ИНФОРМАЦИОННОЕ ПРАВО

УДК 343.1

Фам Ньы Хан
Академия народной безопасности Вьетнама
Кафедра профессиональных основ
Вьетнам, Ханой
nik.fam.89@mail.ru
Pham Nhu Han
People's Security Academy
Department of Professional Fundamentals
Vietnam, Hanoi

КИБЕРПРЕСТУПНОСТЬ И МЕТОДЫ БОРЬБЫ С НЕЙ ПО ЗАКОНОДАТЕЛЬСТВУ ВЬЕТНАМА

Аннотация: преступления, связанные с высокими технологиями, распространенные в киберпространстве, значительно увеличиваются по количеству, опасности и причинению вреда. Следовательно, создание новых стандартов для предотвращения и борьбы с этими правонарушениями имеет решающее значение. Для создания правовой основы для расследования, сбора и обоснования доказательств, особенно электронных доказательств, крайне важно своевременно изучить и доработать нормы уголовно-процессуального законодательства.

Ключевые слова: преступник, преступления в сфере высоких технологий, электронные доказательства, расследование, киберпространство, киберпреступность, электронные данные.

CYBERCRIME AND ITS REPRESENTATION IN VIETNAM'S LEGISLATION

Annotation: High-tech crimes, which are frequent in cyberspace, are rising in frequency, severity, and impact. As a result, developing new standards for preventing and combating these offences is vital. To provide a legal foundation for the investigation, acquisition, and substantiation of evidence, particularly electronic evidence, it is essential to analyse and update criminal process laws on a timely basis.
Key words: criminal, High-tech crimes, electronic evidence, investigation, cyberspace, cybercrime, electronic data.

Within the framework of the Fourth Industrial Revolution, there is a notable surge in the quantity, techniques, and tactics used by technologically advanced criminals operating in the cyber domain, resulting in more intricate and hazardous criminal activities. Based on the figures from the Department of Cyber Security and High-Tech Crime Prevention and Control, during the first half of 2023, the unit actively engaged in combating, dismantling, and collaborating with other authorities to prosecute 38 cases involving roughly 180 offenders [1].

The emergence of various criminal activities in cyberspace includes gambling, organized gambling, fraud, asset misappropriation, and illicit multi-level corporate operations. Furthermore, the individuals also exploited the internet to engage in various illicit activities, including launching cyberattacks on critical national security networks and the information systems of financial, banking, electricity, oil, and gas sectors. Their objective was to unlawfully obtain classified government documents, trade secrets, and customer data.

Unlike conventional crimes, cybercrime is done in a virtual context rather than a physical one. This poses several complexities and obstacles for the authorities in the investigation and management of this kind of criminal activity.

Provisions pertaining to the existing procedural law

The Criminal Procedure Code 2015 (further – CPrC) [2] contains several provisions aimed at fulfilling practical needs and establishing a legal framework for

authorities to effectively address cybercrimes via procedural and investigative measures.

Notably, the CPrC 2015 has incorporated electronic data as a valid form of evidence, on par with other specified sources of evidence mentioned in Article 87. This recognition marks the first instance where the CPrC acknowledges electronic data as a legitimate source of evidence.

Article 99 of the CPrC 2015 stipulates: “electronic data as symbols, scripts, numerals, images, sounds, or similar forms that are created, stored, transmitted, or received through electronic means. Electronic data can be collected from various sources such as electronic means, computer networks, telecommunications networks, transmission lines, and other electronic sources”. The evidentiary value of electronic data is determined by considering factors such as the method of generation, storage, or transmission of the data, ensuring and preserving the integrity of the data, and identifying the originator and other relevant factors.

The CPrC 2015 outlines specific procedures for collecting electronic data and electronic means. These procedures include field examination (Article 201), search (chapter XIII), requesting agencies, organizations, and individuals to provide information (Clause 1, Article 88), implementing special procedural investigation measures (Article 223, Article 224), and seeking expertise to recover, search, and inspect electronic data (Clause 3, Article 107, Articles 206, 207)...

These restrictions are crucial for the investigation and detection of crimes, particularly when offenders use advanced technology, telecommunications networks, and the internet...

Several constraints and deficiencies exist within procedural law.

Examining legislation pertaining to the investigation, collecting, and substantiation of cybercrime evidence reveals that although regulations concerning this field have been primarily established. Nevertheless, there are still some constraints and deficiencies that need the authorities to promptly investigate and address in order to enhance the efficacy of combating cybercrime [3, c.54].

As per Article 201 of the CPrC 2015, the examination of the crime scene is conducted at the location where the crime took place or was discovered. This examination aims to identify evidence of the crime, collect exhibits, documents, objects, and electronic data relevant to the case, and gather important information to help resolve the case.

Nevertheless, as previously said, cybercriminals distinguish themselves from conventional criminals by using digital gadgets, computer networks, and software programs as instruments to perpetrate illicit activities. Hence, the crime scene, papers, evidence, and traces of the crime possess distinct attributes. They do not manifest as tangible exterior entities, but rather reside inside digital devices, computers, and computer networks. The scene, documents, evidence, and traces associated with this particular kind of crime has distinct characteristics. However, we now lack precise legislation governing the investigation of the scene, the collecting of evidence, traces, and documents in the digital environment, specifically in cyberspace.

The evidence and traces of cybercrime are distinct and do not manifest in a tangible, outward physical form. Hence, the inquiry and acquisition of evidence for this offense need certain norms and protocols.

Article 107 of the CPrC 2015 contains explicit provisions for the gathering of electronic devices and electronic information. Hence, it is imperative to expeditiously and comprehensively confiscate electronic devices, accurately document their characteristics, and instantly secure them with appropriate seals upon confiscation. The act of affixing and removing seals must be conducted in compliance with the legal regulations. If it is not feasible to confiscate the electronic data storage device, the responsible agency must create a backup of the electronic data on another device and preserve it as physical evidence. Simultaneously, the agency must request that other relevant entities and individuals also store and preserve the backed-up electronic data. These entities and individuals will be legally accountable for this responsibility. During the process of gathering, intercepting, and safeguarding electronic data from electronic media, computer networks, telecommunications

networks, or transmission lines, the authorized agency responsible for the investigation is required to create a detailed record and incorporate it in the official case documentation...[4, c.44]

Although electronic evidence possesses distinct characteristics from traditional evidence, the process of inspecting, evaluating, preserving, and sealing it adheres to existing general regulations. However, in order to safeguard the data's integrity and preserve its evidentiary value, it is imperative to establish stringent legal provisions specifically addressing the inspection, evaluation, preservation, and sealing of electronic evidence.

Furthermore, as stipulated in the 2015 CPrC, electronic data is also obtained by means of expert examination solicitation, as outlined in Article 206 and Article 207 of the Code. A solicitation for expertise on electronic data is a method used to gather crucial electronic data. This helps in obtaining evidence through the analysis of electronic data and devices during investigations of criminal activities involving the use of information technology and cyberspace.

However, in situations when it is necessary to seek specialized knowledge according to the regulations (as stated in Article 106 of the CPrC), there have been no instances using electronic data. The request for specialized knowledge on electronic data is applicable in cases where the investigating agency thinks it appropriate, allowing for discretion in its implementation.

Furthermore, it should be noted that the CPrC of 2015, along with other existing legal texts, lacks explicit provisions for the retrieval and handling of electronic data. Does it qualify as a form of evidence? Indeed, the examination of cybercrimes reveals that several individuals have deliberately eliminated, rectified, and obliterated electronic evidence pertaining to illegal activities just before to their apprehension. To definitively establish the illegal activities of the individual, it is essential for the authorities to retrieve this electronic data. Due to the absence of precise legislation regarding electronic data recovery operations, the use and

application of recovered electronic data as legal documents and evidence to substantiate criminal offenses remain insufficient...

Suggestions

Cyber-crimes differ from typical crimes in that they are not limited to physical environments. Instead, criminals use digital gadgets, computer networks, and software programs as means to carry out their illegal activities. The investigation and management of this sort of crime provide several problems and obstacles for the authorities, particularly in regards to the search and analysis of crime scenes, as well as the gathering and preservation of evidence [5, c.31].

Based on the aforementioned analysis and research, we assert that in order to enhance the caliber and efficacy of cybercrime prevention and control in the near future, it is imperative for the authorities to promptly examine and finalize legal provisions such as the Penal Code, the Criminal Procedure Code, the Law on Cybersecurity, the Law on Information Technology, the Law on Electronic Transactions, and various other legal instruments. Specifically, there is a need to enhance the legislation governing criminal proceedings pertaining to the investigation and management of cybercrimes.

Expanding and refining the examination of digital and electronic evidence in the CPrC is important and should be done promptly. Due to the unique nature of cyber-crimes, such as the absence of physical proof and the presence of digital footprints, scenes, documents, and evidence associated with these crimes lack a tangible form. Although it may seem separate from physical reality, the digital realm encompasses gadgets, computers, and computer networks. Consequently, it necessitates particular legislation pertaining to the investigation of acts conducted in the digital environment, also known as cyberspace [6].

Furthermore, it is essential to establish explicit and precise guidelines on the examination, assessment, safeguarding, and sealing procedures to safeguard the integrity of data and preserve its evidentiary significance.

Furthermore, it is imperative that proficient authorities promptly provide guidelines pertaining to the acquisition, safeguarding, and utilization of digital information [7, c.20]. Identify the particular instances where it is necessary to request the assistance of experts in electronic data, particularly in situations where electronic devices used to create, store, or transmit electronic data are intentionally destroyed by criminals or fail to cooperate in the search, retrieval, identification, preservation, or examination of electronic data.

Conversely, cybercrime refers to illicit activities, such as the creation of illegal papers, gathering of evidence, and leaving behind criminal traces, that occur in the digital realm and may transcend national boundaries. Hence, it is essential for responsible authorities to enhance global collaboration in order to tackle this kind of criminal activity.

Список литературы:

1. Báo cáo thống kê của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao về tình hình tội phạm mang 06 tháng đầu năm 2023/ Статистический отчет Департамента кибербезопасности и предотвращения и борьбы с высокотехнологичной преступностью о криминогенной ситуации за первые 6 месяцев 2023 года/ [Электронный ресурс]. URL: https://namcan.camau.gov.vn/wps/portal/?1dmy&page=nc.chitiet&urile=wcm%3Apath%3A/huyennamcanlibrary/siteofnamcan/hdhdhuyen/kht5nk20212026/vb3 (Дата обращения: 30.11.2023)

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: 02.12.2023)

3. Nguyễn Ngọc Thương, Một số giải pháp phòng ngừa tội phạm sử dụng công nghệ cao, Tạp chí CSND số 02/2017, tr.54./ Нгуен Нгок Туонг, Некоторые

решения по предотвращению преступности с использованием высоких технологий, Журнал «Народная полиция» № 02/2017, с.54.

4. Phạm Văn Tuân, Lê Thanh Nam, Một số giải pháp phòng ngừa tội phạm sử dụng công nghệ cao trong lĩnh vực ngân hàng trên địa bàn Thành phố Hồ Chí Minh, Tạp chí Khoa học Kiểm sát số 03 (29)/2019, tr.44./ Фам Ван Туан, Ле Тхань Нам, Некоторые решения по предотвращению преступлений с использованием высоких технологий в банковском секторе Хошимина, Журнал прокуратуры № 03 (29)/2019, с.44

5. Đàm Thanh Thế, Nhận diện tội phạm sử dụng công nghệ cao trong quản lý nhà nước và một số giải pháp, Tạp chí CSND số 08/2019, tr.31./ Дам Тхань Те, Выявление преступников, использующих высокие технологии в государственном управлении, и некоторые решения, Журнал «Народная полиция» № 08/2019, с.31.

6. Tình hình an ninh mạng và xu hướng tội phạm mạng tại Việt Nam giai đoạn 2022 – 2023./ Ситуация с кибербезопасностью и тенденции киберпреступности во Вьетнаме в период 2022 – 2023 гг./ [Электронный ресурс]. URL: https://ninhthuan.dcs.vn/vptu/1307/31798/55131/285879/An-Toan-Thong-tin/Tinh-hinh-an-ninh-mang-va-xu-huong-toi-pham-mang-tai-Viet-Nam-giai-doan-2022---2023.aspx (Дата обращения: 30.11.2023)

7. Nguyễn Đức Hiếu, Cảnh giác với các “chiêu” lừa đảo của tội phạm công nghệ cao, Báo Pháp Luật số 04/2023, tr.20./ Нгуен Дык Хиеу, Остерегайтесь мошеннических «проделок» преступников в сфере высоких технологий, Юридическая газета № 04/2023, с.20.