MINISTRY OF EDUCATION AND TRAINING MINISTRY OF JUSTICE
HA NOI LAW UNIVERSITY

NGUYEN QUY KHUYEN

CRIME IN THE FIELD OF INFORMATION TECHNOLOGY, TELECOMMUNICATIONS ETWORKS UNDER THE VIETNAMESE CRIMINAL LAW

SUMMARY OF THE THESIS FOR DOCTOR OF LAW

Hà Nội 2021

MINISTRY OF EDUCATION AND TRAINING MINISTRY OF JUSTICE

HA NOI LAW UNIVERSITY

NGUYEN QUY KHUYEN

CRIME IN THE FIELD OF INFORMATION TECHNOLOGY, TELECOMMUNICATIONS ETWORKS UNDER THE VIETNAMESE CRIMINAL LAW

SUMMARY OF THE THESIS FOR DOCTOR OF LAW

Major : Criminal Law and Criminal Procedure

Code : 9380104

Supervisors : **1. Assoc. Prof. PhD. Cao Thi Oanh**

2. PhD. Le Dang Doanh

Hà Nội 2021

INTRODUCTION

Nowadays, Information technology, Telecommunications networks have been widely applied in all fields of the social life. Along with the development and the popularity of Information technology, Telecommunications networks it is the appearance of criminals in the fields of Information technology, Telecommunications networks. Although the combat against this crime has achieved certain results, it is still limited. This crime was specified in the 1999 Criminal Code, which was amended and supplemented in 2009 and the 2015 Criminal Code. These regulations are increasingly being supplemented and completed, but there are still certain disadvantages and limitations. The practice of applying the provisions of the Criminal Laws on crimes in the fields of Information technology and Telecommunications networks in recent years (2009-2020) has also encountered a number of difficulties and problems. Meanwhile, the number of researches on this crime in recent years is just a few. Therefore, now the request is to continue conducting researches on this crime. That is the reason why the author chose the research topic *"Crime in the field of information technology, telecommunications networks under the Vietnamese Criminal Law"* for the doctoral thesis.

The research purpose of the thesis is to build solutions to improve the efficiency of applying the regulations of Vietnamese Criminal Law on crimes in the fields of Information technology and Telecommunications networks in the upcoming time. The research tasks of the thesis include: (1) studying the theoretical issues about

crime in the fields of Information technology and Telecommunications networks; (2) studying the provisions of international law on criminals in the fields of Information technology and Telecommunications networks; (3) studying the provisions of Vietnamese Criminal Law on crimes in the fields of Information technology and Telecommunications networks; (4) practical research on the application of the Vietnamese regulations of Vietnamese Criminal Law on criminals in the fields of Information technology and Telecommunications networks over the past few years.

The research subject of the Thesis is the domestic and foreign scientific points of view on criminals in the fields of Information technology and Telecommunications networks; regulations and practice of applying Vietnamese regulations of Criminal Laws on criminals in the fields of Information technology and Telecommunications networks; regulations of international legal documents on criminals in the fields of Information technology and Telecommunications networks.

The research scope of the Thesis in the perspective of Criminal Law is in the major of Criminal Law and Criminal Procedure. The practice of applying regulations of Criminal Laws criminals in the fields of Information technology and Telecommunications networks is the practice of the Court nationwide in the period from 2009 to 2020.

The research results of the Thesis will contribute new content in theory and practice as follows:

Firstly, building and perfecting the theoretical system of crimes in the field of information technology and

telecommunications networks such as crime concepts, characteristics and classification.

Secondly, analyzing the legal signs and punishments of crimes in the field of information technology and telecommunications networks in accordance with the 2015 Criminal Code.

Thirdly, summarizing and assessing the practice of applying provisions of the Criminal Law on crimes in the field of information technology and telecommunications networks in the period of 2009 - 2020.

Fourthly, proposing a number of solutions to improve the application efficiency of the 2015 Criminal Code provisions on this crime in the upcoming time.

Regarding the structure, in addition to the introduction, the overview of the research issue, the conclusion, the list of references and appendices, the content of the thesis is structured into 3 chapters as follows:

Chapter 1. General issues of the crime in the field of information technology and telecommunications networks.

Chapter 2. Regulations of Vietnamese Criminal law on crime in the field of information technology and telecommunications networks.

Chapter 3. Practical application and solutions to improve the effectiveness of the application of the provisions of Vietnamese Criminal law on crime in the field of information technology and telecommunications networks.

CHAPTER 1.
GENERAL ISSUES OF THE CRIME IN THE FIELD OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS NETWORKS

1.1. Theoretical issues of crime in the field of information technology and telecommunications networks

1.1.1. Crime concept in the field of information technology, telecommunications networks

Cyber environment is the artificial environment created from the connection of information technology infrastructure, in which information and data are provided, transmitted, collected, processed, stored and exchanged; which is the place where humans, through communication tools and techniques, interact with each other without being limited by space and time.

In cyber environment, with technical tools, humans can interact with each other and carry out activities according to their purposes, so humans might commit crimes in that environment as well. Crime committed in cyber environment, using information technology and telecommunications networks to commit crimes or directly attack on cyberspace, is known as information technology and telecommunications networks related crimes. However, currently, there are still many different views on the conceptual connotation, as well as the name of this crime. It can be understood that criminals related to information technology and telecommunications networks are dangerous for the society specified in the Criminal Laws, performed by the person with the criminal responsibility and capacity

using information technology and telecommunications networks with intentional errors, to violate the social relationships which is protected by the Criminal Laws. Crime related to information technology and telecommunications networks has the following characteristics: (1) it is a new crime compared to a traditional crime; (2) information technology and telecommunications networks are criminal-related in one of their roles as a target of a criminal's attack or as a tool to commit another crime; (3) the scope of crime related to information technology and telecommunications networks is very wide.

Crimes in the fields of information technology and telecommunications networks is one of those crimes related to information technology and telecommunications networks. Crime in the fields of information technology and telecommunications networks has a narrower scope than crimes related to information technology and telecommunications networks. Accordingly, crimes in the fields of information technology and telecommunications networks only include criminal acts that violate on social relations to ensure the safety of computer networks, telecommunications networks, electronic means, and electronic data which is called crimes in the fields of information technology and telecommunications networks. And crimes which criminals use information technology and telecommunications networks to commit crimes but violate other social relations groups will not be crimes in the fields of information technology and telecommunications networks. Therefore, the concept of crimes in the fields of

information technology and telecommunications networks can be drawn as follows:

Crime in the fields of information technology and telecommunications networks is the dangerous behavior to society specified in the Criminal Code, performed by the person with the criminal responsibility and capacity using information technology and telecommunications networks with intentional errors, to violate the safety of computer networks, telecommunications networks, electronic means, and electronic data.

1.1.2. Characteristics of crimes in the field of information technology and telecommunications networks

Crimes in the field of information technology and telecommunications networks has the following basic characteristics:

Firstly, criminals use information technology and telecommunications networks as the tool, means to commit crimes in the field of information technology and telecommunications networks has the following basic characteristics

Secondly, criminals' objective behaviors in the field of information technology and telecommunications networks are very diverse and complex with sophisticated tricks that are constantly changing according to the development and application of information technology and telecommunications networks in real life.

Thirdly, the consequences of the crime are often very serious but easy to hide and hard to detect.

Fourthly, crimes in the field of information technology and telecommunications networks are carried out without limitation in space and time.

Fifthly, criminal offenders are usually people with knowledge of information technology and telecommunications networks and related to foreign countries.

Sixthly, crime is committed with intentional error.

Seventhly, the object of crime is social relations to ensure safety of computer networks, telecommunications networks, electronic means and electronic data violated by this crime.

1.1.3. Crime classification in the field of information technology and telecommunications networks

There are many different ways of classifying crimes in the field of information technology and telecommunications networks. Depending on different purposes, there will be different classification criteria. Specifically:

(1) On the basis of the nature and level of danger to society of the criminal acts specified in the Criminal Laws, crimes in the field of information technology and telecommunications networks is divided into 04 categories: less serious crime, serious crime, very serious crime and extremely serious crime.

(2) On the basis of the role of information technology and telecommunications networks for crimes in the field of information technology and telecommunications networks, this crime can be divided into two categories: Firstly, crimes in the field of information technology and telecommunications networks, in which computer networks, telecommunications networks, electronic means, and electronic data are the targets of criminals' attacks. Secondly, crimes in the field of information technology and telecommunications networks, in which offenders use information technology and

telecommunications networks to commit criminal acts, violating the interests of agencies, organizations, legitimate rights and interests of individuals in cyberspace environment.

(3) On the basis of the role of information technology and telecommunications networks and criminal purposes, crimes in the field of information technology and telecommunications networks is divided into 4 groups: Firstly, crimes in the field of information technology and telecommunications networks has the purpose of violating on integrity, confidentiality or availability of computer networks, telecommunications networks, electronic means, electronic data. Secondly, crimes in the field of information technology and telecommunications networks in which criminals have the purpose of appropriating property. Thirdly, crimes in the field of information technology and telecommunications networks, in which criminals use information technology and telecommunications networks to violate on the rights and interests of agencies, organizations and individuals. Fourthly, crimes in the field of information technology and telecommunications networks, in which criminals use information technology and telecommunications networks to violate safety and order in the field of radio frequency.

1.1.4. The basis and significance of the regulations on crimes in the field of information technology and telecommunications networks in the Criminal Code

The theoretical and practical basis of the regulations on crimes in the field of information technology and telecommunications networks in the Criminal Code is that we have enough conditions to describe this crime; the criminal act is

significantly dangerous to the society; the criminal act is very common in the society.

The regulations on crimes in the field of information technology and telecommunications networks in the Criminal Code have met the requirements of crime fighting and prevention; protecting the social order and safety, the legitimate rights and interests of organizations and individuals; solving current issues and problems; aligning with the trend of foreign countries around the world and the provisions of international law on crimes in the field of information technology and telecommunications networks.

1.2. International law on crimes in the field of information technology and telecommunications networks

1.2.1. Council of Europe Convention on Cybercrime (2001)

According to the 2001 Budapest Convention, cybercriminals are divided into the following four groups:

- Group of crimes violating on confidentiality, integrity and availability of computer data and computer system includes: illegal access; illegal prevention; disrupting computer data; disrupting the system; misuse of equipment;

- Group of crimes related to computers includes: computer-related forgery crimes; computer-related fraud;

- Group of crimes related to the contents includes: crimes related to child pornography; crimes of racism or xenophobia through the computer system;

- Group of crimes of violation of copyright and related rights.

1.2.2. Model Laws of Computer Crime and Computers related Crime of the Commonwealth of Nations (2002)

The Model Law in 2002 does not provide for the concept of computer crimes and computers related crimes , but only specifies the following crimes: illegal access; disrupting computer data; disrupting the system; illegal data prevention; misuse of tools and equipment related to computers; crime related to child pornography;

1.2.3. Conventions of African countries on cybersecurity and the protection of personal data (2014)

Accordingly, cybercrime includes the following crimes:

- *Crimes which attack on computer systems include:* Illegally accessing or intentionally accessing a part or the whole of a computer system or exceeding the authority to access; Accessing or intentionally illegal access to part or all of a computer system or beyond the authority to access with the intention of committing another crime or preparing to commit another crime; Cheating to maintain or intentionally maintain access to part or all of a computer system; Concealing, falsifying or intentionally hiding or falsifying the functions of the computer system; Entering or intentionally entering fake data into the computer system; Destroy or intentionally destroy; Delete or intentionally delete; Damage or intentionally damage; Replacement or intentional replacement; Fraudulently altering or intentionally altering computer data;

- *Crimes of damaging computer data, including the following crimes:* Blocking or intentionally unauthorized blocking computer data by technical measures during data transmission (not publicly) to the computer system, from the computer system or by the computer system; Deliberately inserting, replacing, deleting or intercepting computer data to create fake data, then intentionally using this fake

data as real data; Using data that is well aware of it being collected falsely from a computer system; Fraudulent trading for oneself or for others any benefit by adding, replacing, deleting or intercepting computer data or any act of interfering with the function of a computer system; Intentionally or unintentionally not following proper procedures in handling personal data; Joining or establishing a criminal organization to prepare or to commit one or more of the crimes regulated by this Convention.

- *Crimes related to the contents of information technology and telecommunications networks:* Producing, registering, proposing, providing, distributing and transmitting child pornographic images or performances through a computer system; Buying and selling for oneself or for others, importing or already imported; exporting or already exported child pornographic images or performances through a computer system; Possessing a child pornographic image or representation in a computer system or on a medium containing computer data; Facilitating or providing access to data that contains images, material, sounds or performances about child pornography; Creating, downloading, distributing or making available regardless of written material, text messages, pictures, drawings or other representations of racist or racist ideology or doctrine through a computer system; Through computer systems, threatening to commit crimes against others because of race, color, origin, nationality or religion or belief; Through computer systems, insulting others by reason of race, color, origin, nationality or religion or belief; Through the computer network, accepting, encouraging or justifying genocide or crimes against humanity

- *Crimes about property related to information technology and telecommunications networks (Clause 1, Article 30)*: That is the crime of using information technology and telecommunications networks to commit property theft, fraud, consume property theft, abuse of trust, blackmail, terrorism and money laundering.

1.2.4. Arab Nations Convention against Information Technology Crime

Criminal acts are defined by the Convention from Articles 6 to 18, including: crime of illegal access (Article 6); crime of illegal intervention (Article 7); Crime of infringing upon the integrity of data (Article 8); crime of misusing tools and software used to commit crimes (Article 9); crime of forgery (Article 10); fraudulent crimes (Article 11); crime of child pornography (Article 12); gambling crimes and sexual exploitation through the use of information technology and telecommunications networks (Article 13); privacy violations (Article 14); terrorism crimes through information technology and telecommunications networks (Article 15); related crimes such as money laundering, drug trafficking, human trafficking, organizing human trafficking, arms trafficking (Article 16); Crime of copyrights and related rights (Article 17); crime of illegal use of electronic payment instruments (Article 18).

CHAPTER 2.
REGULATIONS OF VIETNAMESE CRIMINAL LAW ON CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS NETWORKS

2.1. Overview of the legislative history of crime in the field of information technology, telecommunications networks

2.1.1. The Period from 2010 onwards

The 1985 Criminal Code did not have any regulations on crime in the field of information technology, telecommunications networks. Crime in the field of information technology, telecommunications networks was first regulated in the 1999 Criminal Code, including 3 articles: Article 224 (Crime of creating and spreading computer virus programs), Article 225 (Crime of violating the regulations on operation, exploitation and use of electronic computer networks) and Article 226 (Crime of illegally using information on the network and inside the computers).

2.1.2. The Period from 2010 to 2017

After 10 years of implementation, the regulations on crime in the field of information technology, telecommunications networks in the 1999 Criminal Code were amended and supplemented gradually. Specifically:

- Adding 2 new articles, Article 226a (Illegal access to computer networks, telecommunications networks, Internet or digital devices of others) and Article 226b (Crime of using computer networks, telecommunications networks, Internet or digital equipment to misappropriate property).

- Amending Article 224, Article 225 and Article 226 towards the direction of making the articles more specific and clear, adding the aggravation of a number of framing details.

Although the crime in the field of information technology, telecommunications networks was specified in the 1999 Criminal Code and amended and supplemented in 2009, but these provisions still have certain limitations. In particular, the newly emerging criminal tricks (negative consequences of the development in the field of information technology, telecommunications networks) raise the issue of further amendment and completion of the Criminal Laws's regulations on crimes in the field of information technology, telecommunications networks. That is the reason why the 2015 Criminal Code in 2015 made significant amendments and supplements to criminal regulations in the field of information technology, telecommunications networks compared to the 1999 Criminal Code.

2.2. Crime in the field of information technology and telecommunications networks in accordance with the regulations of the 2015 Criminal Code

2.2.1. The elements of crimes in the field of information technology, telecommunications networks

2.2.1.1. Objective side of crime in the field of information technology, telecommunications networks

** Group 1: Objective side of crimes violating the integrity, confidentiality or availability of electronic data, computer networks, telecommunications networks, electronic means*

(1) Crime of manufacturing, buying, selling, exchanging, giving tools, equipment and software for illegal use (Article 285):

Objective behaviour of the crime is the producing, buying, selling, exchanging, giving tools, equipment or software with the ability to attack computer networks, telecommunications networks or electronic means for illegal purposes of use. Subjects affected by the crime are tools, equipment or software with the ability to attack computer networks, telecommunications networks or electronic means.

(2) Crime of spreading informatics programs harmful to computer networks, telecommunications networks, electronic devices (Article 286):

Objective behaviour of the crime is the spreading informatics programs harmful to operation of computer networks, telecommunications networks or electronic means. The object of the behaviour of distribution is information technology programs with harmful features. Acts of distributing computer programs with harmful features to the operation of computer networks, telecommunications networks, and electronic devices shall be considered a crime in the following cases: (1) illegally earning profits from 50 million VND or above; (2) causing a loss of from 50 million VND or above; (3) infecting 50 or more electronic means or an information system that has 50 or more users; (4) has been administratively sanctioned for this act or has been convicted of such crime, the criminal record has not been removed and the act of distributing a harmful computer program.

(3) Crime of obstructing or disrupting operation of computer networks, telecommunications networks or electronic means (Article 287):

Objective behaviour of the crime of obstructing or disrupting operation of computer networks, telecommunications networks or electronic means includes 3 following groups: acts of arbitrarily deleting, damaging or altering software, electrical data; acts of illegally preventing data transmission by computer networks, telecommunications networks or electronic devices; other acts that disrupt the operation of computer networks, telecommunications networks or electronic devices.

Subjects affected by the crime of obstructing or disrupting the operation of computer networks, telecommunications networks and electronic means include: (1) Electronic software and data; (2) Computer networks, telecommunications networks information, electronic devices.

All the above acts are considered crimes if they belong to one of the following cases: (1) Gaining illicit profits from 50 million VND or more; (2) Causing a loss of 100,000,000 VND or more; (3) Paralyzing, interrupting or stopping the operation of computer networks, telecommunications networks, electronic media for 30 minutes or more or 03 times or more within 24 hours (the case may stop delay the operation of computer networks, telecommunications networks, electronic means for less than 30 minutes each time but do so many times, from 3 to 10 times a day); (4) Delaying the operation of agencies or organizations for 24 hours or more (may be the case of stopping the operation of computer networks, telecommunications networks, electronic media for less than 30 minutes and less than 3 times within 24 hours, but in order to troubleshoot the agency or organization must delay operation for 24 hours or more); (5) Having been administratively sanctioned for this act or having been

convicted of this offense, the criminal record has not been removed but also commit.

(4) Illegally breaking into computer networks, telecommunications networks or electronic devices of other people (Article 289):

Objective behaviour of the crime of accessing computer networks, telecommunications networks or electronic means without consent of the owner or operator of the computer network, telecommunications network, or that electronic devices. These acts are performed through tricks such as: (1) Passing the warning means passing a notification that does not allow unauthorized people to access the database; (2) Passing an access code means passing the required conditions that meet a certain standard before using, accessing the protected device, data content; (3) Bypassing a firewall for unauthorized intrusion, in which a firewall is a collection of components or a system of equipment, software or hardware placed between two or more networks to control all of the connections from the inside to the outside and vice versa, at the same time preventing unauthorized access and connection; (4) Using the administrative rights of others is means using the right to manage, operate, exploit and maintain the stable operation of computer networks, telecommunications networks of individuals and organizations; (5) Other methods of unauthorized access such as cracking, theft of passwords, passwords of others for unauthorized or physical intrusion such as unlocking the door to the room, the unauthorized area to get access to computer networks, telecommunications networks, electronic media ...

After illegally getting access to computer networks, telecommunications networks or electronic means of other people, criminals carry out one of the following activities: (1) hijacking computer networks, telecommunications networks, electronic means; (2) interfering with the functioning of electronic means; (3) stealing electronic data; (4) altering or destroying electronic data; (5) falsify electronic data; (6) unauthorized use of the services.

** Group 2: Objective side of crimes in the fields of information technology and telecommunications networks to violate on the ownership of others people:*

This group only has the crime of illegally using computer networks, telecommunications networks, electronic means to appropriate property (Article 290). Objective behaviour of the crime is the act of using computer networks, telecommunications networks or electronic means to appropriate property of other people in one of the following cases:

Firstly, using information about accounts, bank cards of agencies, organizations or individuals to appropriate the properties of card owers, account owers or to pay for services or purchase goods.

Secondly, making, storing, buying, selling, using, circulating fake bank cards to misappropriate the property of the account owers, card owers or pay for goods or services.

Thirdly, illegal access to the accounts of agencies, organizations or individuals in order to appropriate property.

Fourthly, fraud in e-commerce, electronic payment, currency trading, capital mobilization, multi-level business or online securities transactions to appropriate property.

Fifthly, illegally establishing and supplying telecommunications and internet services in order to appropriate property.

** Group 3: Objective side of crimes of violating the rights and interests of organizations and individuals in the fields of information technology and telecommunications networks:*

(1) Illegally uploading or using information on computer networks or telecommunications networks (Article 288):

Crime is committed through one of the following objective acts:

Firstly, uploading on computer networks and telecommunications networks the information which is contrary to law, except for the cases specified in Articles 117, 155, 156 and 326 of the Criminal Laws in 2015. Subjects affected of the crime are the information contrary to the provisions of the law.

Secondly, buying, selling, exchanging, giving, repairing, changing or publicizing legal private information of agencies, organizations or individuals on computer networks, telecommunications networks without permission of owners or person in charge of that information. Subjects affected by the crime are "legal private information of agencies, organizations or individuals".

Thirdly, other acts of illegally using information on computer networks or telecommunications networks.

All the above acts are considered crimes if they belong to the cases of illegally gaining profits of 50 million VND or more or causing damage of 100 million VND or more or causing bad public

opinion, reducing the reputation of agencies, organizations, individuals.

(2) Crime of illegally collecting, possessing, exchanging, trading, disclosing information about bank account (Article 291):

Objective behaviour of the crime is one of the acts of illegally collecting, possessing, exchanging, trading, and disclosing information about bank account of other people. The subject of the crime is "bank account information".

All the above acts are considered crimes if they belong to one of two cases as follows: (1) illegally collecting, possessing, exchanging, purchasing, selling, disclosing 20 or more accounts; (2) Illegally collecting, possessing, exchanging, trading, publicizing less than 20 accounts but the offender has illegally earned 20 million VND or more.

** Group 4: Objective side of crimes violating the safety and order in the field of radio frequencies:*

(1) Illegally using radio frequencies exclusively for purposes of emergency, safety, searching, rescuing, saving, defense and homeland security (Article 293):

Objective behaviour of the crime is illegally using radio frequencies exclusively for purposes of searching, rescuing, saving, defense and homeland security for other purposes. The subject of the crime is radio frequencies reserved for purposes of searching, rescuing, saving, defense and homeland security.

The act of illegally using radio frequencies exclusively for purposes of searching, rescuing, saving, defense and homeland security is considered crimes when causing damage of at least 200 million VND or more or have been administratively sanctioned for

this act or have been convicted for this offense, the criminal record has not been removed but also violate.

(2) Crime of intentionally causing harmful interference (Article 294):

Objective behaviour of the crime is causing harmful interference. The act of causing harmful interference is considered crimes if they cause damage of 200 million VND or more or have been administratively sanctioned for such acts or have been convicted of this crime, their criminal records have not been removed but also violate.

2.2.1.2. Subjects of the crime in the field of information technology and telecommunications networks

According to the Article 12 of the 2015 Criminal Code, the people with 16 years or older, who does not lose the ability to perceive or control acts, is subject to criminal responsibility for all crimes. Therefore, these people can be the subject of all the criminals in the field of information technology and telecommunications networks. For people from 14 years old to under 16 years old, are subject to criminal responsibility for crimes in the field of information technology and telecommunications networks, specified in clause 3 Article 286, clause 3 Article 287, clause 3 Article 289 and clause 3, 4 Article 290 of the 2015 Criminal Code.

2.2.1.3. Subjective side of the crime in the field of information technology, telecommunications networks

Criminals in the field of information technology and telecommunications networks are all intentional errors, without unintentional errors. Crime can be committed with direct or indirect intentional error.

Criminal intent is a mandatory sign for a number of criminals in the field of information technology and telecommunications networks.

2.2.2. Penalties for crimes in the field of information technology, telecommunications networks according to the 2015 Criminal Code

2.2.2.1. Type and level of penalties for crimes in the field of information technology and telecommunications networks

- The main penalties applied to crimes in the field of information technology and telecommunications networks include: fine, non-custodial reform, term imprisonment.

- Additional penalties that can be imposed on crimes in the field of information technology and telecommunications networks include: Penalties for prohibiting holding certain positions, prohibiting practicing certain occupations or doing certain jobs; penalty for confiscation of part or all of the property.

2.2.2.2. Framing signs of the crime in the field of information technology and telecommunications networks

The signs of aggravating the framework of crimes in the field of information technology and telecommunications networks in accordance with the Criminal Laws in 2015 include many different signs, but can be divided into the following 4 groups:

Firstly, framing signs related to criminal acts, including signs that increase the social danger of criminals such as: (1) organized crime, (2) committing crimes two times or more, (3) committing crimes with a professional nature.

Secondly, framing signs related to the consequences of the crime include: (1) Aggravating signs that reflect the consequences are

the change in the normal functioning of the agency, organization, and the normal behavior of the individual; (2) aggravating framing signs that reflect the consequences of damage to the safety of computer networks, telecommunications networks, electronic means, and electronic data; (3) Aggravating markings reflect the number of users, the number of electronic media affected by the number of vehicles or by the number of users of that vehicle; (4) Aggravating signs that reflect damages are material benefits destroyed, damaged, or lost due to criminal acts in the the field of information technology and telecommunications networks and is attributed to a certain amount of money. ; (5) Aggravating signs that reflect the damage are revenue, illicit benefits or the amount the criminal has taken.

Thirdly, framing signs relating to the relavtives of the criminal include: (1) dangerous recidivism; (2) taking advantage of rights to administer computer networks, telecommunications networks; (3) abusing positions and powers.

Fourthly, framing signs related to the subject of the crime: (1) data system belonging to government secrets; (2) information systems serving national defense and security; (3) national information infrastructure; (4) national grid operator information system; (5) financial and banking information systems; (6) traffic control information system; (7) the national internet transit station, the domain name database system and the national domain name server system.

CHAPTER 3.
PRACTICAL APPLICATION AND SOLUTIONS TO IMPROVE THE EFFECTIVENESS OF THE APPLICATION OF THE PROVISIONS OF VIETNAMESE CRIMINAL LAW ON CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS NETWORKS

3.1. Practical application of Vietnamese Criminal Laws on crimes in the field of information technology and telecommunications networks

3.1.1. Achievements in the application of the Criminal Laws on crimes in the field of information technology and telecommunications networks

In the period of 2009 - 2020, The Courts throughout the country have proceed instance trials for 445 cases with 933 defendants of crimes in the field of information technology and telecommunications networks.

In the process of applying the regulations of the Criminal Laws on crimes in the field of information technology and telecommunications networks, the Court has tried to improve the efficiency of solving cases. Despite many difficulties, the rate of solving cases achieved 82.4% in the period of 2009 - 2020.

During the Court's trial, a number of laws were regularly applied. In contrast, some regulations have not been applied or are rarely applied.

The decision on punishment for crimes in the field of information technology and telecommunications networks: the majority of defendants are subject to imprisonment penalty. The common imprisonment penalty is 3 years or less. In particular, the Court gave suspended sentences with a very high rate, accounting for 21.6% of the total number of defendants. Additional penalties are less applicable.

Foreigners committing crimes in the field of information technology and telecommunications networks in Vietnam account for a high rate.

3.1.2. Limitations, difficulties and issues in the practice of applying the provisions of the Criminal Laws on crimes in information technology and telecommunications networks

In the process of implementation from 2009 to 2020, some of the following limitations, difficulties and problems have occured:

Firstly, although there are provisions of the Criminal Laws in the field of information technology and telecommunications networks and the fact that this type of crime is also quite common, the authorities cannot handle or handle a limited number of cases.

Secondly, in many cases, legal proceedings agencies applied the regulations of the Criminal Laws on crimes in the field of information technology and telecommunications networks has not yet reached agreement.

Thirdly, authorized agencies have difficulty handling new criminal acts and tricks in the field of information technology and telecommunications networks.

Fourthly, legal proceedings agencies still mistakenly charge crimes in the field of information technology and telecommunications networks.

Fifthly, the decision on penalties for criminals in the field of information technology and telecommunications networks is still inaccurate and inconsistent.

Sixthly, legal proceedings agencies will face difficulties when dealing with cases related to foreigners.

3.1.3. The causes of limitations, difficulties and issues in the practice of applying the provisions of the Criminal Laws on crimes in information technology and telecommunications networks

3.1.3.1. The causes of limitations and issues in the provisions of the Criminal Code on crimes in information technology and telecommunications networks

Firstly, the Criminal Code lack of specific provisions to handle newly arising criminal tricks, while the amendment and supplementation of provisions of the Criminal Code has not been timely;

Secondly, provisions of the Criminal Code are still general, not specific, causing confusion in the application process;

Thirdly, there are many crimes that define the consequences of the crime as a mandatory sign in the composition of the basic crime, while the consequences of this crime are difficult to determine, leading to a number of laws that are less applicable or not applied used to handle these crimes that have happened in practice;

Fourthly, some specific provisions of the 2015 Criminal Code on crimes in the field of information technology and telecommunications networks are still inadequate and limited, so it has or will cause difficulties in the application process;

Fifthly, Legislative techniques of the Criminal Code are not reasonable, causing confusion and misunderstanding when applying some laws.

3.1.3.2. The causes of delay, lack of explanation and guidance from competent authorities to apply the regulations of the Criminal Code on crime in the field of information technology and telecommunications networks

Crimes in the field of information technology and telecommunications networks is the new type of crime related to specialized technical fields, so it is difficult to understand for the majority of people applying the law. Moreover, in fact, the provisions of the Criminal Laws are still general, many contents are not specific. Therefore, the explanation and guidance on the application of the Criminal Laws plays a very important role. However, in recent years, this work has been slow, causing difficulties for the legal proceedings agencies.

3.1.3.3 The causes of limitations in the organization and implementation of the provisions of the Criminal Laws on crimes in information technology and telecommunications networks

Firstly, the human resources for fighting and preventing crimes in the field of information technology and telecommunications networks are still limited.

Secondly, investing in equipment and facilities to fight crimes in the field of information technology and telecommunications networks has not met the requirements.

Thirdly, international cooperation activities in the fighting and prevention of crimes in the field of information technology and telecommunications networks have not been given adequate attention.

3.2. Solutions to improve efficiency of the application of the Criminal Laws on crimes in the field of information technology and telecommunications networks

3.2.1. Solutions to improving the provisions of the 2015 Criminal Code on crimes in the field of information technology and telecommunications networks

Firstly, additional regulating the acts of "possessing, owning for others to use" and "requesting others to use, import" tools, equipment and software to use for criminal purposes in Article 285 (Crime of manufacturing, buying, selling, exchanging or giving tools, equipment or software for illegal use).

Secondly, amending and supplementing the provisions on basic criminal constituents of a number of specific crimes as follows:

First, regarding the Article 286 (Crime of spreading informatics programs that causes harm to the operation of computer networks, telecommunications networks, electronic means), adding a sign that the subject of the crime is “the data system of the government secrets; information system for national defense and security” constitutes the basic component in Clause 1 and the aggravating component in Clause 3.

Second, regarding the Article 287 (Crime of obstructing or disrupting the operation of computer networks, telecommunications networks, electronic means), adding the following objects to the basic components of Clause 1: (1) data system belonging to the government secrets; information systems serving national defense and security; (2) national information infrastructure; information system operating the national grid; financial and banking information system; traffic control information system.

Third, regarding the Article 288 (Crime of illegally putting or using information on computer networks, telecommunications networks), adding the object of "information causing great harm to society" to the basic constituent of the crime. Accordingly, criminal acts, even though they have not caused damage, have not caused bad public opinion, reduce the reputation of agencies, organizations or individuals or have not gained illicit benefits, but for "information causing great harm to society" will be considered a completed crime.

Thirdly, amending inadequacies in the number of articles of the 2015 Criminal Code on crimes in the field of information technology and telecommunications networks:

(1) For Crime of manufacturing, buying, selling, exchanging or giving tools, equipment or software for illegal use (Article 285):

First, replacing the phrase "illegal purposes" in the name of the article and Clause 1 with the phrase "criminal purpose" to narrow the handling scope of this law.

Second, removing the signs of aggravation of the frame specified at Point dd, Clause 2 and Point b, Clause 3, Article 285 of

the 2015 Criminal Code in 2015 (causing property damage of 100 million VND or more).

Third, supplementing the provisions of criminal liability prosecution for commercial legal entities.

(2) For Crime of obstructing or disrupting the operation of computer networks, telecommunications networks, electronic devices (Article 287), amending some of the following contents::

First, correcting the name of the crime of Article 287 into: "Crime of obstructing or disrupting the operation of computer networks, telecommunications networks, electronic means or electronic data"

Second, amending Point e Clause 2 of Article 287 and Point d Clause 3 of Article 287. Specifically:

+ Regarding the Point e Clause 2 of Article 287 "*Paralyzing, interrupting or stopping the operation of computer networks, telecommunications networks, electronic means from 24 hours to 168 hours or from 10 times to 50 times within 24 hours",* will be amended into: "*Paralyzing, interrupting or stopping the operation of computer networks, telecommunications networks, electronic means from 24 hours to 168 hours or from 10 times to 50 times from 24 hours to 168 hours".*

+ Regarding the Point d Clause 3 of Article 287, "*Paralyzing, interrupting or stopping the operation of computer networks, telecommunications networks or electronic means for 168 hours or more or 50 times or more within 24 hours",* same as above will be amended into: "*Paralyzing, interrupting or stopping the operation of computer networks, telecommunications networks or electronic*

means for 168 hours or more or 50 times or more for more than 168 hours".

(3) For Crime of illegally uploading or using information on computer networks or telecommunications networks (Article 288), amending the following contents:

Adding signs of aggravation to frame "dangerous recidivism" to Point h, Clause 2, Article 288 of the 2015 Criminal Code.

(4) For Crime of using computer networks, telecommunications networks or electronic means of appropriating property (Article 290), amending the following contents:

First, amending Clause 1, Article 290 in the direction of removing the phrase "if not belong to the cases specified in Articles 173 and 174 of this Law" (the 2015 Criminal Code).

Second, amending to increase the highest level of the penalty frame to life imprisonment for the offense of using computer networks, telecommunications networks, electronic means to appropriate property.

3.2.2. Solutions for explaining and guiding the application of the provisions of the Criminal Code on crimes in information technology and telecommunications networks

** Some terms in the 2015 Criminal Code are explained as follows:*

First, "Tools, equipment and software with the ability to attack computer networks, telecommunications networks, electronic means" in Clause 1, Article 285 are understood as tools, hardware equipment or computer programs, which are designed or improved to have the basic function of penetrating, obstructing or disrupting the

operation of computer networks, telecommunications networks, electronic means or collecting or falsifying electronic information or data.

Second, "Legal private information of agencies, organizations and individuals" in Clause 1, Article 288 of the 2015 Criminal Code is electronic data, attached to each agency, organization or individual but is not disclosed or only disclose for one or a group of objects that have been identified, with specific addresses.

Third, "Causing bad public opinion" in Clause 1 of Article 288 is causing the majority of negative comments, disparaging or proscribing against agencies, organizations, and individuals to reduce the reputation of agencies and organizations and individuals.

Fourth, "Leading to demonstrations" at Point g, Clause 2, Article 288 of the Criminal Laws in 2015 is leading to a large gathering of people to express their will, aspirations or show their common force.

** Guidance to distinguish confusing cases of criminal convictions:*

First, distinguishing the cases specified in Article 286, Article 287 and Article 289 of the 2015 Criminal Code.

Second, distinguishing the cases specified in Article 290 and Article 173 and Article 174 of the 2015 Criminal Code.

3.2.3. Solutions to perfecting and renovating the organization and implementation of the Criminal Laws on crimes in information technology and telecommunications networks

** Solutions to improve the professional qualifications and capabilities of procedure-conducting people:*

First, raising awareness of officers of legal proceedings about criminal justice in general, especially criminals in the field of information technology and telecommunications networks.

Second, actively training and raising knowledge of information technology and telecommunications networks, legal for procedure-conducting people.

Third, regularly training and disseminating experience fighting against criminals in the field of information technology and telecommunications networks.

Fourth, arranging officers of investigators, procurators, judges with qualifications and experience fighting crime in the field of information technology and telecommunications networks to solve cases.

** Solutions to increase investment in facilities, technical equipment to fight crime in the field of information technology and telecommunications networks:*

Investment in equipping the functional forces with the most modern tools and means to detect and fight against this type of crime. In order to get the most modern equipment, the functional forces not only buy the software available on the market, but depending on the purpose of use can order for technology companies to design and write specialized software.

** Solutions on international cooperation in combating crime in the field of information technology and telecommunications networks:*

First, signing and implementing international conventions to perfect the legal system on crime prevention in the field of information technology and telecommunications networks.

Second, cooperating with other countries to provide mutual legal assistance when investigating, prosecuting and adjudicating criminal cases in the field of information technology and telecommunications networks.

Third, cooperating with other countries and international organizations in providing information and learning experiences in the fight against crime in the field of information technology and telecommunications networks through the organization of international conferences and seminars.

GENERAL CONCLUSION

The thesis has solved the following issues:

Firstly, the Thesis has outlined both domestic and international research studies on the crimes in the field of information technology and telecommunications networks .

Secondly, the Thesis has built and completed a system of theories about the crimes in the field of information technology and telecommunications networks . In which:

Criminals in the field of information technology and telecommunications networks with dangerous behaviors to the society are specified in the Criminal Code, performed by a person with the criminal liability ability to use information technology and telecommunications networks with intentional errors, violating the safety of computer networks, telecommunications networks , electronic media, electronic data.

Criminals in the field of information technology and telecommunications networks have basic characteristics such as: (1) Offenders use information technology and telecommunications networks as tools and means to commit crimes in the field of information technology and telecommunications networks; (2) Criminals' objective behavior in the field of information technology and telecommunications networks is very diverse and complex with sophisticated tricks, which are constantly changing according to the development and application of information technology and telecommunications networks in life; (3) Consequences of crime in the field of information technology and telecommunications networks

are often very serious but easy to conceal and difficult to detect; (4) Crime is committed without limitation by space and time; (5) The subject of the crime is usually someone with knowledge of information technology and telecommunications networks and related to foreign countries; (6) Crime is committed with intentional error; (7) The object of crimes in the field of information technology and telecommunications networks is a social relationship to ensure the safety of computer networks, telecommunications networks, electronic means, electronic data violated by this crime.

The crime classification in the field of information technology and telecommunications networks can be based on different criteria such as: (1) based on the nature and level of danger to the society of the crime; (2) relying on the role of information technology and telecommunications networks to the crime; (3) based on the role of information technology and telecommunications networks and criminal purpose.

Thirdly, the Thesis has researched quite fully international legal documents on crimes in the field of information technology and telecommunications networks such as the Budapest Convention in 2001, the Model Law in 2002, …

Fourthly, the Thesis has analyzed and evaluated the regulations of Vietnamese Criminal Laws on crimes in the field of information technology and telecommunications networks. The contents of the regulations of Vietnamese Criminal Laws have been gradually built up and completed in accordance with international documents. However, there are still contents that need further research and completion. In the process of applying the regulations of

Vietnamese Criminal Laws on criminals in the field of information technology and telecommunications networks, difficulties still arise. The cause of the difficulties and problems is that the regulations of Vietnamese Criminal Laws are still inadequate; the explanation and guidance on the application of the regulations of Vietnamese Criminal Laws is insufficient and delayed; the organization and implementation of the regulations of Vietnamese Criminal Laws have not been very effective.

Fifthly, The thesis has built groups of solutions to improve the effectiveness of the application of the regulations of Vietnamese Criminal Laws on criminals in the field of information technology and telecommunications networks in the upcoming time as a group of solutions to complete the regulations of Vietnamese 2015 Criminal Code on criminals in the field of information technology and telecommunications networks; solutions to explain and guide the application of Vietnamese Criminal Laws on criminals in the field of information technology and telecommunications networks; group of solutions for organizational innovation, implementing Vietnamese Criminal Laws on criminals in the field of information technology and telecommunications networks.

AUTHOR'S SCIENTIFIC RESEARCH WORKS PUBLISHED RELATED TO THE THESIS'S SUBJECT

1. Nguyen Quy Khuyen, "Regarding the crime of manufacturing, buying, selling, exchanging or giving tools, equipment or software to use for illegal purposes (Article 285) the 2015 Criminal Code", *The Journal of the People's Court*, No 3/2017;

2. Nguyen Quy Khuyen, "Signs of quantitative damage of criminals in the fields of information technology and telecommunications networks according to the Criminal Code", *The Journal of Procuracy*, No 18/2017;

3. *Scientific commentary on the 2015 Criminal Code (amendments and supplements in 2017)*, Prof. Le Dang Oanh and Assoc. Prof. PhD. Cao Thi Oanh (Chief Author), Hong Duc Publications, 2017, *(Nguyen Quy Khuyen - Sector 2 Chapter XXI: Criminals in the fields of information technology and telecommunications networks);*

4. Nguyen Quy Khuyen, "Regarding the use of computer networks, telecommunications networks and electronic means performing acts of appropriation of property", *The Journal of Procuracy*, No 9/2020.