УДК 343.1

Хо Зуй Тхань
Академия национальной безопасности Вьетнама
г. Ханой
Ho Duy Thanh
People's Security Academy Vietnam,
Hanoi city

Хуа Нгок Ту
Академия национальной безопасности Вьетнама
г. Ханой
Hua Ngoc Tu
People's Security Academy Vietnam
Hanoi city

НЕСКОЛЬКО СООБРАЖЕНИЙ ОБ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВАХ ВО ВЬЕТНАМЕ
A FEW CONSIDERATIONS ABOUT ELECTRONIC EVIDENCE IN VIETNAM

Аннотация: Вьетнам и другие страны мира живут в эпоху информационных технологий. Электронная связь стала подходящим средством ведения бизнеса, и очевидно, что внутренние и международные транзакции через Интернет стали популярными, что позволяет людям вести бизнес в любое время, в любом месте и без границ. Быстрое развитие информационных технологий оказало влияние на все области и способы общения, а также на оценку доказательств в суде, поскольку электронное общение является неизбежной тенденцией. В настоящее время вьетнамское законодательство признает доказательную значимость передачи данных.

Abstract: Vietnam and other countries around the world are living in an era of information technology. Electronic communication has become an appropriate means of doing business, and it is clear that domestic and foreign transactions via the internet have become popular, allowing people to do business anytime, anywhere, and without borders. With the rapid advancement of information technology, it has influenced all fields and modes of communication, and this has had an impact on the evaluation of evidence in court, since electronic communication is an unavoidable trend. Currently, Vietnamese law acknowledges the evidentiary significance of data transmissions.

Ключевые слова: электроника, информация, технология, доказательства, суд, внешнеторговая сделка.

Keywords: Electronic, information, technology, evidence, court, foreign transaction.

1. Theoretical concerns about electronic evidence

According to the 2006 Law on Electronic Transactions, “data is information in the form of symbols, letters, digits, images, sounds, or the like, and this regulation reveals that electronic data is regarded a source of evidence in electronic transactions” [1].

In order for “electronic data” to be considered as evidence or called electronic evidence, electronic data must be collected in the order and procedures prescribed by the criminal procedure law 2015 on evidences [2]. However, the current law does not have a legal concept of “electronic evidence” but can be understood as any authentic information stored or transmitted in digital form that the parties can use in court [3, c.29].

From the perspective of electronic evidence, it is possible to generalize that “electronic evidence” refers to all information and data collected from electronic devices such as computers and information storage devices, as well as data from computer networks, mobile phones, digital cameras, and the Internet.

1.1. Types of Electronic Evidence

An electronic document or information that contains a variety of data, such as content transmission data, location of transmission and arrival, time, date, and so on. Each piece of data corresponds to a distinct sort of electronic evidence.

Based on the electronic evidence framework.

Electronic signatures can take various forms, including words, letters, numbers, symbols, sounds, and more, and can be attached or combined with a data message to confirm the person's signature and consent to the message's content [4, c.17].

A digital signature is an electronic signature created by transforming a data message using an asymmetric cryptosystem. The public key of the signer and the person obtaining the original data message can be correctly identified [5, c.18]. This definition applies to all electronic documents and data messages with an electronic signature verified by the public key listed in the original data message.

Crytopraphy encrypts personal information transmitted through public channels, allowing only the intended recipients to read and process it [6]. The code is kept secret and can only be decrypted with an electronic key.

Electronic symbols represent an individual's identity and are attached to electronic messages, documents, or processes used to authenticate, sign, or approve electronic data. Encryption is a method for protecting sensitive data.

Electronic data messages (E-Messages) refer to information generated, sent, received, and stored electronically from legal documents (e.g., petitions, evidences, and procedural documents).

Electronic archives (electronic documents) are data messages created by agencies, organizations, or individuals, or digitized from other information carriers. These documents can be interpreted as information, data, symbols, or other written expressions in digital form.

Based on electronic proof sources.

Man-made electronic evidence includes papers, tables, emails, and other data authored by humans and preserved in electronic memory.

Computers produce electronic evidence by analyzing incoming data using predetermined algorithms. Examples include payment schedules, online registration forms, and transaction histories.

Based on the storage capacity.

Communication electronic data refers to online discussions, text messages, audio, and photographs that are not stored.

Electronic data in the information and communications system refers to data generated, transferred, received, saved, or processed on computer systems or similar devices and kept.

1.2. Characteristics of Electronic Evidence

Electronic evidence has a variety of qualities that distinguish it from conventional evidence, including:

Electronic evidence is not always evident to the human eye. It may be located via instructions, in areas only available to new specialists, or in areas that need specific instruments.

Second, it is easy to hide or disappear: Some devices and certain conditions of computer memory (data containing evidence) may be overwritten (or changed) by the normal function or operation of the device. This could be due to a sudden stop of the system, a new information installation that overlaps old information due to a lack of memory space, or environmental factors such as high temperature and humidity causing damage to the storage memory [7, c.76].

Electronic devices' memory state may be modified or destroyed during routine operation, such as when updating or storing data, or when the operating system automatically updates the data.

Fourth, electronic data may be replicated endlessly and yet be deemed evidence since it retains all the original qualities.

2. Vietnam's present electronic evidence legislation

2.1. Validation of Electronic Evidence

The Internet has transformed the way people communicate and conduct business, and it has become the foundation of electronic evidence worldwide, challenging the traditional rules of evidence

that require the presentation of original documents. As a result, the authenticity of electronic data collected as evidence must be clear, not lost or hidden, and not infringe on individuals' or organizations' copyright, privacy, or security and defense.

In the People's Court of Binh Duong province's Judgment No. 20/2019/KDTM-PT dated August 12, 2019 on the dispute of the goods purchase and sale contract, the Court did not accept electronic evidence. Specifically, the defendant of the Goods Production Company Limited, to whom the plaintiff of the Company B delivered defective goods and poor quality paint, was required to export abroad to be compensated and

2.2. Electronic evidence collecting.

Electronic data mining can be done offline on a computer, smartphone, or other electronic device, or on a communications network, because electronic data can be easily searched instead of hard documents that need to be checked manually. Electronic data can appear on many drives and digital files, and even if deleted, there may be a command to restore them, and if you want to destroy a data set, you must destroy all hard drives where the data is stored [8].

Furthermore, the variety of electronic evidence allows for data mining of sources of evidence such as electronic documents, document files, databases, audio and visual files, websites, and computer programs. Malware such as viruses, Trojans, and spyware can also be considered acceptable.

However, some problems in collecting electronic evidence are the recovery of destroyed data, the assessment of the legality of data, or the encryption of electronic data... in the assessment of evidence in case of protection of disadvantaged parties such as consumers, workers, or low-income people... However, this issue has not been discussed by the law on the cost of data recovery and evidence verification because this cost is usually borne by the obligor.

In addition, there are many legal issues related to security, politics, and personal privacy in the process of exploiting and searching for electronic data. For example, the litigant may ask the Court to consider conducting a data search, but it is not always necessary, and there is no law obligated to delete the data that has been copied during the data search, increasing the risk of violating an individual's privacy.

Furthermore, the geographical scope affects the search because electronic data is not limited in terms of space and time with transitional and transboundary nature. As a result, retrieving electronic data is not feasible when it comes to a country's political and security diplomacy.

2.3. Preservation of electronic evidence.

Because of the rapid rise of e-governance, agencies and organizations are opening their doors to adopt various e-governance rules and periodic records to regulate and manage sectors that use electronic means.

In law, electronic evidence is increasingly being used in the trial stage, where the judge is required to make a decision. This is due to the fact that paper documents have traditionally been kept at the expense of money, space, and time, which has resulted in the proliferation of methods for storing and creating electronic documents. Unlike paper documents, most electronic documents can maintain their integrity and accuracy.

However, electronic data may be altered without leaving any trace, it may be fabricated or falsified, or other types of electronic evidence such as CD/VCD, hard disk/memory card data may appear hardware or software errors, or Web site data, communication of social networks, emails, SMS/MMS messages, and computer-generated data pose unique problems and challenges for conformity validation. All of these concerns highlight a fundamental problem when information is stored as electronic [9].

2.4. Use electronic evidence.

Electronic evidence is easy to collect, store, and preserve because it can be collected online and stored in personal data, or if it is programmed by a computer, the individual cannot change the data in it except for the administrator of the system, and sometimes the data is stored

However, information security concerns a fundamental issue when information stored as electronic data may not be exploited, accurately collecting all electronic data, leading to the integrity

and completeness of electronic evidence is not guaranteed. This affects the authenticity of types of electronic evidence that currently exist, and relevant legal documents do not have standards related to electronic evidence, leading to the use of electronic evidence that is objective.

Establishing the legal value of electronic evidences, such as electronic documents and signatures, is a procedural difficulty in data processing and procedural regulations. This difficulty is due to a lack of appropriate regulations and legal guidelines on electronic data processing procedures. Additionally, the Judge and Prosecutor may not have a thorough understanding of the situation.

Second, the collection, use, and preservation of electronic evidence face difficulties in the process of copying evidence, which may cause data loss, data modification, or the fact that electronic evidence is related to state secrets, privacy, fine customs and traditions, etc., resulting in electronic evidence not ensuring integrity. Furthermore, proving the originator of electronic evidence is a major challenge in the cyber environment, because cyberspace is both tangible

In order to facilitate Vietnam's active participation in the fourth industrial revolution, the government has set out a policy to improve the legal system in general and the law on electronic evidence in particular. The fourth industrial revolution is affecting most fields, including health, culture, education, the economy, and financial-banking, necessitating a rethinking of economic and social management, as well as the creation and improvement of institutions.

Список литературы:

1. Luật Giao dịch điện tử nước Cộng hoà xã hội chủ nghĩa Việt Nam Số: 51/2005/QH11 ngày 29 tháng 11 năm 2005/ Законе об электронных сделках Социалистической Республики Вьетнам №51/2005/QH11, 29 ноября 2005 года. URL: https://thuvienphapluat.vn/van-ban/Thuong-mai/Luat-Giao-dich-dien-tu-2005-51-2005-QH11-6922.aspx (Дата обращения: 10.6.2024)

2. 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: 10.6.2024)

6. Nghi định 130/2018/NĐ-CP của Chính Phủ về quy định chi tiết thi hành luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số ngày 27.9.2018 / Постановление Правительства № 130/2018/ND-CP о подробных правилах реализации закона об электронных транзакциях, касающихся цифровых подписей и служб аутентификации цифровых подписей от 27 сентября 2018 г., URL: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-130-2018-ND-CP-huong-dan-Luat-Giao-dich-dien-tu-ve-chu-ky-so-358259.aspx (Дата обращения: 10.6.2024)

4. Nguyễn Văn Điền, Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015, Tạp chí Tư pháp số 6/2019, tr.17./ Нгуен Ван Диен, Электронные доказательства в Уголовно-процессуальном кодексе 2015 г., Судебный журнал № 6/2019, с.17.

5. Bùi Hồng Hiếu, Bàn về một số khía cạnh của dữ liệu điện tử trong tố tụng hình sự, Tạp chí Bảo vệ pháp luật số 17/2021, tr.18

3. Nguyễn Thành Minh Chánh, Pháp luật về chứng cứ điện tử tại Việt Nam. Tạp chí Nghiên cứu Lập pháp số 4/2022, tr.29

7. Nguyễn Đức Hạnh, Dữ liệu điện tử và chứng cứ điện tử, Tạp chí Khoa học kiểm sát, Số chuyên đề tháng 1/2019, tr. 76/ Нгуен Дык Хань, Электронные данные и электронные доказательства, Журнал прокуратуры, выпуск за январь 2019 г., с.76

8. Chứng cứ điện tử trong tố tụng dân sự theo pháp luật Việt Nam và một số quốc gia trên thế giới [электронный ресурс] URL: https://danchuphapluat.vn/chung-cu-dien-tu-trong-to-tung-dan-su-theo-phap-luat-viet-nam-va-mot-so-quoc-gia-tren-the-gioi#:~:text=Ch%E1%BB%A9ng%20c%E1%BB%A9%20%C4%91i%E1%BB%87n%20t%E1%BB%AD%20c%E1%BA%A7n,c%C3%A1ch%20kh%C3%A1ch%20quan%2C%20li%C3%AAn%20quan (Дата обращения: 09.6.2024)

9. Hironao Kaneko, Electronic evidence in civil procedure in Japan, Digital Evidence and Electronic Signature Law Review, Vol 5, [электронный ресурс] URL: https://journals.sas.ac.uk/deeslr/issue/view/305. (Дата обращения: 08.6.2024)