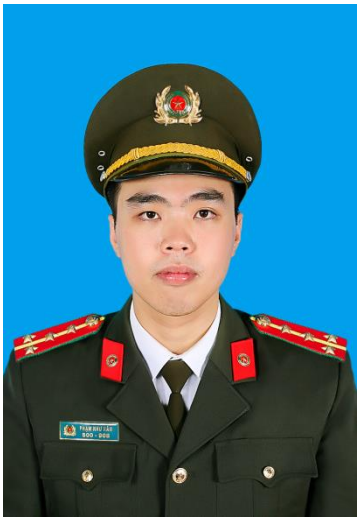
УДК 343.1



Фам Ньы Хан
Волгоградская академия МВД Российской Федерации
Факультет Адъюнктуры
Россия, Волгоград
nik.fam.89@mail.ru
Pham Nhu Han
Volgograd Academy of the Ministry of Internal Affairs of Russia.
Faculty of Postgraduate Studies
Russia, Volgograd

Фам Куок Чинь
Академия национальной безопасности Вьетнама
Кафедра профессиональных основ
Вьетнам, Ханой
chinhphamquoc.designer1986@gmail.com
Pham Quoc Chinh
People's Security Academy
Department of Professional Fundamentals
Vietnam, Ha Noi

НЕСКОЛЬКО ПРЕДЛОЖЕНИЙ ПО СОВЕРШЕНСТВОВАНИЮ ВЬЕТНАМСКОГО УГОЛОВНОГО ПРОЦЕССА В ОТНОШЕНИИ ЭЛЕКТРОННЫХ ДАННЫХ

Аннотация: Обновленные и дополненные части Уголовно-процессуального кодекса (далее – УПК), которые являются ключевой правовой основой деятельности органов по предупреждению и уголовному преследованию преступлений, особенно преступлений, связанных с информационными

технологиями сетями и телекоммуникациями, отвечающих насущным требованиями практики. Регулирование электронных данных и сбор электронных данных являются двумя наиболее важными новыми частями. Чтобы быть полезным в предотвращении и борьбе с преступностью в новом мире, необходимо регулярно дополняться и обновляться. Это связано с тем, что электронные данные и сбор электронных данных являются первыми проблемами, подлежащими регулированию.

Ключевые слова: электронные данные, сбор, уголовный процесс, борьба, преступность, технология сеть.

A FEW SUGGESTIONS TO IMPROVED THE VIETNAM CRIMINAL PROCEDURE CONCERNING ELECTRONIC DATA

Annotation: The updated and expanded parts of the Criminal Procedure Code (further – CPrC), which is a key legal foundation for agencies that work to prevent and prosecute crimes, especially those that involve information technology and telecommunications networks, have met the pressing needs of reality. The regulation of electronic data and the collection of electronic data are two of the most important new parts. For it to be useful in preventing and fighting crime in the new world, it needs to be constantly added to and updated. This is because electronic data and electronic data collection are the first concerns to be regulated.

Key words: electronic data, collection, criminal process, fight, crime, technology network.

The 13th National Assembly passed in the Criminal Procedure Code Vietnam in 2015 [1], which marks a new step in the process of conserving and promoting legislative triumphs while taking into account the experiences of other countries. The CPrC's updated and added provisions, which are a key legal basis for agencies that work to prevent and prosecute crimes, especially those that involve information technology and telecommunications networks, were changed in 2015 to meet the

pressing needs of reality. One of the important new components is the management and collection of electronic data.

- There are rules about what electronic data is, where it comes from, and how to judge its reliability

According to the 2015 CPrC's Article 99:

1. Symbols, codes, numbers, images, sounds, and other similar data that are created, stored, sent, or received using electronic technologies are referred to as "electronic data".

2. Electronic sources such as computer networks, phone networks, transfer lines, and other electronic sources must be used to collect the data.

3. The production, storage, transmission, and security of electronic data, as well as its source and any other relevant factors, should all be taken into account when figuring out the evidentiary value of electronic data.

Before the CPrC 2015, Article 99 offered the notion of digitized data, a subject that caused discussion and complicated research and administration. Electronic data is anything created, stored, sent, or received by an electronic device and that takes the form of characters, letters, numbers, images, sounds, or other comparable data. Examples of sources that include electronic data include electronic media, computer networks, telecom networks, online transmission, and other electronic sources. The method(s) used to generate, store, or transmit the electronic data; the method(s) used to ensure and maintain the integrity of the electronic data; the method(s) used to identify the originator; and other pertinent factors shall be considered in determining the evidential value of the electronic data [2, c. 48].

- Control of electronic data as a source of evidence

Together with other kinds of evidence, electronic data has been incorporated as a new and important source of evidence in Article 87 of the CPrC of 2015 to be used as a foundation for assessing criminal activities and addressing crimes.

- Laws governing electronic data gathering techniques

The CPrC 2015 says that the authorities can collect electronic information in the following ways:

Article 201 of the CPrC 2015 contains specifics on the scene examination. examining the site to look for evidence of criminal activity, confiscating and temporarily holding any exhibits, papers, or items connected to it, and explaining any information crucial to the resolution of the case.

When there is reason to believe that a person, place, or thing has the tools or means to commit a crime, as well as documents, items, or assets relevant to the crime, or electronic objects, data, or other papers related to the case, that person, place, thing, or thing must be searched [3].

To look at letters, telegrams, packages, postal parcels, mailers, and electronic data when there's a reason to think they contain evidence of a crime or documents, items, or property that are important to the investigation.

To employ specific procedural inquiry measures. Electronic data gathering is one of three unique procedural investigative methods that the subjects of criminal investigations are carrying out in accordance with the rules of Article 223 of the CPrC [4]. In situations involving crimes against national security, drug-related crimes, corruption, terrorism, money laundering, and other organized crimes of very severe criminality, subjects of criminal investigations may use electronic data collection methods.

Requesting electronic data from people, companies, and agencies This is the action that the cprc 2015 specifies in Clause 1 and Article 88.

To hire a professional to search for, retrieve, and look over electronic data.

- Rules for using computerized data collection techniques

According to Article 107 of the 2015 CPrC, “1. Electronic media shall be collected in a timely and comprehensive way, accurately depicting the real circumstances, and sealed immediately after the seizure”. Copies of electronic data should be sealed and opened in compliance with applicable legal requirements.

Article 196 also says that anyone who knows how to run a procedure can seize electronic devices and data, and they can let relevant professionals help. Since confiscation is not an option, it has to be backed up to the confiscation and storage media, much like exhibitions.

- Regulations for the protection of electronic data

Article 199 of the CPrC says that seized, detained, or sealed electronic data must be kept in its original state. This is how to keep electronic data safe.

So, it's clear that even though the 2015 CPrC brought the issue of electronic data and electronic data collection into the Code for the first time, the rules were mostly complete and did a good job of addressing how crimes are actually investigated and dealt with. This is a very important legal tool that law enforcement should use to stop crime and keep it from happening. But there are also limits to the rules that govern electronic data and the gathering of electronic data. These include:

First, some of the laws conflict with one another.

In general, there are several places where the requirements of Article 196 of the CPrC cross with the restrictions on collection by electronic means in Article 107 of the CPrC. Article 196 further states that it is unclear what should be backed up and what should be backed up on the storage medium. Is this storage medium an electronic medium in the sense of “backing up electronic data to electronic means,” as explained in Clause 1 of Article 107?

Article 99 says that “electronic data shall be collected from electronic sources such as computer networks, telecommunication networks, transmission lines, and other electronic sources”. However, Clause 2 of Article 107 doesn't say anything about this.

Second, the phrase is used insufficiently and inconsistently.

Articles 107 and 196 of the CPrC aren't good enough or clear enough because they only use the word “seize” when talking about electronic methods. Goods can only be seized if they can't be stored or sold. If this isn't the case, the items must be held by the right authorities until further action is taken.

The collection of electronic means and electronic data is mentioned in Article 107 of the CPrC 2015, but Clause 1 of this Law mandates that "electronic means must be promptly and adequately collected," and if obtaining electronic data storage devices is not possible, the procedure-conducting agency shall backup such data to electronic devices. This rule seems to be combining "electronic media collection" with "electronic media seizure," as may be observed. Although it is merely a question of gathering electronic data since electronic data is the source of evidence and electronic media is only the location to store electronic data.

In Article 99 of the CPrC 2015, the words "create", " transmit and receive" and "transmit" are used in ways that aren't consistent with the rest of the law. This makes it hard for those who enforce the law to do their jobs. The terms "initialization" and "transmission" are mentioned in Clause 2 and Article 14 of the Law on Electronic Transactions of 2005: "The evidence value of data messages is determined based on the reliability of the method of originating, storing, or transmitting electronic messages; the method of determining the originator; and other appropriate factors" [5].

Lastly, there are still some holes in the Criminal Process Code's rules about how to intercept the collection, evaluation, use, and storage of electronic data.

The procedure-conducting agencies may undertake field exams, searches, and seizures of telegraphs, telegrams, packages, postal parcels, etc. for the acquisition of electronic data from electronic means (computer networks, telecommunications networks). At the moment, there are no clear rules about the order or ways to do things like intercept electronic data on the transmission line.

For electronic data backup activities, there are no rules on the sequence and processes of backup, the requirements and conditions of the means used for backup, or the means used for electronic data storage [6, c.27].

When it comes to preserving electronic media, there hasn't been a clear definition of what electronic data is. Because electronic data differs from other types of criminal traces, it is also necessary to have more specific regulations in the case of

damaged electronic means or electronic data. These issues include how to fix, process, and figure out the legal value of electronic data that has been copied over and over again in different ways.

Article 107 of the CPrC 2015 states that only copies may be used for the restoration, search, and evaluation of electronic data. As a result, it is impossible to operate in practice when recovery on electronic storage media (originals) is not regulated.

We would like to suggest some of the following topics in order to make the Criminal Procedure Law's provisions on electronic data and electronic data collection more comprehensive:

Before making any required adjustments to the structure or content, it is important to examine and integrate Article 107 with Article 196 of the CPrC 2015.

It is required to analyze how Articles 196 and 107 may be combined and given the common name "collection of electronic means and electronic data" due to the severe interaction between them.

The seizure of electronic means and electronic data in the chapter "Search, seizure, and custody of documents and objects" is also currently incorrect. This is because the collection of electronic means and electronic data is often the next step after activities like field examination, search, etc., which are outlined in different chapters of the CPrC 2015.

After that, the following should be required as the new paragraph 1 of Article 107 (since Article 196 will have been merged into Article 107):

"Electronic means must be taken and temporarily held in a timely and thorough manner, appropriately characterized, and sealed immediately after the seizure and seizure. The seal must be closed and opened in accordance with legal requirements".

The agency conducting the procedure must back up any electronic data into an electronic medium and keep it as evidence if it is impossible to seize or cannot be done immediately. The procedure-conducting agency should simultaneously require the relevant agencies, organizations, and persons to keep and maintain the electronic

data they have backed up in its entirety, and these agencies, organizations, and individuals shall be legally accountable for their actions.

Persons qualified to carry out operations must seize or possess electronic devices, and they may be invited to do so by experts in the field [7, c.42]. It must be backed up to electronic storage facilities and seized or held temporarily as evidence if it is hard to seize or hold temporarily.

It is possible to take or temporarily keep the peripheral equipment and papers that go with the computer while seizing the computer for a short time [8].

The current versions of Article 107's paragraphs 2, 3, 4, and 5.

Second, to ensure uniformity by changing a few phrases in Article 99 of the CPrC 2015.

It is important to use the words "initialization" and "transmission" in Article 99, which says that “Electronic data is... created, stored, and transferred by electronic means”. This is to make sure that the law is consistent and follows the relevant legal rules.

Finally, documents should set forth the procedure for gathering electronic data.

Electronic data collection has its own rules that must be followed in a scientific and objective way. These rules come from how electronic data is different from other types of data. Thus, in the approaching period, functional agencies will need to research and submit documentation directing the electronic data gathering procedure to satisfy the stated criteria [9, c.372].

There should be clear laws on how to stop the collection of electronic data, including the steps to take, how to stop the collection, and what must be stopped. responsibilities of the ordering agency, as well as those of pertinent agencies, units, and people.

Certain guidelines are also required for electronic data backups. The backup may be done when the functional agency has to back up on the computer network, telecommunications network, or transmission line in addition to being set up in case

it is not feasible to seize or retain electronic data storage methods. There should be clear rules about the frequency and methods of backups, the hardware and software utilized for backups, and the methods for electronically storing data.

Electronic data is one of the new types of evidence that the CPrC 2015 adds. The recording of electronic data shows how the CPrC's evidence institution has grown, helps solve problems in the real world, and meets the practical needs of crime prevention and eradication, especially when it comes to crimes that use telecommunications and information technology. To successfully serve the prevention of and fight against crime in the new scenario, it is required to be continuously supplemented and updated. This is because electronic data and electronic data collection are the first concerns to be regulated.

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: 10.03.2023)

2. Võ Minh Tuấn, Khó khăn, vướng mắc về dữ liệu điện tử trong Bộ luật tố tụng hình sự năm 2015, tạp chí Toà án, số 2, 2021, tr. 48/ Во Минь Туан, Трудности и проблемы с электронными данными в Уголовно-процессуальном кодексе 2015 г., Судебный журнал, № 2, 2021 г., с. 48.

3. Hoàn thiện quy định về dữ liệu điện tử trong tố tụng hình sự [Электронный ресурс] // URL: https://vksndtc.gov.vn/tin-tuc/cong-tac-kiem-sat/hoan-thien-quy-dinh-ve-du-lieu-dien-tu-trong-to-tu-d10-t10468.html (Дата обращения: 12.03.2023)

4. Bàn về một số khía cạnh của dữ liệu điện tử trong tố tụng hình sự [Электронный ресурс] // URL: https://baovephapluat.vn/cai-cach-tu-phap/dien-dan/ban-ve-mot-so-khia-canh-cua-du-lieu-dien-tu-trong-to-tung-hinh-su-116824.html (Дата обращения: 09.03.2023)

5. 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: 14.03.2023)

6. Nguyễn Thành Minh Chánh, Pháp luật về chứng cứ điện tử tại Việt Nam, tạp chí Toà án, số 4, 2021, tr. 27/ Нгуен Тхань Минь Чан, Закон об электронных доказательствах во Вьетнаме, Судебный журнал, № 4, 2021 г., с. 27

7. Lê Thanh Nghị, Hoàng Thị Minh Phương, Hoàn thiện pháp luật tố tụng hình sự về chứng cứ từ nguồn dữ liệu điện tử, Tạp chí khoa học kiểm sát, số 47, 2021, tr. 42/ Ле Тхань Нги, Хоанг Тхи Минь Фуонг, Совершенствование уголовно-процессуального законодательства на доказательствах из электронных источников данных, Журнал прокуратуры, № 47, 2021, с. 42

8. Đặc điểm của dữ liệu điện tử trong bộ luật tố tụng hình sự 2015? [Электронный ресурс] // URL: https://luatminhkhue.vn/dac-diem-cua-du-lieu-dien-tu-trong-bo-luat-to-tung-hinh-su-2015.aspx (Дата обращения: 11.03.2023)

9. Bình luận khoa học Bộ luật Tố tụng Hình sự 2015, sách chuyên khảo. NXB Công an nhân dân, Hà Nội, năm 2018, tr. 372// Научный комментарий к Уголовно-процессуальному кодексу 2015 г.: монография. Изд. Полиций, Ханой, 2018 г., с.372.