil evaluation are necessary for electronic data to have evidentiary value similar to «conventional records» For criminal proceedings, the proper sequence and processes must be followed while searching for, recording, sealing, seizing, and conserving electronic data evidence (computer hard drive, telephone phone Minh, USB, memory card, optical disc, camera, camera, email ...). When giving tangible evidence to data recovery professionals for copying, follow legal procedures to open seals and seals [8].

Legal specialists conduct a variety of electronic data evaluation tasks, such as copying, retrieving, decoding, analyzing, and searching for data held on storage devices used as tangible evidence.

The outcomes of the expert solicitation will provide a solid foundation for bringing the case and the accused to justice.

Electronic data is used in the process of verifying, analyzing, and utilising evidence. The subject offers electronic evidence to support itself in matters where the

value of the data evidence before the Court must be established: particularly when stopping, copying, restoring, decoding, analyzing, and searching don't alter the data.

The evidence significance of electronic data is recognized by Vietnamese law at the moment. However, in the contemporary environment, practically all transactions take place online, making it even more important to complete and enforce the proper execution of the law's electronic evidence requirements.

**Список литературы:**

1. Bộ luật Tố tụng hình sự nước Cộng hòa xã hội chủ nghĩa Việt Nam, số: 101/2015/QH13 ngày 27.11.2015 /Уголовно-процессуальный кодекс Социалистической Республики Вьетнам №101/2015/QH13 27 ноября 2015 г. URL: https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Bo-luat-to-tung-hinh-su-2015-296884.aspx (Дата обращения: 01.12.2022)

2. Ngô Vĩnh Bạch Dương. «Nghĩa vụ chứng minh trong tố tụng». Tạp chí Nghiên cứu pháp luật. Số 07 (287) Tháng 4/2015. /Нго Винь Бак Зыонг. Бремя доказывания в уголовном процессе // Журнал Исследование права, 2015. – №7 (287). – с.45.

3. Нгуен Тхи Нгок Иен. Показания свидетеля и потерпевшего в уголовно-процессуальном праве Социа-листической Республики Вьетнам // Актуальные вопро-сы науки: Материалы XXXVI Международной научно-практической конференции в 09 февраля 2018 г. – М.: Издательство «Спутник+», 2018. – с.80.

4. Trần Văn Hòa , Vấn đề dấu vết điện tử và chứng cứ trong Bộ luật Tố tụng Hình sự, Tạp chí Khoa học và Chiến lược, số chuyên đề 12/2014, Viện Chiến lược và Khoa học Bộ Công an, Hà Nội./ Чан Ван Хоа , Проблемы электронных следов и доказательств в Уголовно-процессуальном кодексе, Журнал науки и стратегии, выпуск 12 2014 г., с.69.

5. Trần Minh Quân. «Sử dụng chứng cứ trong hỏi cung bị can – Những vấn đề lý luận, thực tiễn». Luận án tiến sĩ Luật học - Hà Nội, 2011. /Чан Минь Куан.

Использование доказательств в ходе допроса обвиняемого-теории и практики: дисс.…канд. юрид. наук. – Ханой, 2011. с. 207.

6. Lưu Hưng - VKSND huyện Tiên Yên. Bài viết một số quy định về chứng cứ trong Bộ luật tố tụng hình sự năm 2015. [Электронный ресурс] // URL: http://www.vksquangninh.gov.vn/tin-ho-t-d-ng-xd-nganh/xay-d-ng-nganh/2094-bai-vi-t-m-t-s-quy-d-nh-v-ch-ng-c-trong-b-lu-t-t-t-ng-hinh-s-nam-2015 (Дата обращения: 29.11.2022)

7. Nguyễn Nhật Lệ. «Nguồn chứng cứ trong Pháp luật Việt Nam». Luận văn thạc sĩ luật học, Khoa Luật, Đại học Quốc gia Hà Nội. /Нгуен Ньат Ле. Источники доказательств в уголовном процессе Вьетнам: дис… юрид. м-ра.– Ханой, 2014. – с.106.

8. Thu thập bảo quản chứng cứ là dữ liệu điện tử và những khó khăn vướng mắc. [Электронный ресурс] // URL: http://vkscantho.vn/vkscantho/index.php/news/Trao-doi-nghiep-vu/Thu-thap-bao-quan-chung-cu-la-du-lieu-dien-tu-va-nhung-kho-khan-vuong-mac-3464/ (Дата обращения: 30.11.2022)