УДК 343.1

До Нгок Тан
Академия народной безопасности Вьетнама
Кафедра расследования безопасности
Вьетнам, Ханой
Khanhmon2014@gmail.com
Do Ngoc Tan
People's Security Academy
Department of Security Investigation
Vietnam, Hanoi

МЕТОДЫ СБОРА, ПРЕОБРАЗОВАНИЯ И ПРИМЕНЕНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В ДЕЛАХ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ

Аннотация: одним из новых источников доказательств, определенных в Уголовно-процессуальном кодексе 2015 года Вьетнама, являются электронные данные. Результаты предыдущих расследований, судебных преследований и судебных разбирательств по уголовным делам показали важность установления правдивости и объективности электронных данных для содействия нынешней борьбе с преступностью. В результате необходимо уважать сбор, использование, преобразование и использование этого потока доказательств для установления дел.

Ключевые слова: электронные данные, доказательства, Уголовно-процессуальный кодекс, преступление, дело, компьютерная сеть.

METHODS FOR GATHERING, CONVERTING, AND APPLYING ELECTRONIC EVIDENCE IN CASES INVOLVING HIGH-TECH USE

Annotation: one of the new sources of evidence defined in the CrPC of 2015 is electronic data. The outcomes of previous investigations, prosecutions, and trials of

criminal cases have shown the importance of establishing the truth and objectivity of electronic data in contributing to the present battle against crime. As a result, the collection, exploitation, transformation, and use of this stream of evidence to establish cases must be respected.

Key words: Electronic data, evidence, CrPC, crime, cases, computer network.

High-tech crime in Vietnam

High-tech crime has only been present in Vietnam for little than a decade, but it has grown significantly owing to the rapid growth of information technology. Currently, the situation of high-tech crime is complicated, with developments occurring in many fields such as economy, culture - society, security - defence, causing serious economic damage, disrupting the activities of agencies and organizations, the administration of the Government, limiting the effectiveness of the application of information technology for socio-economic development, particularly threatening security - defence, social order, and safety. After being found and dealt with, high-tech criminal organizations and lines have swiftly altered new tactics and tricks to cope with functional forces. High-tech criminals' activities in Vietnam are becoming more infused with the characteristics of organized crime and multinational crime [1].

There are two major groupings of issues that have emerged from the practice of treating high-tech crime cases:

- The first group: The object of the crime is data integrity, the stable operation of computer networks, telecommunications networks, internet networks, digital devices of agencies, organizations, and individuals (as specified in Articles 286, 287, 288, 293 of the Penal Code 2015), such as spreading viruses, disrupting computer network activities...[2]

- The second group: The object of the crime is most of the objects protected by the penal code, which are: the Fatherland's independence, sovereignty, unity, and territorial integrity; the political regime; the economic regime; culture, defence, and

security; social order and safety; the organization's legitimate rights and interests; citizens' life, health, honour, dignity, freedom, property, and other legitimate rights and interests...

The 2015 Penal code specifies specific actions of high-tech crimes in 08 articles (from Article 285 to Article 294 (abrogating Article 292); The following actions are classified as crimes in seven groups: (1) Deliberately disseminating computer programmes that impair computer networks, telecommunications networks, and electronic devices (abbreviated as computer networks) and infect 50 or more electronic devices; (2) Arbitrarily deleting, destroying, or modifying software, electronic data, or unlawfully stopping computer network data transfer, or conducting other actions that impede or disturb computer network activity (paralysing, disrupting, or disrupting computer network functioning); (3) Posting information contrary to the provisions of law on computer networks; trading, exchanging, donating, repairing, altering, or publicising the lawful private information of agencies, organisations, and individuals on the computer network without the permission of the owner of such information; (4) Deliberately bypassing warnings, access codes, firewalls, using the administrative rights of others, or other methods of illegally intruding into other people's computer network (5) Making use of a computer network to carry out one of the following acts: Using information about agencies, organisations, and individuals' accounts and bank cards to appropriate property or pay for goods and services; creating, storing, trading, using, and circulating fake bank cards; illegally accessing the accounts of agencies, organisations, and individuals in order to appropriate property; e-commerce fraud...; (6) Illegally producing, trading, exchanging, and donating tools, equipment, and software with computer network attack features; (7) Illegally using radio frequencies exclusively for emergency, safety, search and rescue, rescue, national defense and security purposes...

According to crime statistics from December 1, 2009 to November 31, 2019, high-tech crimes primarily focus on the act of appropriating property (Article 290 of

the penal code), accounting for 61%, and illegally using computer network information, telecommunications networks, such as for information trading, reducing the reputation of individuals and organisations (Article 288 of the penal code).

In terms of implementation strategy: 45% of crimes are perpetrated by accomplices and organisations, mostly among people aged 18 to 30; the victims of high-tech crimes are mostly individuals...

High-tech criminals often utilise the following criminal tricks: Stealing, buying, and selling credit card information; using credit card information to pay for services and purchase goods; illegally accessing telecommunications networks to connect and set up unauthorised signal transceiver stations to steal telecommunications fees; hacking emails of individuals and businesses and appropriating property using victims' information theft, appropriation, and control of information of companies, persons, and organisations in order to threaten, blackmail, disrupt, or discredit...; establishment of online trading websites, fraudulently appropriating property, or fraudulently appropriating property in the form of multi-level sales getting acquainted through chat and then cheating, appropriating property, performing depraved acts, prostitution, human trafficking; spreading depraved culture, prostitution, drug trafficking, buying and selling women and children; organising gambling and gambling; using computer networks, telecommunications networks, and the internet to put information online to carry out activities against the people's government, terrorist activities…[3, c. 17]

Some limitations and shortcomings in the fight against High-tech crime in Vietnam

There are still certain deficiencies, restrictions, and challenges in the prevention and battle of high-tech crime in Vietnam, as follows:

To begin with, there are no specific regulations on the necessary processes for handling electronic evidences; there are no regulations and processes for capturing, preserving, and recovering electronic data in order to protect the safety and integrity

of data and preserve the value of electronic evidences; and there are no specific regulations on the preservation and use of this specific type of evidence [4, c. 72].

The Criminal Procedure code (futher - CrPC) [5] states that secret electronic data collection is a special procedural investigation measure related to human rights and civil rights (Article 223), but there is no detailed guidance document on this issue for law enforcement agencies to implement uniformly and in accordance with legal regulations.

Second, the victim and the offender often do not know each other; the victim frequently does not know when he or she has been appropriated property, violated personal information... some are hurt for personal reasons, so he or she does not want to report the crime to the relevant authorities. Victims and family members are often scattered throughout the country, making it difficult to gather testimony, compare statistics, and hold confrontations. The majority of the victims utilised the internet and telecommunications networks, but lacked the requisite knowledge of information technology, as well as a grasp of the tactics and tricks of high-tech criminals, as well as the necessary steps and instruments to maintain the confidentiality and protection of personal information.

Third, electronic data is vulnerable to disruption, modification, and destruction. In many cases, collecting electronic evidence is extremely difficult because criminals use advanced technology to conceal information; when there is a risk of disclosure, they frequently shut down websites or delete related information, and destroy electronic devices, so data recovery takes a long time and is not always collected and recovered. Electronic data contained in devices is quite different in shape and kind; there are devices of very tiny size, intended as watches, buttons, pens, key hangers, plug chargers, etc., making it difficult for untrained investigators and procurators to discover, resulting in non-seize. Some subjects choose the form of online data storage through the servers of online storage businesses such as Google Drive, OneDrive, Dropbox, Box...[6, c. 8] These servers are located abroad or at the tenant's location; thus, to collect data, there must be coordination with the service provider through

international cooperation channels; however, this activity is very difficult due to differences in legal regulations between countries, language barriers, and service providers frequently changing.

Fourth, with the present growth of security information sharing forums, high-tech criminals may now easily infiltrate and damage websites. Meanwhile, many websites in Vietnam are not effectively protected, relying on application software with several weaknesses, allowing high-tech criminals to access and attack.

Fifth, in order to gather, retrieve, decode, analyse, and evaluate electronic data, specialised equipment and software must be continually replaced, bought, or updated in accordance with new equipment (such as smartphone analysis software). These specialised equipment and software are sometimes quite expensive; presently, the cost of inquiry has not been fulfilled.

Sixth, the force of investigators, procurators, and judges who had sufficient training in information technology encountered several challenges in identifying and managing high-tech crimes. They also struggled with the utilisation of electronic evidence. However, the procurators lack basic training in high-tech criminals supervision skills, such as how to seize and preserve electronic means and data, how to analyse, inspect, and convert electronic evidence, how to use electronic evidence and judicial outcomes to prove crimes, how to build indictments, how to exercise the right to prosecute, how to investigate and oversee trials at the court, and how to inspect, seize, preserve, copy, analyse, and build electronic data reports in accordance with the guidelines set forth by the International Computer Evidence Organisation (futher - IOCE) in March 2000 and the CrPC of 2015's provisions on electronic evidence.

Seventh, high-tech crimes are non-traditional, transnational crimes committed in cyberspace. However, Vietnam has only signed mutual legal assistance agreements with 21 other countries, and many Vietnamese legal provisions conflict with foreign laws. As a result, it is challenging to implement international cooperation and judicial mandates to address high-tech crimes.

The aforementioned obstacles, flaws, and restrictions should be addressed as soon as possible in order to contribute to increasing the efficiency of Vietnam's battle against high-tech crime in the future.

Regulations on electronic evidences, measures to collect, store, transform and use evidences in criminal cases

According to Article 99 of the CrPC 2015, electronic data refers to symbols, characters, numbers, pictures, sounds, or similar information that is generated, stored, transferred, or received using electronic methods. Electronic data will be gathered from electronic devices, computer networks, telecommunications networks, transmission lines, and other electronic sources. For electronic data to be considered legitimate evidence, it must adhere to certain criteria such as the manner of creation, storage, transmission, and the measures taken to preserve the integrity of the data.

The CrPC 2015 specifies many sources of evidence, including as exhibits, testimony, presentations, electronic data, and the outcomes of judicial entrustment and international collaboration. The text refers to Article 87.

Therefore, the CrPC 2015 acknowledged electronic data, outcomes of court entrustment, and international collaboration as valid forms of evidence. Presently, the CrPC 2015 has 09 provisions that govern the acquisition and handling of electronic data as evidence.

Firstly, concerning the confiscation and safeguarding of electronic devices and electronic data

Article 88 of the CrPC 2015 outlines the specific sequence and processes for conducting searches, seizing items, creating records, sealing, and conserving various types of evidence, including computer hard drives, cellphones, USB sticks, memory cards, optical discs, video cameras, cameras, and emails.

In order to make their argument more clear, procedure-conducting agencies must ask other agencies, groups, and people for electronic data and to provide any relevant facts.

According to Article 192 of the CrPC 2015, searches of people, places of employment, accommodations, and methods may yield electronic data.

The capable process-conducting agency obtains a search warrant (Clause 1, Article 113 of the 2015 CrPC) to enable the seizure of electronic data.

According to Clause 2, Article 35 of the 2015 CrPC, search warrants issued by investigative agencies need approval by procuracies of the same level before being executed. To oversee the search, the procurator has to be present (Article 193 of the CrPC of 2015). As per Articles 133, 178, and 193 of the 2015 CrPC, every search case has to be documented in the case file.

Information technology specialists may be invited to join in the seizure of electronic devices and data. Electronic data that is not able to be recorded on media must be backed up to storage media and confiscated in the same way as tangible evidence. Article 196 of the CrPC 2015 states that you must take the peripheral equipment that is connected to electronic devices [7, c. 27].

Procedure-conducting authorities should be accountable for maintaining each step of the proceedings; electronic methods and confiscated electronic data must be retained intact (Articles 107 and 199 of the 2015 CrPC); and must be preserved intact (Article 90 of the 2015 CrPC).

A data storage media or an electronic replica of the data must be presented with electronic evidence when it is presented in court. The competent procedure-conducting agency will have the authority to decide whether to request expertise for the recovery, search, and examination of electronic data; this will only be done on copies, and the results will need to be transformed into a format that can be read, heard, or seen.

Second, conditions for electronic data to be used as evidence in criminal cases

The following are the fundamental rules to follow while gathering, maintaining, copying, analysing, and transforming electronic data into electronic evidence: Do not alter the data saved on computers or digital devices. To gather and retrieve electronic evidence, a skilled expert must have access to original material

stored on computers or digital devices. Data recording (copying) must adhere to internationally recognised and verified processes, as well as the usage of equipment and software. The integrity of electronic data held in the computer must be safeguarded, as must the objectivity, status quo, and verifiability of evidence in court. Must be able to demonstrate the data recovery method, locate evidence, and, if required, repeat the process and arrive at the same outcome as given at trial. In certain circumstances, access to original equipment is required to restore evidence.

Electronic evidence may be manipulated or destroyed by inappropriate opening, checking, and saving, as well as by viruses found in computers and USB sticks. To recover, search, gather, store, and examine this form of evidence, it is important to utilise virus-free computers and specialised software mandated by law or recognised by the world [8, c. 81].

Electronic data must fulfil the qualities of evidence, which include objectivity, legality, and relevance, in order to become an evidence source.

+ Objectivity: This data is true, existing objectively, has a clear origin, is not fabricated or distorted, and has been discovered and stored on computers, mobile phones, emails, USBs, online accounts, internet service provider servers...

+ Legality: Evidence must be collected in accordance with the provisions of the CRPC 2015. While electronic data is real, bearing the traces of crimes, it has no legal value and cannot be used as a basis for resolving criminal cases if not collected in the order and procedures prescribed by the CrPC 2015.

In the process of seeking and seizing exhibits, backing up data, intercepting online, archiving, retrieving, analysing, searching, and examining data, the collecting procedure must employ legally recognised technology.

Electronic devices such as computers, servers, tablets, media devices, USB sticks, CD/DVD discs, routers, wifi, smart phones, household electronics (some devices have data storage, can be connected to the network, accessed, and controlled remotely), GPS global positioning system, and so on must be specifically recorded in

the minutes (not recorded in general such as: a sealed sack, carton box), must be sealed and maintained in accordance with regulations (ensure ON/OFF specification).

Data recovery specialists employ data recovery technology and software, such as write-protection devices (Read Only), to copy data and then only use this copy to recover, analyse, search for data, and convert it to a readable, audible, and visual format. Data recovery must be performed only on copies (not on originals), so that the originals are not destroyed; this procedure may be repeated before the Court. The originals must be kept in compliance with the rules.

+ Relevance: The information acquired is connected to the offence, the perpetrator, the victim, the repercussions, and so on, and is utilised to determine the facts of the case. The principle and technology of electronic trace formation, spatial information, data formation time (logfile, IP, metadata, hash function), storage address, information content (origin and content of emails, chats, messages, attack technology, victims, damage...), access cookies... all reflect relevance.

The minutes of the search, sealing, and recording of testimonies and statements must include three data attributes. Subjects must sign any printed copies on paper, pictures, CDs/VCDs recording electronic data, and other documents relating to the case, verifying the content, form, and provenance. This is also a requirement for converting and establishing evidences collected during the reconnaissance phase, as well as converting important electronic data into papers, pens, and exhibits that may be utilised as evidence.

Third, on the conversion of electronic data into evidence

Electronic data recovery, search, and inspection with the goal of turning electronic data into evidence that can be read, heard, or seen (Article 107 of the CrPC 2015).

The following electronic data conversion technique is obtained:

Make minutes, take testimonies on the act of creating this data, the origin of the data; self-declaration of the data and evidence found, sign for confirmation on each sheet of documents, photos, optical discs, printed from the subject's computer as a

pencil, and sign for confirmation on each sheet of documents, photos, optical discs, printed from the subject's computer as a pencil. To maximize the legal value of electronic data used as evidence, it must be supplemented with additional relevant evidence such as exhibits and witness testimony. Use the “Survey Conclusion” findings on electronic data saved in electronic devices [9].

Regarding judicial assessment: Judicial assessment is the use of knowledge, means, scientific and technical methods by judicial examiners at the request of procedure-conducting agencies for the resolution of cases.

Articles 99 and 107 of the CrPC of 2015 specify electronic data inspection as a new rule. Judicial Assessors execute electronic data assessment operations utilising suitable equipment and technology to copy, recover, decode, analyse, and search for data held in exhibits as storage devices.

The outcomes of recuperation, search, and evaluation must be translated into a format that can be read, heard, or seen.

When the competent procedure-conducting agency decides to seek expertise, the person or organisation responsible for expertise will apply and enforce the CrPC's principles, specifically: The assessment (recovery, search, and examination of electronic data) is only carried out on a copy of the data; the assessment is based on the principles specified in Clause 3, Article 99 of the CrPC of 2015, specifically: “The evidential value of electronic data is determined based on the method of generating, storing, or transmitting electronic data; the method of ensuring the integrity of electronic data; the method of ensuring the integrity of electronic data; the method of ensuring the integrity of electronic data”

The process of recovering, locating, collecting, analysing, and evaluating existing data in digital memory must always be coordinated with investigators in order to determine which electronic data is valid for use as evidence in the case; must make a record of the content of recovered and analysed electronic data; and must be enclosed with testimonies and testimonies of offenders and witnesses of such information.

Fourth, on the use of the results of judicial entrustment and international cooperation as a source of evidence

Because criminals in the field of information technology and telecommunications networks are transnational, involving both domestic and foreign subjects, the implementation of judicial mandates and international cooperation to collect documents and evidence proving crimes in the field of information technology and telecommunications networks is critical.

The results of judicial entrustment and international cooperation are a source of evidence, according to Article 87 of the 2015 CrPC this supplement is compatible with the current development process of science - technology and meets the needs of international cooperation in solving cases in the field of information technology and telecommunications networks.

One of the new sources of evidence in the 2015 CrPC is the outcomes of judicial entrustment and other international collaboration. Article 103 of the CrPC (2015) states that: “The results of judicial entrustment and other international cooperation provided by competent foreign agencies can be considered evidence if it is consistent with the evidence of the case”.

Article 494 of the 2015 CrPC expressly states that “documents and objects collected by competent foreign agencies under judicial mandate of competent Vietnamese agencies or documents and objects sent to Vietnam by competent foreign agencies to entrust criminal prosecution may be considered evidence” If these papers and items meet the criteria outlined in Article 89 of this Code, they may be deemed tangible evidence.

One of the solutions suggested to improve the efficiency of preventing and combatting this sort of crime is international collaboration in the sphere of information technology and telecommunications networks. As a result, the 2015 CrPC specifies that the outcomes of judicial entrustment and international cooperation serve as the foundation for promoting international cooperation between Vietnam and other countries, as well as between functional forces in the field of

information technology, telecommunications networks, and specialised agencies of countries in the region and the United Nations.

Список литературы:

1. Tội phạm sử dụng công nghệ cao tăng 42%, [электронный ресурс], URL: https://cebid.vn/toi-pham-su-dung-cong-nghe-cao-tang-42/ (Дата обращения: 30.01.2024)

2. Bộ luật hình sự nước Cộng hòa xã hội chủ nghĩa Việt Nam, số: 100/2015/QH13 ngày 27.11.2015 /Уголовный кодекс Социалистической Республики Вьетнам №100/2015/QH13, 27 ноября 2015 года. URL: https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Bo-luat-hinh-su-2015-296661.aspx (Дата обращения: 30.01.2024)

3. Nguyễn Văn Điền (2019), Chứng cứ điện tử trong Bộ luật tố tụng hình sự 2015, Tạp chí Tư pháp, số 06, 2019, tr.17.

4. Đào Phan Nhật Minh, Nguyễn Đức Trí, Phạm Thành Lâm, Phan Thanh Minh, Đào Thái Bình Dương, Hoàn thiện pháp luật về thu thập dữ liệu điện tử trong tố tụng hình sự Việt Nam, Tạp chí Việt Nam hội nhập, số 298, 2023, tr.72.

5. 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: 03.02.2024)

6. Nguyễn Đức Hạnh, Cao Cẩm Thi, Quy định về chứng cứ điện tử trong pháp luật tố tụng và luật giao dịch điện tử, Tạp chí Kiểm sát, số 03, 2023, tr.08.

7. Nguyễn Thành Minh Chánh, Pháp luật về chứng cứ điện tử tại Việt Nam, Tạp chí Toà án nhân dân, số 04, 2021, tr.27.

8. Nguyễn Hòa Bình, Những nội dung mới trong Bộ luật Tố tụng Hình sự năm 2015 Sách chuyên khảo, Nhà xuất bản Chính trị Quốc gia, 2016, tr.81.

9. Điều chỉnh nhiệm vụ, quyền hạn thu thập tài liệu, chứng cứ của tòa án, [электронный ресурс], URL: https://quochoi.vn/tintuc/Pages/tin-hoat-dong-cua-quoc-hoi.aspx?ItemID=80618 (Дата обращения: 30.01.2024).