Cumhuriyet Üniversitesi Fen Fakültesi
Fen Bilimleri Dergisi (CFD), Cilt:36, No: 3 Ozel Sayı (2015)
ISSN: 1300-1949

Cumhuriyet University Faculty of Science
Science Journal (CSJ), Vol. 36, No: 3 Special Issue (2015)
ISSN: 1300-1949

Investigating Computer Fraud in Criminal Justice System of Iran

Zahed YOSEFI[1,*], Ahmad AHMADI[2]

[1]*MA in Criminal Law and Criminology, Department of Law, Urmia Branch, Islamic Azad University, Urmia, Iran*

[2]*PhD in Criminal Law and Criminology, Department of Law, Mahabad Branch, Islamic Azad University, Mahabad, Iran*

Received: 01.02.2015; Accepted: 06.06.2015

Abstract. The prevalence of computer crimes causes different kinds of damage in the society. Some of these crimes result in considerable financial and economic damage to the society. Among these crimes, computer fraud is considered a completely outstanding crime. The purpose of this research is to show the fact that although committing the crime of computer fraud in the setting of computer systems and generally in cyberspace may have various similarities with its traditional form, committing this crime occurs in a different space and context in which traditional fraud is committed. In addition, the special features of this transnational network due to its unlimitedness have created a situation that has made countries limited in enforcing penal laws on the one hand, and in spite of the existence of these limitations in enforcing penal laws, the criminals of this field commit unauthorized acts in relation to the data and information in cyberspace on the other hand that investigating these crimes requires specialized penal legal procedure, because legal procedure in the cyberspace crimes is different from material space. Many of the principles, which are already conducted in the judgments according to the existing traditions, cannot be applicable in cyberspace and definitely require new knowledge.

Keywords: Cyberspace, Computer Crimes, Computer Fraud, Penal Legal Procedure**.**

1. INTRODUCTION

At any time, along with technologies and tools which are developed recently, we are witnessed the misusing of these facilities. Computer, internet, and cyberspace are examples of relatively new technologies, which have been misused by jobber people as a platform to commit various crimes. Computer fraud is one of the modern crimes, which in English term is called the lords and white collars' crime, because fraudsters have high intelligence, and from the clinical and personality perspective, they are selfish, ambitious and silver tongued. The historical review shows that the rate of commuting this crime was very low in the past, but as the machinery life and new technology improve, it increases statistically. Computer fraud is one of the unforgivable crimes against people and victims' properties and their ownership rights, especially those of gullible and credulous people. The rise of such crimes in cyberspace causes the government and authorities to fight with these crimes, and maintain the cyberspace health. The first taken step was to enact laws and determine violations to be able to deal with criminals seriously. It should be noted that in such an environment tracking suspects and identify the main suspect is more difficult that the real world due to the international scope of Internet access. Exploring the new form of fraud, which is the result of new technology, provided a ground for investigating computer fraud with an emphasis on criminal justice system of Iran. The increasing advancement of science and technology and development of means of communication or in other words the emergence of the global village have consequently necessitated paying attention to social needs and providing new solutions. Since in today's world computer systems and information technology have intertwined with human life, and are one of the social and update issues in the society, the arrival of these new social phenomena such as other ones have many advantages and disadvantages in terms of

* Corresponding author. *Email address: yousefi.zahed@gmail.com*

Special Issue: The Second National Conference on Applied Research in Science and Technology

different aspects. Considering that the discipline of some parts of social phenomena require presenting appropriate strategies which are studied in various fields of science, law, which is a social branch of science organizing human relationships in a collective life framework, is profoundly influenced by information technology. In this regard, criminal law is affected more than other branches of law, because information technology not only has led to commit new criminal behaviors which were not possible before, but also it has facilitated common criminal behaviors by creating a new world. (Moradian, 2011)

With the emergence of information technology, computer fraud is one of the crimes which has been entered the field of specific criminal law, and have challenged the principles and rules governing the traditional fraud. Computer fraud is similar to traditional fraud in terms of name and the outcome of the crime, and differs from it in terms of the process of committing crime and the individual components that make up the crime. This difference has caused the computer fraud to be considered as a crime independent of traditional crime. It should be mentioned that any fraud committed with computer is not considered as computer fraud. Computer is involved in committing fraud from two following aspects.

(a). *Using internet to commit traditional crime:* the offenders use fraudulent means through internet, cheats others, and steals their properties. In this case, since computer is only used as a means of committing crime, and the type of device is not efficient in fulfillment of fraud, the committed crime can be prosecuted by criminal law relating to traditional fraud. The committed crime is a traditional fraud which can be called traditional computer fraud.
(b). *Using Computer to commit computer fraud:* the criminals do not deceive the victim or his or her representative, but they steals the victim's property by interference with computer data or computer system performance, and benefit from the financial services belonging to the victim. Such crime, which cannot be prosecuted by traditional fraud laws, is called traditional computer fraud.

Computer crime is one of the most common computer crimes, which is increased day by day. Some laws should be enacted and enforced to prevent committing such crimes and provide safety. In computer crime law, no definition has been given for computer crime and such as other crimes it has been considered enough to offer some instances of this crime. According to the definitions which are given for computer crime by international organizations, the instances of this crime are beyond the mentioned ones. Therefore, the following definition can be provided according to the law. Computer fraud is referred to committing acts such as entering, altering, fading, creating or intercepting data, disrupting telecommunication and computer systems.

in this paper we compare traditional fraud defined in Article 1 of *Aggravated Penalty Law For Bribery, Embezzlement And Fraud* approved by Iran's Expediency Council in 1988, with computer fraud mentioned in Computer Crime Law of Iran enacted in 2002, and analyze computer fraud, and propose some solutions for equalizing these laws and regulating law to provide security and healthy environment for internet users.

2. CYBERCRIMES AND ITS TYPES

2.1. Cybercrime

It seems difficult to provide a precise and comprehensive definition for cybercrime. For this reason, several different definitions have been proposed. Despites these differences, three main features of cybercrimes should be always considered in different definitions. The first feature is technology complexity (lack of ability to recognize complex and technical dimensions of cybercrime due to complexity of cyberspace). The second one is diversity of cybercrime (due to transformation and development of cyberspace), and the final feature is the ability to make the cybercrimes mysterious. In this regard, legislation authorities of different countries and

international documents including guidance and binding have proposed different definitions of such crimes according to the future needs and threats. Generally, in order to propose a comprehensive definition, cybercrimes can be defined as every criminal act or a criminal omission of an act against computer or its related issues (Williams, 2010).

2.2. Types of cyberspace crimes

According to Convection On Cybercrimes approved in 2001, cybercrimes can be divided into four following types:

(1). *Offences against confidentiality, integrity, and availability of computer data and systems:* these crimes are mentioned in Articles 2 to 6 of convection on cybercrime including "Illegal access", "Illegal interception", "Data interference", "System interference", and "Misuse of devices".
(2). *Computer-related Offences*: "computer-related forgery" and "computer-related fraud" are respectively mentioned in Articles 7 and 8 of the Convection.
(3). *Content-related Offences:* Article 9 of convection talks about child pornography as an instance of this type.
(4). *Offences related to the infringement of copyright and related rights:* the crimes related to the violation of intellectual property rights including copyright are mentioned in Article 10 of the convention as an instance of the fourth type.

In Iran's Law of computer crime, Cybercrimes are presented in 7 chapters titled "computer crimes" in Articles 1-25 including: (1) crimes against data confidentiality and computer and telecommunication systems such as unauthorized access and wiretapping, computer spying, (2) crimes against the authenticity and integrity of data, and computer and telecommunication systems such as Computer forgery, degradation and disruption of data or computer and telecommunication systems, computer-related theft and fraud, (3) crimes against public decency and morality such as dissemination, distribution or trading pornographic contents using computer systems or data carriers, disrespecting and spearing lies, criminal liability of legal persons, (4) other crimes such as production, publication or distribution of the data which are simply used as committing computer crimes and other crimes stipulated in various Articles.

It is necessary to note that in a general categorization, the crimes of this field include computer and telecommunication crimes. The separation of these two types of crimes is taken into consideration in both *2001 Convection On Cybercrime* as the most important international document, and in Iran's *2009 Law Of Computer Crime.* (Varavaei and Momeni, 2013)

3. COMPUTER FRAUD

3.1. Definition

Fraud is a type of crime which is continuously committed due to its specific nature after the rise of computer fraud, and is manifested in the form of computer fraud. After the rise of such crimes, which have traditionally existed in criminal law, they were referred as traditional crimes in the compilation related to information criminal law. So, non-computer fraud cases are referred as traditional or traditional fraud to make its criminal nature and definition distinguished from computer fraud (Dazyani, 2010). It will be useful to give a brief explanation of computer fraud before studying it. According to Article 67 of Iran's *Electronic Commerce Act* which is about fraud criminology in the context of electronic transactions, some believe that the title "computer fraud" does not seem accurate, and argue that the considered crime is not simply committed by computer, but all of the electronic devices provide the opportunity to commit it in cyberspace. Therefore, the title electronic fraud is a more general concept, and seems more appropriate (Ghannad, 2006).

The term computer-related fraud, which is a subset of committable crimes in cyberspace, is used in the Iran's Computer Crime Law. In this regard, some believe that computer crime include all types of crimes such as internet, cyber and network crimes which are totally dependent to computer systems. Thus, computer fraud is a noticeable term. It seems that according to the definition given for internet, it can be concluded that internet is a general term, which as can be explained every machine which has three features, receive structured inputs, process them based on pre-defined rules, and provide the results of computations as input (Alipour, 2011). Therefore, the offense committed by the electronics and telecommunications devices can be punished according to Article hereof in case of having the potential of computer systems in order to provide the environment for committing crimes.

Internet fraud is one of the computer crimes which also called "white collar crime" which has been increased by the development of internet and communication. To give a simple definition of white collars, it can be stated that white collars are those who violate the society members' rights by their social, economic and political positions. Internet fraud means any type of fraud which is committed by computer and internet programs or internet network communications e.g., using websites, email and chat rooms. In fact, internet fraud is referred to any fraudulent scheme which uses one or some parts of the internet to make some fraudulent requests to steal others' properties and do fraudulent transactions with potential victims. So, it is clear that internet fraud became quite common when virtual environment such as internet environment came into existence. Almost ten decades have passed from committing this crime. Some argue that the computer fraud is a Internet fraud, and the two terms are used interchangeably. The first internet crime-related law was approved in US in 1984, which was amended in 1994 and 1996.

In general, it can be said that internet fraud is referred to a crime in which a person steal money, property or financial services or benefits for his or herself or others using information and telecommunication systems. According to the Council of the Europe, computer fraud can be defined as an act in which the fraudsters enter, alter or disrupt computer data or programs or intervene in data processing, which lead to a change in data processing and result in an illegal economic loss for themselves or others. So, in fact, we observe that in computer fraud, an intervention is made in computer data or programs. Therefore, if we suppose that if was not so, for example if an individual falsifies a document using computer, then, shows this forged document to the another one, and acquires a property illicitly, it cannot be called a computer fraud but in this case the individual has falsified the document using computer, and has taken other's property traditionally. Also, there is not any difference between traditional fraud using computer and computer fraud. (Goldouzian, 2011)

3.2. History

In the historical evolution of computer crimes and consequently computer fraud, from the inception of computer to the present, three following generation of crimes can be observed. The first generation includes the crimes which were known since the late 80s, and introduced as computer crimes mostly including stealing and copying programs, and crimes against privacy in computer. This generation of crimes provided the grounds for the emergence of second generation of such crimes in 90s, which was known as crimes against data. So, all the crimes against information, communication and computer technology, satellites, and international networks were introduced as crimes against data. In the middle of 90s, the latter generation of computer crimes was formed named cybercrimes, virtual crimes or crimes in cyberspace by the development of international networks and satellite communications. Despites these accurate times, the first computer crime is unknown, and there are different ideas about this. Also, every country has its own history in this area. There are three different ideas about the accurate time of committing the first computer fraud, which are as follows:

- Some believe that computer crime has been occurred from the emergence of computer. This idea cannot be true because the negative aspects of a phenomenon do not necessarily occur simultaneously with its emergence. The historical records also show that after that the computer was used widely in the society, some users intended to abuse it. Therefore, the idea that computer fraud has existed from the emergence of computer is not true.
- Some others like Canadian authors believe that the first computer fraud was occurred in 1801. Joseph Marie Jacquard invented a mechanical loom which was first demonstrated in 1801. His employees were worried about losing their jobs, and destroyed the loom.
- The preferred one is that the case of Alden Rouis which was raised in 1960s, and led to his conviction has been known as the first computer fraud crime. The mentioned case was a corporate accountant. According to him, since the company had violated his right, he allocated a portion of the company's fund to himself by providing a plan. Thus he was able to withdraw over a million dollars during 16 years. Considering that the computer systems were in the early stages of their development, this action of Rouis was unpredictable because the design of the system was criticized. In that decade, punishing financial abuses including the case of Rouis were faced with the problems of laws relating to fraud, because the offender's act was a mere financial abuse or embezzlement without the victim's deception. This made the European legislators to revise the laws relating to fraud. With the advent of the Internet and the introduction of a new virtual world,

With the advent of internet and the introduction of a new virtual world, several cases of fraud were committed such that the accurate date of the first offense in cyberspace is not clear, because the offenders had left no clue, and the victims had refused to complaint due to some issues such as labeling credulity or fearing of embarrassing. What the above-mentioned says imply is that the accurate exact date of the commission of the first computer crime is not clear. This may have another reason which is lack of knowledge and perception of computer crime in those times.

4. COMPUTER FRAUD IN SUBSTANTIVE CRIMINAL LAW OF IRAN

Every crime is consisted of specific elements which distinguish it from the other crimes. Fraud can be separated from other crimes against property by identifying its constituent elements. In this section, after referring to the legal documents related to criminology of both the traditional and computer fraud, the constituent elements of these crimes will be studied under the title of legal, financial and mental elements, and other related issues.

4.1. The constituent elements of computer fraud

4.1.1. Legal element

In the criminal law of Iran, the Article 1 of the 1988 Act,and its notes include the legal element of traditional fraud. With the advent of computer crimes, considering that such crimes were occurred in computer environments, which differ from physical environments, the process of committing such crimes changed in the legal system of Islamic Republic of Iran such a way that the possibility of punishing the related criminals was faced with a challenge based on the traditional laws, and the necessity of regulating new laws became unavoidable.

About the legal element of fraud, it can be stated that Article 67 of Iran's *Electronic Commerce Act* have discussed the computer fraud criminology in the context of electronic transactions, and also Article 13 of Iran's *Computer Crime Law* is about the legal elements of computer fraud in the laws of Iran. If a committed action in the context of electronic transactions has the conditions mentioned in Article 67 of Electronic Commerce Act, it will be subjected to the Article, otherwise it will be subjected to Article 13 of this law. Therefore, the main elements of computer fraud are Articles 67 of *Electronic Commerce Act*, and 13 of *Computer Crime Law*, in which no definition is given for computer fraud, but with regard to the contents of mentioned ARTICLEs, crime can be defined as the following: Acquisition of financial and services or taking others' properties by

unauthorized misusing of data, massages, computer programs and systems, and telecommunication devices.

Since in fraud-related laws, another one necessarily should be cheated, but in computer fraud it is not so, a legislative vacuum occurs, which is filled by enacting computer fraud-related law in some countries. Criminals' paths are different in the crime of the fraud and other crimes against property. In the crime of theft, the thief steals others' properties. In the crime of fraud, although the owner of the property want to catch the criminal, but in reality, the criminal's fraudulent maneuvers lead the owner to catch the criminal and forgiving the property to the criminal is based on the owner's satisfaction. In the crime of computer fraud, the offender commits the crime using specific software, and does not deceive anyone directly, but deceives the computer in this way that access to the computer without authority and achieves the considered goal.

4.1.2. Financial element

The financial element of fraud is of great importance, because it is considered as the most important and complex element of the crime, while the more increase in new technologies occurs, the more continuously the financial element of crimes changes. Such changes are so rapid and extensive that has made identifying fraud and distinguishing it from other crimes against property so difficult. According to the Article 1 of Iran's *Aggravated Penalty Law For Bribery, Embezzlement And Fraud*, the financial element of traditional fraud consists of (a) offender's action, (b) terms and conditions for the realization of offense, and (c) achievement of criminal result. It should be noted that it is necessary to establish a casualty relationship between the committed behavior and the result of the crime. In this section, three mentioned components of financial element of traditional fraud are compared with the financial element of computer fraud.

***Offender's action*:** The term "anyone" in Article 13 of Iran's Computer Crime Law, clearly implies that everyone can commit computer crimes without any specific requirement, and receive criminal fines. Therefore, it is clear that the existence of one of the positions mentioned in first Paragraph of Article 26 of the Computer Crime Law can results in aggravating the punishments for the crime. Computer fraud is a crime which is committed by a positive financial action. According to Article 13 of Computer Crime Law, the acts leading to the occurrence of computer fraud fall into four following categorizations:

A. The crime should be committed using computer or telecommunication systems;
B. The action should be illegal;
C. Any entering, changing, deleting, creating and obstructing computer data without permission that cause financial losses to others;
D. Any form of unauthorized disruption in computer system performance by means of which money, property, benefit, or services or financial privileges are gained for individual or others.

The main difference between traditional fraud and computer fraud is related to the way crime is committed. The person who commits the offense of computer fraud can enter incorrect data to the computer (i.e., manipulating the input data), manipulate the computer screen processing (i.e., manipulating program, keyboard and hardware) or consequently distort the correct results shown by computer (i.e., manipulating output data). It should be noted that most of the computer manipulations are related to input data manipulations. Such manipulations can be done by adding, deleting, changing, replacing, or sending them to an improper location (Sieber, 1998).

***Terms and conditions for the realization of computer fraud*:** There are three important conditions for the realization of fraud among all other conditions, which are:

i. Fraudulent use of equipment used by the offender to deceive others;

ii. victims who are deceived and cheated due to the lack of awareness to fraudulent devices used by the offender;
iii. The taken property belongs to the other one.

It should be mentioned that existence of the one of two first and second conditions does not necessarily implies the existence of the other condition. In other words, using fraudulent device by the fraudster does not necessarily mean that the victim has been deceived. Also, the fact that a credulous victim is deceived does not inevitably mean that the fraudster has used fraudulent devices. So, the existence of both conditions should be proved. Identifying and distinguishing these two conditions will become easier when we note that the objective and subjective tests are used to meet the first and second condition respectively. (Mir Mohammad Sadeghi, 2008)

***Achievement of criminal result*:** Fraud is one of the crimes which are bound to the achieved result. It means that neither using fraudulent devices nor deceiving victims is sufficient for the realization of the crime without resulting in taking others' properties. According to Article 1 of Iran's *Aggravated Penalty Law For Bribery, Embezzlement And Fraud*: The one who obtains funds, property, document, draft, bill, and etc., by deceiving, and cheating is called "fraudster". This confirms the above-mentioned statement; therefore, the realization of the crime is not possible without achieving the result. Taking others' properties requires causing financial loss to the victim, and the fraudster' or the considered person's financial gain. This loss should be financial, and it does not include non-financial losses. Notably, the incurred loss should not necessarily be permanent (Khoramabadi, 2007). Computer fraud is also a crime which is bound to the achieved result. One of the substantial difference which leads to distinguish this crime from the computer crimes such as data disruption, system disruption and computer forgery is that this crime differs from other ones. The result of committing fraud is the loss incurred to the owner of the property by taking his or her property without permission. By comparing the result of computer fraud with other crimes which their act of crimes is relatively common, the difference among them is easily recognized. The result of the crime of data disruption is simply damaging and destroying the computer data. The result of the crime of system disruption is interfering with the functioning of a system. The crime of computer forgery-related result is creating an incorrect electronic document, while the crime of computer fraud- related result is potential financial loss resulting from any fraudulent manipulating data or computer systems, which is incurred to the owner of the property without having any authorization.

4.1.3. Mental element

According to Article 1 of Iran's *Aggravated Penalty Law For Bribery, Embezzlement And Fraud*, the crime of fraud is one of the intentional crimes. So, this crime is not occurred by neglect. The mental element of computer fraud is consisted of three parts; offender' knowledge, general Malice, and specific Malice.

Offender's knowledge: According to Article 8 of *Convention On Cybercrimes*, one of the conditions of computer fraud is that the criminal behaviors, which constitute a part of financial element of this crime, should be without authority. Also, economic losses made to the owner of the property by the offender should be without authority to make the crime of fraud occurs; Therefore, the offender's knowledge, not being authorized of behaviors and not being authorized of the result of these behaviors are the conditions for the occurrence of the crime of computer fraud, and constitute one of the parts of the spiritual element of computer fraud. If the offender thinks wrongly that he or she has the authority to access to the result, even if these acts are done intentionally, the crime will not be occurred.

General Malice: general Malice means the conscious will of an individual to commit a criminal act. In other words, the fraudster should use a device deliberately having the knowledge that the used device is fraudulent. In the context of electronic transactions, the crime of fraud under both Article 67 of Electronic Commerce Act, and Article 13 of Computer Crime Law is considered as

a type of intentional crimes, in which as well as traditional fraud the ascertain of specific Malice is required in addition to the ascertain of general Malice. Therefore, the offender should do the acts specified in legal provisions including entering, deleting, etc. deliberately. It means that the offender should have intention in doing an act.

Specific Malice: Specific Malice is the third element of the crime of fraud which means having the intention to take other's property (Mir Mohammad Sadeghi, 2009).To make the mentioned crime occurs, in addition to general Malice (having intention to use fraudulent devices), and specific Malice (having intention to take others' property) the offender should also be aware that the device is fraudulent while the victim is not aware of this.(Habibzadeh, 2009)

In the case of computer fraud, according Article 67 of Electronic Commerce Act, and Article 13 of Computer Crimes Law, the intention relates to acieving financial privileges or takes other's property for oneself or others. So, if the offender performs the mentioned acts without any intention, his or her action is not considered as a computer fraud (Mir Mohammad Sadeghi, 2009).

4.2. The punishment for computer fraud in Iran

In general, punishments are divided into three categories including principal, supplementary and accessory punishments. The legislator has specified one or some punishments for the offender, which can only be implemented based on a final decision of the court. Such types of punishments are principal. As the name implies, the supplementary punishments are added to the principal one, and it should be presented in the petition; moreover, it should not beruled alone by the court.Imposing punishments on the penetrators of such crimes is defined in Article 23 of Islamic Penal Code, according to which the court is able to impose one or some of the supplementary punishments stipulated in Article 23 on the person who has been received the discretionary punishment from sixth-degree to first-degree in compliance with the conditions prescribed in Islamic Penal Code of Iran, commensurate with the offence and its characteristics. In case of traditional fraud, the legislator has considered different punishments for simple and aggravated fraud. The punishment of simple fraud is imposed based on the Article 1 of Iran's *Aggravated Penalty Law For Bribery, Embezzlement And Fraud*. In this case, in addition to return the taken property to the owner, the offense carries imprisonment sentence of 1-7 years and a fine with a value equal to the taken property. In case of complex fraud, the related cases are mentioned in Article hereof. This fraud is committed using public interpretation, or when the offender is one of the employees of the government or governmental institutions and organizations. In this case, the punishment for the crime of fraud is exacerbated. It means that the punishments for such offense are aggravated to 2-10 years of imprisonment, a fine, and dismiss of governmental services forever. The latter punishment i.e., dismiss of government services only referrers to cases in which the offender is one of the government's employees. In general, the main punishment for the computer fraud under Article 13 of Computer Crimes Act is to return the original property to its owner; moreover, the offender is sentenced to 1 to 5 years in prison or to pay a fine of 20-100 Million Rials, or both. In case of committing computer fraud in the context of computer transactions, by virtue of Article 67 of Electronic Commerce Act of Iran, the offender is sentenced to 1 to 3 years in prison, and to pay a fine of taken property. It seems that the legislator should have paid an extra attention to the imposed punishment, and handed down a heavier punishment for the computer crime rather than the traditional fraud, because computer fraud happens faster, has a lower cost, and causes a greater loss in comparison to traditional fraud. It should be noted that computer fraud is a complex crime as well as the traditional crime with a different process of crime commitment. Traditional fraud occurs in a physical environment, and can be ascertained easier than the computer fraud which is occurred in computer system environment or generally virtual environment, because detecting, prosecuting, and proving the committed crimes in cyberspaces is very difficult, and sometimes impossible considering that the cyberspace is based on the principle of anonymity. In terms of supplementary and accessory punishments, both

traditional and computer fraud are punished under Articles 23-26 of Islamic Penal Code of Iran issued by 2013, and the court is able to impose supplementary punishment on the offender according to Article 23 for supplementing the offender's punishment.

5. CONCLUSION

The world of today differs from the world of a few centuries ago or even a half-century ago. The advent of computer and internet has influenced the citizens' everyday lives such that it has changed methods and criteria. The role of such technologies can no longer be denied, and its existence cannot be ignored in terms of developing solutions and easy accessing the sheer volume of information. This giant of knowledge serves people and the humanity benefits from its valuable presence, considers it worthy, and watches its progresses and developments. But It should be remembered that Although this technology plays a positive and constructive role in individuals' everyday lives by honorable, conscientious and philanthropist peopler, sometimes it is in the hands of criminals and evil people, and leads to inhuman and damaging consequences. These consequences result in occurrence of new and complex types of crimes, which are not in consistence with the traditional types.

In this paper we tried to discuss computer fraud in criminal justice system of Iran. Traditional type of fraud is a known crime, which is contained in Article 1 Iran's *Aggravated Penalty Law For Bribery, Embezzlement And Fraud*. Despites the similarities between the occurrences of fraud crimes in a physical space, or in a cyber space, the differences among the processes of committing these crimes faced punishment the perpetrators of the crime of fraud in the computer systems by the traditional rules with uncertainty. New technologies necessitate us to become familiar with new ways of using them and their applications. It is not possible anymore to swim in this vast ocean of technology only with traditional methods and known tools. According to this study, The Code of Criminal Procedure in cyberspaces differs from that of in physical and traditional spaces. Most of principles that have already done accordance with the tradition in proceedings, cannot be employed in cyberspace, and certainly requires new knowledge. Judge, judicial officers, and all those involved in criminal process should become familiar with related methods used in cyberspaces.

REFERENCE

[1] Moradian S. (2011). Investigating Computer Fraud And Comparing It With Traditional Fraud In Criminal Provisions Of Iran. Msc Thesis, University Of Tabriz, Tabriz, Iran.
[2] Williams M. (2010). "Cybercrime". In Brookman, F., Bennett, T., Maguire,M., And Peirpoint, H(Eds) Handbook Of Crime. Cullompton: Willan.
[3] Varavaei A., And Momenipour H.(2013). Cyber Crime: The Etiology And Prevention. Tehran: University Of Judicial Sciences And Administrative Services.
[4] Dazyani, M.H. (2010). Feasibility Study Of Computer Crimes: Necessary Regulation In Substantive Criminal Law. First Edition, Tehran: Secretariat Of The High Council Of Informatics, Vol. 1 And 2.
[5] Ghannad F. (2006). Dimensions Of E-Commerce Law. Phd Thesis, University Of Shahid Beheshti, Tehran, Iran.
[6] Alipour H.(2011). Criminal Law Of Information Technology. First Edition, Tehran: Khorsandi Press.
[7] Goldouzian I. (2011). General Criminal Law. Vol. 1, Tehran: University Of Tehran.
[8] Sieber U. (1998). Legal Aspects Of Computer-Related Crime In The Information Society: A CONCRIME Study. Available At: Http://Www.Oas.Org/Juridico/English/COMCRIME%20Study.Pdf
[9] Mir Mohammad Sadeghi H. (2008). International Criminal Court. 3rd Edition, Tehran: Dadgostar Press.
[10] Khoramabadi A. (2007). Computer Fraud In Iran And International Level. Journal Of Law, Faculty Of Law And Political Science, University Of Tehran, Vol.2.

[11] Mir Mohammad Sadeghi, H. (2009).Crimes Against Properties And Ownership. 19th Edition, Tehran: Mizan Press.
[12] Habibzadeh J.(2009). *Specific Criminal Law: Crimes Against Properties*. 6th Edition, Tehran: Samt Press.