Nhu Han PHAM*
Department of Criminal Procedure,
Volgograd Academy,
Ministry of Internal Affairs
of the Russian Federation

Review paper
Recieved: 13 July 2021
Accepted: 18 October 2021
UDK: 343.53:004.738.5(597)
https://doi.org/10.47152/rkkp.59.3.7

Nikolay Nikolayevich DEMIDOV, PhD**
Dr. Assocociate Professor, St. Petersburg University,
Ministry of Internal Affairs of the Russian Federation,
Kaliningrad Branch, Faculty of Special Training

E-EVIDENCE OF CYBERCRIMINAL ACTIVITIES AS A NEW LEGAL PHENOMENON (BASED ON THE CRIMINAL PROCEDURE CODE OF THE SOCIALIST REPUBLIC OF VIETNAM, 2005)

Today's modern global society is facing an unexpected situation where cybercrimes are becoming more and more complicated, severely violating social order and security. The Criminal Procedure Code (CrPC) Vietnam 2015 has made important amunpredictable endments and supplements to evidence and evidence institutions, which are important institutions on which procedural bodies base to perform their duties and exercise their powers. Most prominently, the regulation of evidence sources which is electronic data, an entirely new source of evidence, is to respond promptly to crimes using high technology. Within the scope of this article, the author focuses on the new points of the CrPC Vietnam 2015 on the source of evidence that

* E-mail: cavoi89@yandex.ru
** E-mail: n_demidov@hotmail.com, ORCID: https://orcid.org/0000-0002-6914-8236

is electronic data in high technology crimes. Further the principles of the evidence act has been explained with amendments in regard to electronic evidence. Finally the safeguards and procedure which needs to be adopted by the Vietnamese judiciary in handling electronic evidences.

Keywords: electronic evidence, proof process, cybercrime, data message, electronic document value evideniary.

1. Introduction

According to the recent Global Cybersecurity research currently, 3.5 billion people are online and the digital world is estimated to be 44 zettabytes, with no risk of unavailable storage thanks to cloud computing. Furthermore, the proliferation of ICTs has hit the broader national ecosystem, giving rise to new organizational possibilities, such as e-government services, and new economic and productive paradigms such as Industry 4.0 and the broader digital economy.

All countries are affected to some extent by the digital divide, and as a key driver of economies, societies and governments, which depend on digital systems, cybersecurity should be a top priority.

The COVID-19 pandemic has dramatically affected how societies operate. As the pandemic began to take hold in April 2020, Akamai noted Internet traffic increased by 30 per cent.[1] From teleworking to distance learning, technology has played a key role in keeping people connected. For the digital age to realize its potential, a reliable and secure cyberspace must be essential. A year after COVID19 was declared a pandemic by the World Health Organization and the development of new vaccination and management systems, our dependence on digital technology continues to grow. And because the world connects what is not connected, a safe and reliable cyberspace must be guaranteed.

There is an increased recognition of cybersecurity risk.[2] The ongoing pandemic has created distrust, especially online. Many challenges today erode online trust and prevent the digital society from operating at its full potential. For example, global losses due to cybercrime are estimated from as low as USD 1 trillion in 2020[3],

1 *Can the internet keep up with the surge in demand,* available at: https://blogs.akamai.com/2020/04/can-the-internet-keep-up-with-the-surge-in-demand.html, accessed on 29.09.2021.

2 *Global risks report 2020,* available at: *http://reports.weforum.org/global-risks-report-2020/executive-summary/*, accessed on 02.10.2021

3 *The Hidden Costs of Cybercrime,* available at: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf, accessed on 05.10.2021.

to as high as USD 6 trillion in 2021.[4] Developing legal and regulatory frameworks to protect the public and promote a secure digital environment is critical and should be the start of any national cybersecurity effort.

The legal and regulatory framework includes the establishment of legislation identifying what constitutes illegal activity in cyberspace, along with definitions of the procedural tools needed to investigate, prosecute and enforce those laws; establish a cybersecurity baseline and compliance mechanism for various national stakeholders; and procedures to ensure consistency with international obligations.

More than 90% of responding countries reported that cybercrimes were most often brought to the attention of law enforcement authorities through individual or corporate victim reports. Responding countries estimated that the true victimization rate of cybercrimes reported to the police was over 1%. A global private sector survey shows that 80% of individual victims of basic cybercrimes do not report the crime to the police. The lack of reporting stems from a lack of awareness of victimization and reporting mechanisms, victim shame and embarrassment, and perceived reputational risk to businesses. Authorities from all regions of the world are highlighting initiatives to improve reporting, including online reporting systems and hotlines, public awareness campaigns, connecting with the private sector and increasing police awareness and information sharing. However, incident-based responses to cybercrime must be accompanied by medium- and long-term tactical investigations that focus on the crime market and the architects of criminal patterns. Law enforcement in developed countries is involved in this area, including through undercover units targeting offenders on social networking sites, chat rooms, instant messaging, and P2P services. Challenges in cybercrime investigations arise from criminal innovation by perpetrators, difficulties in accessing electronic evidence, and internal resources, capabilities, and logistical limitations. Suspects often use anonymization and undercover technology, and new techniques are rapidly reaching large criminal audiences through the online crime marketplace.

Law enforcement cybercrime investigations require a mix of traditional and new policing techniques. While some investigative actions can be carried out with traditional strengths, many procedural settings do not translate well from spatial and object-oriented approaches to approaches that involve electronic data storage and real-time data flow. The research questionnaire refers to ten investigative acts on cybercrime, ranging from general searches and seizures to special powers, such as computer data storage.

4 *Cybercrime To Cost The World $10.5 Trillion Annually By 2025,* available at: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, accessed on 04.10.2021.

Vietnam is ranked 25th out of 182 countries in the 2020 Global Cyber Security Index (GCI) by the International Telecommunication Union, the United Nations specialized ICT agency, compared to 50th and 100th positions in 2018 and 2017. This jump has surpassed the goal of joining the top 30 GCI countries by 2030 (Prime Ministerial Decree No. 749 / QDTTg 3 June 2020) and demonstrating its determination and performance in ensuring cyber security, and in combating cyber crime.

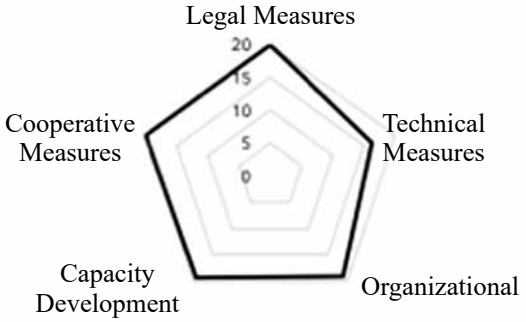
In 2019, Vietnam established the Vietnam Cybersecurity Emergency Response Teams / Coordination Center (VNCERT / CC). This agency is dedicated to coordinating security incident response and verifying information security nationally. The establishment of VNCERT/CC is timely, given the increasing number of cyber attacks in Vietnam. Another agency responsible for dealing with major cybercrimes is the Department of Cybersecurity and Crime Prevention Hitech (Department A05) under MPS.

Table 1. GCI results: Asia-Pacific region[5]

Overall Regional Country Name Score Rank
Korea (Rep. of) 98.52 1
Singapore 98.52 1
Malaysia 98.06 2
Japan 97.82 3
India 97.49 4
Australia 97.47 5
Indonesia 94.88 6
Viet Nam 94.55 7
China 92.53 8
Thailand 86.5 9
New Zealand** 84.04 10
Bangladesh 81.27 11
Iran (Islamic Republic 81.06 12 of)
Philippines 77 13
Pakistan 64.88 14
Sri Lanka 58.65 15
Brunei Darussalam 56.07 16
Nepal (Republic of) 44.99 17
Myanmar 36.41 18

5 *Global Cybersecurity Index,* available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, accessed on 01.10.2021.

Viet Nam (Socialistic Republic of)



Development Level:
Developing Country

Area(s) of Relative Strenght
Legal, Cooperative Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
94.55	20.00	16.31	18.98	19.26	20.00

Source: ITU "Global Cybersecurity Index", 2021.

Chart 1. CGI of Vietnam[6]

Cybercrime acts are perhaps unique amongst crime in general, in that widespread technology-based prevention measures exist – including anti-virus and network security products and firewalls.[7] The role of such products is usually based on scanning, identifying and filtering for certain electronic "signatures". These may be content-based, or traffic-based, such as communications to or from "blacklisted" IP addresses.[8] Many products also include heuristic detection that checks for suspicious file and connection behavior against predefined conditions. Activity logs generated by technology-based security products then capture a subset of cyber content and traffic events that may, in some circumstances, correspond to the component of a cybercrime act. Attempts or completion of acts of illegal access to computer systems or illegal interference with computer systems or computer data, for example, may be detected by the product and result in a response. An obscure analogy is a home burglar alarm that detects events on the doors and windows of a house. The fact that the alarm has been triggered does not necessarily mean that a crime has been committed. However, a certain percentage of crime can raise the alarm.

6 *The Global Cybersecurity Index (GCI) 2020,* available at: https://www.itu.int/en/ITUD/Cybersecurity/Pages/ global-cybersecurity-index.aspx, accessed on 02.10.2021

7 *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems andnetworkstowardsacultureofsecurity.htm , accessed on 05.10.2021.

8 Callanan, C. et al. (2009) *Study on Internet blocking, balancing cybercrime responses in democratic societies*. Aconite Internet Solutions.

The advantage of technology-based cybersecurity products is that a large number of "anti-theft tools" can report events logged in a central location, enabling the production of aggregated cybersecurity statistics. Many private sector cybersecurity vendors generate reports based on these statistics. However, providers often use very different definitions; calculation method.

1.1. Criminal activities

Vietnam has become a hotbed of cybercrime, with criminals turning into more and more more state-of-the-art at the same time as banks nonetheless the usage of old, insecure technologies.

Many banks in Vietnam have suggested approximately clients dropping statistics approximately their money owed to criminals via phishing assaults and different methods.

In a latest assertion Techcombank stated it had detected many instances of fraud and misappropriation of cash via way of means of faking Western Union transactions.

The criminals could ship sufferers faux Techcombank messages claiming that they'd acquired cash via Western Union, and inform them to visit a faux Techcombank internet site and log in to verify the transaction, ensuing of their account informatons being stolen.

In this year, Maritime Bank has issued a statement warning customers about a scam in which criminals contact them via phone calls, text messages, social networks, and emails posing as bank employees. They then ask victims to provide their account information in exchange for money, promotions or gifts. Other major banks such as VPBank and Vietcombank have also issued similar statements warning customers against disclosing their OTP codes to anyone, including the bank itself, under any circumstances. They are also required to closely monitor their accounts for any abnormal activity and immediately report to the bank if they receive suspicious phone calls or text messages. According to global statistics recently released by cybersecurity firm Kaspersky Lab, nearly 36% of cyberattacks in the second quarter 2021 involved financial services, of which more than 21% targeted banks and 8.17% targeted online stores[9].

Eight criminals were arrested in Vietnam and three more in the UK[10]. All of these criminals are linked to the „mattfeuter" family of websites (mattfeuter.ru,

9 Le, T. T. et al. (2020) Cyber crimes in the banking sector: Case study of Vietnam. *International Journal of Social Science and Economics Invention, 6(*5), pp. 272-277. https://doi.org/10.23958/ijssei/vol06-i05/207

10 *Vietnamese Carders arrested in MattFeuter.ru case,* available at: *https://blogs.msmvps.com/garwarner /2013/06/05/vietnamese-carders-arrested-in-mattfeuter-ru-case/,* accessed on 02.10.2021.

mattfeuter.cc, mattfeuter.su, mattfeuter.com, etc.) where about 16,000 members buy and sell stolen credit card data in bulk. Purchases from the website are believed to have facilitated more than $200 million of credit card fraud worldwide through the sale of more than 1.1 million credit cards. SOCA and PCeU merged to form a new National Crime Agency later this year, but are already conducting joint operations such as this one in anticipation of the UK's new National Cyber Crime Unit.

Operations of this nature could now no longer be feasible with out the guide of personal area partners, in this example on the whole Visa and MasterCard.

In retaining with UK law, the names of the 3 arrested there aren't given, simplest their names and locations:

- 37 year old man from West Ham .
- 34 year old man from Thornton Heath .
- 44 year old man from Manor Park.

In the US, the New Jersey US Attorney's office has filed charges on 23 year old Duy Hai Truong, of Ho Chi Minh City, in Vietnam.

Vietnamese media has identified those arrested in Vietnam, the five in HCM City were accused of illegally publishing and using information from the Internet. The three in Hanoi are accused of using credit card information for online gambling. The gang leader, is accused of setting up the website Mattfeuter, where credit cards are sold for between $2 and $20 per card. As site operators, he and his group have earned about $1.5 million in commissions from their sales. While we haven't heard of many Vietnamese cybercrime cases, improvements in Vietnamese laws passed in 2009 have made it a crime to fraudulently obtain card data from overseas targets, as well as from victims in Vietnam.

In a statement from the New Jersey US Attorney's Office, Paul Fishman announced that Truong was charged with "conspiring to commit bank fraud. From 2007 until his recent arrest, Truong was suspected of defrauding financial institutions as part of a large-scale scheme in which information Personal identities are linked to more than 1.1 million credit cards stolen and resold to criminal customers worldwide". The New Jersey statement alludes to "arrests made last week in the UK, Vietnam, Italy, Germany and elsewhere", so I'm sure there will be more news in the near future as details of this case come to light.

The official complaint against Truong revealed that fees on the mattfeuter.biz and mattfeuter.com websites ranged from $1 to $300 per "garbage dump" (a landfill which refers to the magnetic stripe read by credit cards), and that taxes are generally paid via Western Union or Liberty Reserve. Truong is being held in Vietnam awaiting settlement of the charges in the UK, but if convicted in the US, Truong could face up to 30 years in prison and a $1 million fine or double the income from the offence, or double. much of the loss caused by the infringement,

if greater. New Jersey also released a sworn complaint from FBI Special Agent Russell Ficara, who testified that he had reviewed more than 1,100 bank accounts and numerous searches for email accounts, residences, offices, and addresses linked to the case. His testimony includes many of the email accounts used, including mattfeuter123@gmail.com, augustino267@gmail.com, ho.robbie@gmail.com, and included more than 150,000 email messages with more than 1.1 million credit card numbers being traded, including cards and Personally identifiable information (PII) related to many victims residing in New Jersey.

Like many criminals, Truong also has a Facebook account that refers to his real name, refers to the conspiracy and contains photos of messages to and from landfill buyers and refers to stolen credit cards.

It has been documented that one Western Union office "in Ho Chi Minh City, Vietnam or surrounding areas" has received over $1.9 million in payments related to the MTCN (money transfer control number) alone documented in emails from three account referrals, all controlled by Truong.

Evidence in criminal cases not only has a great legal significance to prove criminal acts, but it also has a very important meaning when manipulating to collect, analyze and convert electronic evidence to traditional evidence in order to investigate, prosecute and adjudicate cases that criminals abused advanced scientific and technical achievements as tools and means to commit crimes (high-tech crimes)[11].

One of the most important sources of evidence in high-tech crimes cases is the evidence seized at the place where the crime occurred, bearing a criminal trace such as: „cookies", „URLs", web servers logs, Email logs... (these are computer generated information); or may also be man-made electronic information stored in computers or other electronic devices, such as documents, tables, images, information stored in electronic signals.

Most people who use high technology to commit crimes have a high level of legal awareness and knowledge, and when committing crimes, there are sophisticated tricks to hide criminal information, When they detect a risk of disclosure, they quickly remove traces to denounce (such as deleting related data; demolishing Web sites), so collecting, restoring and transmitting electronic evidence into the traditional evidence to prove the crimes of the subjects is extremely important, it determines the success or failure of a specialized case.

At the present time, developments in information technology, digital evidence plays an increasingly significant role in criminal and civil litigation. Today, digital evidence is now applied to prosecute all types of crimes, not just cybercrime.

11 *Một số bất cập về chế định chứng cứ trong Bộ luật Tố tụng dân sự năm 2015,* availabe at: *https://tapchitoaan.vn/bai-viet/phap-luat/mot-so-bat-cap-ve-che-dinh-chung-cu-trong-bo-luat-to-tung-dan-su-nam-2015,* accessed on 01.10.2021.

Because many types of digital evidence may be necessary for litigation, the judicial system has to be assured of its accuracy, dependability, and verifiability. Correspondingly, establishing the chain of custody when authenticating digital evidence in the courtroom is extremely important and utterly necessary. The chain of custody must account for the seizure, storage, transfer, and the condition of the evidence. This sounds far beyond just finding and extracting the data, examining and interpreting its relevance, and generating a report.

Digital evidence can be active, deleted, hidden, encrypted, or overwritten, and cannot be determined by the naked eye. When dealing with digital evidence, relevant scientific principles relating to the collection, processing, and examination of evidence must be accompanied

These days, the admissibility of electronic evidence in any jurisdiction is increasingly more common: comments in social media, video recordings, instant messaging, certified emails, etc.

Taking into account the complex and dangerous situation of this group of criminals, if the 1999 Criminal Law only provides for 3 crimes in the field of information technology, including the crime of creating, disseminating and disseminating computer virus programs (Article 224); violation of computer network operations, The crime of using and using the rules (Article 225); the crime of illegally using the network and computer information (Article 226), the criminal law revised in 2009 added two new crimes in this regard, namely the crime of illegally entering the computer network, telecommunications networks, the Internet (Article 226a); crimes involving the use of computer networks, telecommunications networks, the Internet, or digital devices for the purpose of embezzling property (Article 226b). With the passage of the 2015 Criminal Code on November 27, 2015, the number of crimes officially stipulated by laws in the field of information technology has increased significantly.

But this wide variety of sources of digital evidence must have access to the judicial process through some of the legally prescribed means of proof. For clarifying this topic, in this article we will answer the following question : what is electronic evidence?

1.2. What is electronic evidence?

In a presentation presented at the Workshop „Prevention of traditional and non-traditional crimes" organized by the Ministry of Public Security and the People's Police Academy in April 2018; Dr. Tran Van Hoa, Deputy Director of the High-tech Crime Prevention Police Department, said: "Electronic evidence is

evidence stored in the form of electronic signals in computers or in devices with a set of digital memory involved in criminal cases". According to the International Criminal Police Organization (Interpol), electronic evidence is investigative information and data that is stored or transmitted by a computer, computer network or others technical electronic device.

We define electronic evidence as all information with probative value that is included in an electronic media or is transmitted by said media.

For this, we distinguish two basic types of electronic evidence:

1. Data stored in computer systems or devices.

2. Information transmitted electronically through communication networks.

The 2015 Criminal Procedure Code (CPrC) has great significance for the reality of the investigation, prosecution, and adjudication of criminal cases[12]. One of the new and progressive regulations to effectively serve the requirements to fight against crime in the new situation is the provision of sources of evidence - electronic data (electronic evidence). A newly added source of evidence requires the corresponding provisions on the collection, inspection, and evaluation as well as monitoring these processes on such evidence to create a premise for the proper resolution of criminal cases. This will be especially appropriate for cases in the field of high technology and the cases using information technology as tools and means of crime.

It can be assumed that the overall situation of current crimes, especially information technology crimes, is becoming more and more complex, and behaviors and tricks are becoming more and more complex. Ordinary criminals also use electronic means to commit crimes. Therefore, the 2015 Criminal Procedure Code added „electronic data" as a new and valuable source of evidence, as an additional source of evidence, as a basis for determining criminal offenses and handling criminal offenses. In addition, the regulations are in full compliance with international conventions and Vietnamese laws.

2. Methodology

2.1. The provisions of the law on electronic evidence

Electronic data - as a source of evidence, is defined as "symbols, letters, numbers, images, sounds or the other similar forms which are stored, transmitted or received by electronic means "(Art. 99 CPrC). This provision expresses the consistency and concretization of the concept of "data" in the 2006 Law on Electronic

12 Criminal Procedure Code of the Socialist Republic of Vietnam, No. 101/2015/QH13, dated November 27, 2015

Transactions: "Data is information in the form of symbols, letters, numbers, images, sounds or similar format"[13]. Electronic data has been recognized as legal and valid as evidence since 2006 - in electronic transaction law. However, it was not until the 2015 CPrC, that electronic data was legalized, considered as one of the sources of evidence. This overcomes the inconsistency between content law and formal law in the CPrC of 2003.

When electronic data is collected in accordance with the measures provided by the CPrC and satisfies the properties of the evidence, the electronic data is considered to be electronic evidence. So, what is electronic evidence? Although the current law does not have the legal concept of "electronic evidence", but in terms of legal science, we can understand: "Electronic evidence is the evidence stored in the form of electrical signals in computers or in devices with digital memory related to criminal cases" (Nguyen, 2016: 317). In addition, it can be understood that "electronic evidence is investigative information and data stored or transmitted by a computer, computer network or other digital electronic devices" (Tran, 2015:70).

From the above interpretations, electronic evidence can be seen having the following characteristics:

- It's a type of non-traditional evidence, not an object or event as previously conception. It's digital characters stored in media, electronic devices or on the global information network which, after the processing process, will produce data including numbers, words, sounds, images, etc., thereby providing information related to the crime event;

- It's created in cyberspace and without borders or territories. Therefore, the collection, inspection, and evaluation as to convert them into traditional evidence, which is used as a basis for proving crimes, is also unique, requiring specific provisions and in-depth instructions. However, at present, the CPC only stipulates the "collection of electronic means and electronic data" (Article 107 of the CPrC). As for the examination and evaluation of electronic evidence, there are no separate regulations. Therefore, the examination and evaluation of electronic evidence shall comply with the general provisions on examination and evaluation of evidence prescribed in Article 108 of the CPrC.

In addition, to evaluate electronic evidence, the provisions of Clause 3, Article 99 of the CPrC can be applied. Accordingly, "the value of evidence in electronic data is determined based on the manner in which it is created, stored or transmitted electronically, and the way to ensure and maintain the integrity of electronic data, the manner to identify creators and other relevant factors" (Tran,

13 Law on Electronic Transactions of the Socialist Republic of Vietnam, No: 51/2005/QH11, dated November 29, 2005

Phung, 2018). It can be said that the provisions on "evidence value of electronic data" in the CPrC are derived from the provisions on evidence value of data messages prescribed in Clause 2, Article 14 of the 2006 Law on Electronic Transactions. "The evidence value of data messages is determined based on the reliability of the way the data are created, stored or transmitted; the way ensure and maintain the integrity of data messages; the manner to identify creators and other relevant factors".

Based on the above grounds, they divide electronic data into categories:

Firstly, electronic data created by users: are documents and data created by human beings and stored in electronic memory, such as documents, tables, digital images, e-mail, web pages, service user information, online chat content, customer feedback ...

Second, electronic data generated by a computer automatically: A result created after a computer program processes the input data according to a defined algorithm. For example: Computer file transfer logs (FTP transfer logs), network protocol logs from internet providers (IP logs from ISPs), operating system logs/ registry files (Operating System Logs / Registry Files); Webmail IP logs and records ... The human impact on computer-generated data is very limited. Therefore, this type of data has a very high level of evidence.

Most electronic evidence is created by both humans and computers. We can exploit them from many electronic devices such as:

- Mobile devices: Mobile devices often store important evidence for investigations: Messages, calls ... or even some mobile devices automatically save the user's browser schedule.

- CD Roms, removable drives (External Drives), routers.

- Service providers (Email, website, server ...) is an important source of electronic data. They will provide litigation agencies with information about users of services, data logs, copies of computer data, etc.

However, the problem of discovering, preserving, evaluating and using this type of evidence is very difficult because its existence depends on the time, storage setup process, storage devices and time of detection. Criminals can delete, edit quickly to destroy electronic data, making it difficult to collect and recover evidence (according to Tran, Phung, 2018).

2.2. Actual work of collecting, checking and evaluating electronic evidence

Criminals increasingly tend to use sophisticated tricks related to information technology. Criminal cases in which subjects using electronic means and technological

equipment to commit crimes are increasing, taking place in many types of crimes such as fraud, appropriation of property, prostitution, gambling ...

In criminal cases where criminals use information technology and electronic devices as means of crime without electronic data provisions, the procedure-conducting bodies still collect, examine and evaluate electronic evidence. The collection of electronic evidence shall be conducted in the same order as other sources of evidence. It is an electronic means of the seizure (usually a telephone), which holds information about electronic data. After seizing electronic means, the Procedure Agency conducts the data extraction, duplicates the data but mainly transcribes the contents of the conversation (in the form of messages still stored in the device) or statistics of transaction history (mainly incoming calls, outgoing calls). However, there are also cases where Procedure Agency does not seize electronic means (computers) but extract data with the owners from computers on paper, as documents to record (signed) confirmation by extractor). For complex cases, Procedure Agency conducts data recovery through professional individuals and organizations. These individuals and organizations are committed to the restored content. These data are transformed into physical evidence and used to fight the criminals.

However, due to the absence of specific regulations related to collecting, examining and evaluating electronic evidence, in reality, electronic evidence collection, test, and evaluation often depend on capacity, qualifications of direct performers. On the other hand, the collection of electronic evidence as above is incomplete, which is not true to the nature of electronic evidence; especially in the case of Procedure Agency transcribing the content of transactions that are still stored in electronic media. Collecting in this way will miss data that the user has deleted. In this case, it is difficult to recover data in electronic media system logs or extract data from the operator because it has not been legalized, so the operator often take reasons of Customer information security and refuse to cooperate.

The establishment of the 2015 Criminal Procedure Code with legalized data and specified measures to collect electronic means and electronic data (Article 107) have overcome the previous disadvantages. Through practical work of resolving a number of criminal cases related to information technology, it is realized that the collection, examination, and evaluation of electronic evidence are carried out as follows:

- For electronic media with electronic data storage (computer hard drive, smartphone, USB, memory card, optical disc, camera, camera, email ... smartphone ...) of offenders, crime victims, persons with related rights and obligations: Procedure Agency seizes, records, seals and preserves the evidence. When handing over material evidence to data recovery experts for copying data, they must

ensure the provisions of the law on procedures for opening and sealing. In case the Procedure Agency directly copies electronic data (for example, messages stored in the phone), to ensure objectivity, they must make a record of the content of the electronic data, accompanied by testimony and confirmation of digital device owner and bystander.

- Electronic data related to the case is not only stored on the device of the culprit, the victim, but also stored on the servers of internet providers, banks, and other third-party servers, network operators, electronic exchanges, electronic payment gateways, tax authorities, customs authorities ... Therefore, besides the act of Procedure Agency directly copying electronic data from captured digital devices as evidence, The electronic data collection at operators of mobile phones that the subjects have used is essential to check the accuracy of information copied from captured digital devices.

- In procedural practice, Procedure Agency also conducts electronic data assessment. The electronic data assessment performed by judicial examiners is mainly recovering, decoding and analyzing activities focusing on finding data stored, existing in-network storage devices or in your personal digital device, to find data as evidence. This is not a comparison, traceability of electronic data because there is no original file as a standard but this activity is only to search for data with content related to criminal acts, perpetrators, victims, or damage.

After the conclusion of the assessment, the electronic evidence is converted into physical evidence in combination with other relevant evidence such as material evidence, testimony, etc. which is the basis for proving the crime and contributes to the correct and objective judgment. It can be said that the collection of electronic evidence is very important in the practice of proceedings for the type of technology crime. However, the practice of collecting, examining and evaluating electronic evidence still faces many difficulties and obstacles.

2.3. Difficulties and problems in the collection, inspection, and evaluation of electronic evidence

Firstly, In terms of legal documents: In the current legal system, electronic data is specified in the 2006 Law on Electronic Transactions. As a source of evidence, electronic data is recorded in the CPrC 2015 of Articles 87, 88, 99, 107. In addition, Clause 3, Article 223 of the CPrC also refers to the "collection of confidential electronic data" as a special method of investigating proceedings. At present, there are no legal documents detailing this issue. Besides the specific provisions on the collection of electronic means, electronic data (Article 107),

other contents such as: inspection, evaluation, preservation, sealing, etc., shall be applied to evidence. Electronics comply with current general regulations. However, electronic evidence with characteristics differ from traditional evidence requires strict legal provisions on the process of seizure and restoration of this type of evidence to protect the integrity of data, maintain the evidence value of the data; as well as regulations on the responsibilities of individuals in the use and preservation of this particular kind of evidence; Especially with regard to "collecting electronic data", it is also related to human rights and civil rights. The lack of specific guidance has led to an arbitrary, similar application by investigating authorities.

In addition, the provisions of the CPrC also reveal inconsistencies, namely: Article 107 of the CPrC 2015 provides for the collection of electronic means and electronic data but in Clause 1 of this law stipulates that "electronic media must be seized promptly and fully…" and "in case electronic storage media cannot be seized, competent authorities shall carry out electronic data backup procedures...". It can be seen that lawmakers seem to agree on the concept of "electronic media collection" and "electronic media seizure"[14]. They only pose a problem for electronic data collection because electronic data is only a source of evidence, and electronic means are only where electronic data is contained.

Secondly, regarding the conditions of facilities, capacity and coordination with agencies and organizations in the inspection and evaluation of electronic evidence: To solve criminal cases with evidence being electronic data, it requires legal proceeders to be knowledgeable about electronic data types and have a certain understanding of information technology. The reality shows that for cases that are not too complicated, such as cases of prostitution, drug trafficking, gambling, subjects often use digital devices to send messages, make phone calls and exchange content together. The collection of electronic data to prove or consolidate evidence is usually at a simple level, after seizing the digital device, the investigating authority shall make a record of checking, extracting and copying data such as messages, call history between subscribers used by the subjects to fight the object (Ngo, 2015). When the subject declares appropriately, a copy of the above data is included in the case file as proof of a crime.

However, in more complex cases, the subject uses more sophisticated tricks, leaving traces of criminals in computer network data, telecommunications networks, transmission lines, and other electronic sources. We must access encrypted

14 *Bài viết một số quy định về chứng cứ trong Bộ luật tố tụng hình sự năm 2015,* available at: *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,* accessed on 28.09.2021.

database sources, block data collection on the transmission line (between server-server, personal-server computer, data transmitted by ADSL, mobile, satellite), decode encrypted data, etc., and must cooperate with professional organizations, experts or competent agencies (third agencies) to conduct the search, recovery, conversion of electronic data into visible form that we can read, listen, look... However, waiting for the results from these agencies is related to the time limit for the procedure. For cases where electronic evidence is the most important basis for determining the criminal acts of the subjects, this greatly affects the progress of the case resolution.

Thus, although the collection of electronic means takes place quickly, promptly and in accordance with the provisions of the Criminal Procedure Code, the law does not strictly stipulate the time limits and responsibilities of third agencies. As there is no coordination mechanism, the use of electronic evidence to solve criminal cases has not been effective.

3. Discussion

The author will show the following some solutions to remove difficulties and obstacles in the work of collecting, inspecting and evaluating electronic evidence in the next time:

Firstly, in terms of legal documents, it is necessary to have clear and specific regulations on the collection, inspection and evaluation of electronic documents as well as the promulgation of guidance documents on the way to deal with High-tech crimes in the 2015 Penal Code, amended in 2017[15]. Also, it is necessary to have strict regulations on responsibilities and even sanctions against individuals and organizations (third agencies) in delaying the provision of electronic data, electronic data expertise affects the resolution of the case.

Secondly, the people conducting legal proceedings need to improve the basic knowledge about electronic data, information technology (certain knowledge about the objects being exploited) ... In order to do that well, it is necessary to determine the direction for the electronic data collection activities that are: (i) Must come from the information, documents and initial evidence on the collected case, this is the first basis to help the competent authority determines the direction for electronic data collection; (ii) Deriving from the rule of electronic traces that are distinct from other criminal traces, based on the origin and characteristics of electronic traces (electronic media, computer networks), telecom

15 Penal Code of the Socialist Republic of Vietnam, No. 100/2015/QH13, dated November 27, 2015

network or online); (iii) The operation rules of the offenders for different systems and types of subjects are different, such as: The operation rules of high technology users violating national security will have unique characteristics compared to the operation rules of information technology-using subjects for fraudulent activities of appropriating property...

Thirdly, it is necessary to have scientific and practical conclusions on the collection, evaluation, and use of electronic evidence in criminal cases. On the other hand, electronic data is a non-traditional source of evidence, exists in cyberspace, that existence can go beyond the scope of a country and the type of crime that leaves this trace is often of nature. substance transnational. Therefore, the competent authority should strengthen international cooperation in combating this type of crime.

It can be said that the legalization of electronic data as a source of evidence in the CPrC 2015, along with the addition of regulations on some new crimes in the field of information technology in the 2015 Penal Code, is a timely and suitable adjustment of lawmakers, meeting the urgent needs of the reality of fighting against high-tech crimes that are increasing in number, complexity, and danger to society (Nguyen, Le, 2016).

4. Conclusion

In summary, compared with the 2003 Criminal Procedure Code, the 2015 Criminal Procedure Code has made important amendments in terms of evidence and proof, making the proceedings faster, more objective and comprehensive, and better protecting human rights through specific regulations, meeting the requirements set out in the 2013 Constitution and the judicial reform strategy up to 2020. In which, the addition of several new sources of evidence, especially data sources. Electronic data is a great step forward, in line with the extremely complex situation of computer crime in practice and also following the international conventions to which Vietnam is a member. However, the regulations on the collection of electronic media and electronic data as well as the method of confidential collection of electronic data still have many limitations and are unclear, making it difficult for the application process, needs to be supplemented and perfected

We thus realize that the mere mention of e-evidence in the statute cannot help the cause. The procedural glitches that have been induced by the inclusion of e-evidences need to be dealt at the earliest. With commuting times, the law needs to keep pace with improvements in technology.

References

- Callanan, C. et al. (2009) *Study on Internet blocking, balancing cybercrime responses in democratic societies*. Aconite Internet Solutions.
- Criminal Procedure Code of the Socialist Republic of Vietnam, No. 101/2015/QH13.
- Law on Electronic Transactions of the Socialist Republic of Vietnam, No. 51/2005/QH11.
- Le, T. T. et al. (2020) Cyber crimes in the banking sector: Case study of Vietnam. *International Journal of Social Science and Economics Invention, 6*(5), pp. 272-277. https://doi.org/10.23958/ijssei/vol06-i05/207
- Ngo,V. B. D. (2015) Obligation of proof in proceedings. *Journal of Legal Studies, 7, pp.* 287
- Nguyen, T. N. Y. (2016) Electronic data as a source of evidence in the criminal process of the Socialist Republic of Vietnam. *Bulletin of Economic Security*, *3*, pp. 315–317.
- Nguyen, V. H., Le, L. C. (2016) *Scientific commentary of the Criminal Procedure Code 2015.* Hanoi: Labor Publishing House.
- *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesfor thesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm, accessed on 05.10.2021.
- Penal Code of the Socialist Republic of Vietnam, No. 100/2015/QH13.
- Prime Ministerial Decree, No. 749 / QDTTg.
- Tran, V. H. (2015) Evidence is electronic data and evidence in the Draft Criminal Procedure Code (amended). *Procuracy Journal, 9,* pp. 67-72.
- Tran, V. L., Phung, T. V. (2018) *Scientific commentary on Criminal Procedure Code 2015.* Hanoi: People's Public Security Publishing House.

Online sources

- *Bài viết một số quy định về chứng cứ trong Bộ luật tố tụng hình sự năm 2015,* available at: *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,* accessed on 28.09.2021.
- *Can the internet keep up with the surge in demand*, available at: *https://blogs.akamai.com/2020/04/can-the-internet-keep-up-with-the-surge-in-demand.html*, accessed on 29.09.2021.
- *Cybercrime To Cost The World $10.5 Trillion Annually By 2025,* available at: *https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, accessed on 04.10.2021.*

- *Global Cybersecurity Index,* available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, accessed on 01.10.2021.
- *Global risks report 2020,* available at: *http://reports.weforum.org/global-risks-report-2020/executive-summary/*, accessed on 02.10.2021.
- *Một số bất cập về chế định chứng cứ trong Bộ luật Tố tụng dân sự năm 2015,* availabe at: *https://tapchitoaan.vn/bai-viet/phap-luat/mot-so-bat-cap-ve-che-dinh-chung-cu-trong-bo-luat-to-tung-dan-su-nam-2015,* accessed on 01.10.2021.
- *The Global Cybersecurity Index (GCI) 2020,* available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, accessed on 02.10.2021
- *The Hidden Costs of Cybercrime*, available at: *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf*, accessed on 05.10.2021.
- *Vietnamese Carders arrested in MattFeuter.ru case,* available at: *https://blogs.msmvps.com/garwarner/2013/06/05/vietnamese-carders-arrested-in-mattfeuter-ru-case/,* accessed on 02.10.2021.