MedCrave
Step into the World of Research
Forensic Research & Criminology International Journal

Review Article

Open Access

CrossMark

An elaboration on computer frauds from the perspective of Iran's law and international instruments

Abstract

Our modern society demands a degree of connectivity between citizens, businesses, financial institutions and governments that must cross political and cultural boundaries. Digital technology provides this connectivity and gives its users many valuable benefits. But at the same time, it provides a rich environment for criminal activity, ranging from vandalism to stolen identity to theft of classified government information. One of the modern crimes against property and ownership in the cyber-space is computer fraud. Despite being modern, the aforementioned crime has its roots in the principles of religious jurisprudence. In some cases, this crime is compatible with traditional regulations, and that is, when the computer is considered as a crime instrument. Some of the computer frauds that take place in the context of electronic exchanges are considered as crimes as per the E-commerce Law (approved in 2003) of Iran. However, these regulations are flawed and until recent years, there was no comprehensive law in this regard. After so many years of legal vacuum, legislation of the Computer Crime Act 25/05/2009 led to partial settelment of the problems arising thereby. The present study intends to investigate computer fraud according to Iran's Computer Crime Act and also elaborate upon those international instruments in this regard.

Keywords: fraud, computer fraud, computer crimes, cyber crimes, classic fraud

Volume 6 Issue 2 - 2018

Babak Pourghahramani

Department of Law, Maragheh Branch, Islamic Azad University, Iran

Correspondence: Babak Pourghahramani, Assistant Professor, Department of Law, Maragheh Branch, Islamic Azad University, Maragheh, Iran, Email pourghahramani@iau-maragheh.ac.ir

Received: February 12, 2018 | **Published:** April 10, 2018

Introduction

The fraud is one of the crimes against property and ownership. Subsequent to the formation and evolution of computer systems, computer frauds and those happening in cyber-space has duly been recognized and considered as one of the most important forms of economic crimes. In this crime, the offender appropriates another person's property through false programming, changing the data, misusing the computer system, etc. This crime is structurally different from the classic fraud crime since in computer fraud, the data acts as the representative of the material property in the data processing systems. In most cases of computer fraud, the property whose representative is the computer data is immaterial, e.g., the deposits, receivables, work time, value of credits, and balance sheet calculation results.[1] In some cases, the data of the computer fraud problem which is the representative of tangible and material things is stolen after computer system is manipulated by the offender. These cases are specifically related to cash, different materials and goods. Manipulation of the data related to these traditional issues of crime generally causes less damage compared to the changes in incorporeal property since here the damage is confined to the real value of the available goods.[1] Nowadays, owing to the increase in the ATM and emergence of the "very efficient electronic devices for good sales" equipped with electronic sensors, it has been made possible to commit a specific group of computer crimes which are basically related to tangible cash, goods and services recorded by computer systems.

In addition to the difference between computer and traditional fraud problems, the victim of crime is mostly unknown to the offender of fraud and the time required for perpetrating the crime is reduced to a minimum and the time of crime commitment is clouded in ambiguity. Due to these new qualities and in order to affect the perpetration conditions of traditional crime, the international instruments and criminal law of most countries have recognized traditional crime committed via the computer as the new type of crimes entitled as computer crimes. Most cyber crimes are committed by individuals or small groups. However, large organized crime groups also take advantage of the Internet. These "professional" criminals find new ways to commit old crimes, treating cyber crime like a business and forming global criminal communities. Criminal communities share strategies and tools and can combine forces to launch coordinated attacks. They even have an underground marketplace where cyber criminals can buy and sell stolen information and identities. It's very difficult to crack down on cyber criminals because the Internet makes it easier for people to do things anonymously and from any location on the globe. Many computers used in cyber attacks have actually been hacked and are being controlled by someone far away. Crime laws are different in every country too, which can make things really complicated when a criminal launches an attack in another country. Having described this, the importance of identification and investigation of the computer fraud crime will be investigated subsequently.

Computer fraud background

Computer fraud is among the first generation of computer crimes, and in this generation, the computer is considered merely as a crime commitment device and therefore the computer fraud can be regarded as one of the computer crimes after the indisputable interference of the computer in the everyday activities of humans' life.[2] Cybercrime first started with hackers trying to break into computer networks. Some did it just for the thrill of accessing high-level security networks, but others sought to gain sensitive, classified material. Eventually, criminals started to infect computer systems with computer viruses, which led to breakdowns on personal and business computers.

Computer viruses are forms of code or malware programs that can copy themselves and damage or destroy data and systems. When computer viruses are used on a large scale, like with bank, government or hospital networks, these actions may be categorized as cyberterrorism. Computer hackers also engage in phishing scams, like asking for bank account numbers, and credit card theft.[3] In the 1960s, financial abuses such as the financial abuse of Royce was less compatible with the regulations related to fraud since the offender's act, in the absence of victim deception, was a kind of sheer financial abuse or embezzlement, and this forced legislators to revise the regulations related to fraud. Since the 1960s and up to now, computer fraud crime has become more and more diverse and interesting and has become more evolved generation after generation and step by step in tandem with the improvement and progress of computer and communications technology. In the 1970s, we witnessed computer fraud crime with the immense volume of loss resulting from committing this crime or other computer crime against property. Over a general course, computer fraud crime has gone through some periods. This course started with false programming, false structuring, etc., and in 1980s, the evolutionary process of the mentioned crime became more complicated; and therefore today, computer fraud is committed in different and various ways. The Internet Fraud Complaint Center (IFCC) of the United States of America in 2001 divided computer fraud into nine parts: Financial institution fraud, Gaming fraud, Communications fraud, Utility fraud, Insurance fraud, Government fraud, Investment fraud, Business fraud, Confidence fraud. Nevertheless, it can be said that as long as there is cyber-space and as long as humans take virtual steps there, computer fraud will exist and no one may claim its insinificance compared to other crimes.

Definition of computer fraud

Does computer fraud have a definition different from classic fraud? In order to clarify this, we will begin by defining traditional and classic fraud; subsequently, considering the definitions, it will be determined whether the aforementioned definition can include computer fraud or not; to be precise, whether fraud has a single definition or along with changes in situations that the definition might vary. In the current regulations of Iran, no definition has been rendered of the crime of fraud, and like some crimes, only examples have been cited. These examples have been cited in Article 1 of the Law of Resonance of Punishing Bribery and Embezzlement and Fraud Act approved in 1988; and according to this law, a professor of the criminal law has defined fraud as: "fraud refers to appropriating another person's property through ill-willed resorts to fraudulent devices or operations",[4] while in another definition it has been cited that: "appropriating another person's property by resorting to fraudulent means or fraudulent appropriation of another person's property".[5] What can be gathered from the aforementioned definitions and the mentioned law is that one of the prerequisites for the perpetration of crime of fraud is deception of the victim and for this "deception" to take place, the commitment of this crime against a human is also necessary.

Now according to this point, do the definitions include computer fraud as well? Here, two cases must be distinguished; the first case is when a computer is used as a "device" in fraud and the computer "as the fraudulent device" is used for the aforementioned items in Article 1 of the Law of Resonance of Punishing Bribery and Embezzlement and Fraud. For instance, when through the computer someone introduces themselves as the owner of a company that does not really exist and through this action appropriates another person's property or when by trusting them to be a particular notable person, targeted individuals give them some property; here, the definition includes this case as well. The second case is when the fraudulent attempts made by the offender are against the computer system without a person being deceived; in other words, property or financial benefits are appropriated through misleading the computer. Now, the next question proposed is whether a machine can be deceived or not. It seems that fraud requires the existence of a human mind which is capable of being deceived; therefore, the definitions said above cannot include all the cases of computer fraud. Furthermore, in most countries, no definition of computer fraud has been rendered; yet the Council of Europe makes reference to it in a broad definition: "computer fraud refers to the input, alteration, deletion or suppression of the computer data or programs or other considerations in the data processing that affect the result of processing and cause economic losses or appropriation of another person's property with the intention of gaining illegal economic benefits for oneself or others".[6]

Also, Article 8 of the Convention on Cybercrime defines computer-related fraud as: "any kind of input, alteration, deletion or suppression of the computer data or any interference with the functioning of a computer system that is conducted deliberately and unjustly and with the intention of fraudulent or unjust appropriation of an economic benefit for oneself or others and causes financial damage to another person".[6] In addition to these, the Computer Crime Act approved in 2009/26/5 by the Islamic Council of Iran has allocated Article 13 to computer-related fraud without any definitions; the aforementioned Article has appointed: "anyone who illegally appropriates money or property or services or financial benefits for oneself or others through the computer or telecommunications systems by taking measures such as the input, alteration, deletion, creation or suppression of the data or any interference in the system, will be sentenced to … years' imprisonment in addition to rejecting the property to its owner" (page 9). As can be observed, the aforementioned Article is highly influenced by international laws and regulations, but in domestic and international regulations on computer fraud there is this common point that firstly the person must have illegally undertaken fraudulent measures on the data or have interfered in the system, and that secondly, they must have appropriated property or financial benefits from these actions.

Therefore, it is observed that one of the basic differences between computer and classic fraud is that perpetration of classic fraud requires the deception of the victim of the crime, while computer fraud is committed without deception of the victim of the crime and happens through undue interferences with the computer data or functioning of the computer system.[7] Furthermore, this definition of classic fraud cannot be applied to computer fraud. With regard to computer frauds it has been stated in the Article 67 of the E-commerce Law[1] that: "computer fraud refers to appropriation of another person's property by fraudulent use of the computer";[8] although the definition above has been rendered at the time of E-commerce Law, it can be compatible with the Computer Crime Act and is in other words the best and briefest definition for computer fraud. Thus, it can be noted that in some cases when the computer is used as a device in fraud, it is compatible with all the conditions of the definition of traditional fraud, yet in cases when fraud is committed by fraudulent use of the computer, the definition above does not include these cases.

[1]In Iran's criminal law prior to 2003 computer fraud wasn't discussed. Finally, in 2003 when E-commerce Law was approved, without rendering a definition of computer fraud Article 67 cited the examples of computer fraud.

Citation: Pourghahramani B. An elaboration on computer frauds from the perspective of Iran's law and international instruments. *Forensic Res Criminol Int J.* 2018;6(2):107–114. DOI: 10.15406/frcij.2018.06.00192

Legal review of the computer fraud crime

Computer fraud from the perspective of international documents and recommendations

As the result of easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries, such as the Philippines, laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington. They proceeded to lure the two Russian men into the United States by offering them work with this company. Upon completion of the interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cybercriminals when weak legislation makes it impossible otherwise.[9] A document published by the Organization for Economic Cooperation and Development (OECD) in 1986 suggested measures based on comparative analysis of substantive rules; paragraph "A" has emerged in computer fraud and in fact economic crime of the computer:[10] "A-Input, alteration, deletion or suppression of the computer data or computer programs that is deliberately conducted with the intention of illegal transfer of money or any other thing of value…".[11]

After presentation of the report (OECD), in Recommendation 9 of R (89) approved in 1989 in the list of the minimum computer crimes, the Council of Europe explicitly mentioned computer fraud as below:

A. Computer fraud; input, alteration, deletion or suppression of the computer data or programs or other interferences in the data processing that affect the processing result and cause economic losses of appropriation of another person's property in order to gain illegal economic benefits for oneself or others".[6]

As can be observed, the main goal of the Article is identification as a crime any kind of misuse in the area of data processing due to affecting the results and illegal transfer of property and infliction of damage. The data is the goal of computer fraud. Limiting the crime to computer data and programs indicates the minor role of this crime i.e. committing rcomputer fraud crime is a subordinate of data misuse. In addition to these, the Convention on Cybercrime (Budapest), the only international document that investigates the substitutive and formal regulations of computer crime, has also explored computer fraud and the other relevant crimes in Article 8. Based on this Article, "in their domestic law, each of the countries must enact law in this regard and criminalize any deliberate and unlawful actions that are taken with ill intentions and in order to gain unlawful economic benefits for oneself or others. These actions include:

i. Input, alteration, deletion or suppression of the computer data or programs

ii. Any interference with the functioning of a computer system".[6]

Article 8 of the Convention is written such that it considers the computer system merely as a device for gaining economic benefits and as if it is unaware of the fact that if the physical actions of input, alteration or deletion of the data or interference in the system leads to gaining computer data or software using the computer functioning or specific software, whether fraud still takes place or not. However, the term "economic benefits" might be used, and it might be said that if the data has financial value and has economic benefits, it has predicted two types of computer fraud; a fraud in which the computer is the crime commitment device and a fraud in which the computer is both the crime commitment device and also the crime commitment subject.[2]

The International Criminal Police Organization (Interpol) has also classified computer fraud into the six following crimes in its classification list:

a. Misuse of ATM banks;

b. Computer hoax;

c. Misuse of the arcade machines;

d. Manipulation in the input and output stages;

e. Misuse of the payment devices based in the stores; and,

f. Telephone abuse (for wiretapping or using telecommunications services".[12]

Since the 1980s, the UN also, as the most important international organization, considered the problem of computer crime and in the Seventh United Nations Congress in 1985, computer crime was one of the issues proposed in the report of the Secretary General of this organization and in the Eighth United Nations Congress the Secretary General was asked to publish a technical manual on the prevention and prosecution of computer offenders. This manual was prepared in 1992 by Ottawa and its result was published in numbers 43 and 44 of the International Review of Criminal Policy, and one of the crimes that are mentioned in this review is computer fraud.[13] Also, in the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in Vienna, April, 10-17, 2000, supreme technological crimes were divided into three groups and the second group is allocated to traditional crime committed using a computer or communicational technologies - computer fraud is among this group.[14]

Computer fraud from the perspective of Iran's law

Regulatory element

Countries around the world have adopted three approaches to computer fraud:

A. The regulatory element of countries that have explicitly enacted separate criminal laws regarding computer fraud; in these countries there are practically two kinds of fraud; traditional fraud and computer fraud; for instance Article 93 and Article 115 of the Economic Crimes Act related to the computer (approved in 1985) or Article 363 of German Criminal Law (amended in 1986) or Article 279 of Danish criminal law (approved in 1985) or Article 13 of the Computer Crime Act (approved in 2009), and in these countries, appropriation of money or benefits through illegal methods of data processing or deletion or alteration or creation of data in the computer system is recognized as computer fraud.[2]

B. Although some countries have not enacted a new regulation for computer fraud, by adopting a general regulation they have

Citation: Pourghahramani B. An elaboration on computer frauds from the perspective of Iran's law and international instruments. *Forensic Res Criminol Int J.* 2018;6(2):107–114. DOI: 10.15406/frcij.2018.06.00192

asserted that if a crime is committed through the computer, it will be punished based on traditional criminal provisions; e.g. the Indian Penal Code.[2]

C. Meanwhile, some other countries have basically preferred to remain silent regarding computer fraud and the crimes related to that are charged under the existing criminal provisions. These countries are mostly developing, where computers and the Internet have not fully developed yet.

In Iranian criminal law, the principle of computer fraud is distinguished by two issues: A- In the case where the computer is merely the crime commitment device. B- In the case where the computer itself is the subject of crime.

Concerning the former, it should be noted that traditional regulations of fraud (Article 1 of the Law of Resonance of Punishing Bribery and Embezzlement and Fraud approved in 1985/19/9) can compensate for this deficiency and be recognized as the main regulatory element of the crime, since the computer is a mere fraudulent device for appropriation of property and has all the elements of traditional fraud. In fact, it can be said that it is the same as traditional fraud but what distinguishes this from other cases is using the computer as a fraudulent device. In other words, it does not make any difference what the device is, what matters is that the victim is deceived; thus, if through the computer by sending an e-mail a person introduces themselves as a famous businessman and by trusting them people deposit some money into their accounts so as to receive a particular good (while the aforesaid person has been an ordinary employee), in case of not receiving the good, the aforementioned person has become subject to Article 1 of Law of Resonance; the only difference it has with other cases is that it has deceived people via the computer.

Also, regarding pyramid companies or network or multi-level marketing that are known as MLM or NM and have been operating in countries for some years now, computer fraud can be cited. In addition to the aforementioned law according to Article 131 of the Criminal Code of the Armed Forces (approved in 2003/30/12) any change or deletion of the data, accession, submit or delay of the date compared with the actual date and the like that is illegally carried out by the military in the computer system and the related software and also actions such as submitting classified computer information to the enemy or people that are not qualified to access the information, unauthorized disclosure of information, theft of valuable items of information such as the CDs or Disks containing information or their obliteration or financial abuses that the military commits by the computer are considered as crime and are subject to the punishments set forth in the cases related to this law. Nevertheless, although this Article has referred to financial abuses of a computer, it is firstly only specific to the military, and secondly, has determined its punishment because of the previous regulations of the Criminal Code of the Armed Forces; this law does not basically refer to computer fraud and therefore the term financial abuses is not connected to computer fraud.[2] Also, the E-commerce Law (approved in 2003/17/1) regarding crimes and punishments in Article 67 has explicitly referred to computer fraud. Based on Article 67 of this law that "anyone who deceives others in the context of electronic exchanges by misusing or illegally using the data, data messages[2], programs and computer systems[3] and telecommunications equipment's and committing actions like input, deletion, suppression (of the data messages), interference in the functioning of the program or computer system et al., or misleads the automated processing systems and the like and through this appropriates money, property or financial benefits for oneself or others and steals the others' property, they are considered offenders and, in addition to returning the property the property owners, they are sentenced to one to three years' of imprisonment and payment of fine equivalent to the property…".

This Article is a combination of Article 1 of the Law of Resonance of Punishing Bribery and Embezzlement and Fraud and Article 8 of the Budapest Convention. Although this Article has used the title of computer fraud, it is specific to electronic exchanges[4] and has no position in other than these cases.

Article 67 of the aforementioned law has cited two ways for fraud; one is the deception of others which is the common method and the other is the deception or misleading of computer systems and so on or the automated processing systems and the like that is related only to the hardware and software devices that operate through implementation of automated processing programs. Eventually, the Penal Code on the Computer Crime (approved in 2009/26/5) that was approved after many years, has allocated its third chapter that contains two Articles to "computer-related theft and fraud" and Article 13 of the aforementioned law is related to computer fraud; based on the data above:

"Article 13 - Anyone who illegally appropriates money or property or benefits or services or financial advantages for oneself or others through computer or telecommunications systems by committing acts like the input, alteration, deletion, creation or suppression of the data or any interferences in the system, in addition to rejecting the property to its owner, they will be sentenced to one to five years' imprisonment or 20 million Iranian Rials (RLS) to one hundred million Rls. fine or both".

As can be observed, in this Article:

Firstly, the aforementioned law has merely allocated the title of the chapter to "computer-related theft and fraud" and also the Articles, including that of Article 13, do not mention computer fraud at all. At this point, it is necessary to reflect on whether without mentioning computer fraud in the Article it can be considered as fraud merely based on the "title" and also the fact that the court will charge the accused under any criminal term. Nevertheless, the aforesaid article is ambiguous in this regard and basically the court should not charge the accused with the computer fraud; rather, the accusation set forth in Article 13 of the Computer Crime Law, accession of appropriation of money or property, etc. must be conducted through computer systems; yet based on the content of the Article and its title, we may allocate Article 13 to the computer fraud. Secondly, fraud, the way it is spoken of in traditional fraud, does not exist here. Thirdly, the point here is the deception of the victim while computer fraud lacks this prerequisite since in computer fraud people are not in contact with one another

[2]It is any symbol of the event, information or concept that is produced, sent, received, stored or processed by electronic, light devices or new information technologies.

[3]It is any connected hardware-software device or set of devices that operates by execution of automatic processing programs of "the data message".

[4]Electronic exchanges refer to the fact that all the information and business negotiations with determined and defined structure and form and by using standardized messages are transferred from one computer to another computer through electronic and telecommunications devices and as in this method paper is not used, it therefore is known as the paperless trading method.

Citation: Pourghahramani B. An elaboration on computer frauds from the perspective of Iran's law and international instruments. *Forensic Res Criminol Int J.* 2018;6(2):107–114. DOI: 10.15406/frcij.2018.06.00192

and the offender works with a device named computer which cannot be said to have been deceived; due to this, the aforementioned article does not refer to the problem of deception duly.

As a result, what at present constitutes the regulative element of computer fraud crime in its general sense is:

a. When the computer is merely a crime commitment device; as proposed before, this has no difference with traditional fraud and Article 1 of the Law of Resonance of Punishing Bribery and Embezzlement and Fraud contains the aforementioned case.

b. Fraud based on Article 67 of the E-commerce Law; this crime does not have generality either; it is specific and applicable only in the context of electronic exchanges.

c. Fraud based on the Computer Crime Act (Article 13) that is comprehensive compared with the two first Articles concerning computer crimes and our main discussion will be in this regard as well.

Material Element

In the discussion on the material element of this crime, three things must be considered: 1- physical behavior, 2- conditions and states necessary for perpetration of crime, and 3- the result obtained from the behavior of the accused.

The behavior of the offender

Based on Article 13 of the Computer Crime Act and according to the Convention on Cybercrime and recommendations of the Council of Europe, the physical behavior of computer fraud must be based on action, since the examples that are deployed for committing computer fraud in Article 13 are somehow a positive form; therefore, leaving the action cannot constitute the material element of computer fraud. These behaviors include:

i. Illegal input, alteration, deletion, creation or suppression of data that leads to the appropriation of money or property or benefits or services or financial advantages for oneself or others.

ii. Illegal interferences in the computer that lead to appropriation of money or property or benefits or services or financial advantages for oneself or others.

The point that should be noted regarding the aforementioned examples is that unlike the Convention on Cybercrime, the aforementioned examples are figurative, and therefore, any behavior other than the examples stipulated in Article 13 can also constitute the material element of fraud when allocated to the appropriation of property and money.

Examples of misuse in the computer fraud

i. Input of computer data: includes input of data and information in the computers and includes input of accurate data and also false data that causes a person to use the facilities of this technology and appropriate property for themselves or others; for instance, they enter the information with the content that they have a certain amount of money in their bank account; as a result, the bank appoints this amount to them and the stipulated regulation (input of false data and illegal input of accurate data) not only includes misuse of stolen checks and credit cards in an automatic bank; rather, it also contains misuse of a personal card and transgression of credit limits.[15]

ii. Alteration of computer data: It includes amendment, conversion, partial and general alterations of the data illegally by appealing to which property, money and financial services are appropriated; in other words, if the computer hoax is considered an abuse case and as a result of the aforementioned change, property, money or financial advantages and services are appropriated, a crime is perpetrated such as the change in the title of a company or financial institution or trading house of the bank when the customers of the aforementioned institutions end up depositing their payable money to the bank account of the person who has changed the information.[8]

iii. Deletion of computer data: includes the destruction and omission of data; in other words, it equals the destruction form of a physical and tangible object.[7] In case financial results are obtained from its deletion, it can be still considered as one of the examples of computer fraud; for instance, when by illegal penetration into the computer system of a bank or institution from where they have obtained a loan and are in fact indebted to the bank or institution, a person deletes the information related to their debt or decrease their debt; here, the person has committed computer crime through deletion of the data.

iv. Creation of computer data: this term has not been cited in international documents and refers to the creation and generation of data so that it leads to appropriation of property or financial benefits.

v. Suppression of computer data: It refers to interruption in the process of data and information exchange; in other words, suppression includes storing and holding data, which results in the act of processing not to be conducted simultaneously, and which might be temporary or permanent. The most interesting example of manipulation a computer keyboard or hardware was carried out in West Germany in the mid-70s, which involved concealing large transactions of foreign currencies at Hirsch Tat Bank. All accounting matters of Hirsch Tat Bank regarding transactions of foreign currencies and money were recorded by means of the keyboard of a small computer, and subsequently transferred to a central computer; by pressing the 'stop' key on the keyboard of a small computer, the bank clerk managed to withhold substantial sums foreign currency transactions and keep it hidden such that the data related to these interactions was not transferred to the bank's central computer. Therefore, the clerks could receive a complete approval of the small computer regarding these interactions with the contract side (contractor) without any computational records in this area being recorded in the central computer. This made possible the hiding of the losses and keeping of the general money of the bank for the future interactions. In addition, the clerk could claim that the losses are created due to the business of the bank only and, thus, opt for further actions.[1]

vi. Interference with the function of computer system: any other act such as misuse of the hardware including the actions preventing the printer to work, the acts effective in recording and etc. When this act leads to the appropriation of property or money or to benefits or advantages computer fraud is perpetrated.[1] For instance, the offender was hired as a programmer in a large company in West Germany. Using the program that was written in the list, they had also found access to some items of information regarding the wage of non-real persons and to the memories of the data storage and also their accounts as the destination account

Citation: Pourghahramani B. An elaboration on computer frauds from the perspective of Iran's law and international instruments. *Forensic Res Criminol Int J.* 2018;6(2):107–114. DOI: 10.15406/frcij.2018.06.00192

to which the wages of these unreal people must be transferred. The most known manipulation is the "salami" fraud processing (Italian sausages) in which one program collected small amounts of accounts while group processing was being carried through deducting a small fraction and placed the obtained money in a hidden account belonging to the offender.[16]

In addition to the cases above, the legislator has used the term "and so on", and refers to the fact that the examples mentioned in this Article are not limitative and in any form that the person has used a computer system and appropriated property, computer fraud has taken place.

The conditions for perpetration of computer fraud crime

In traditional fraud, there are three important conditions for its perpetration: 1- the fraudulent nature of the devices used by the fraudulent person, 2- deception of the victim, and 3- appropriation of other people's property. Now the question posed is whether the aforementioned conditions are also necessary for perpetration of computer fraud. However, it should be primarily noted that if the computer acts as a device for deception and appropriation of another person's property, no damage is leveled to the aforesaid conditions and in order to perpetrate fraud the aforementioned conditions must be achieved; yet when computer fraud refers to the specific sense of the word, in this case, the aforementioned conditions must be reflected. Regarding the first condition (appealing to fraud), it must be said that unlike traditional fraud, in computer fraud such a condition has not been specified; yet it can be said that according to Article 13 of the Computer Crime Act and using the statement "illegal…committing acts like input,…" and also according to the Budapest Convention and recommendations of the Council of Europe, it is observed that the aforementioned statements indicate fraud, and therefore in computer fraud also, somehow an appeal to fraud is a prerequisite for its perpetration, since there is deception in the existence and basis of fraud and in the absence of this condition, no crime under the name of fraud will take place.

Therefore, if the actions set forth in Article 13 of the Computer Crime Act i.e. input, alteration, deletion, creation and suppression of the data or other interferences with the computer system are not present, computer fraud will never be committed. In other words, if the offender did not take the aforementioned measures, the computer system would not be misled allowing for someone to appropriate property or take advantage as a result; hence, the examples of fraudulent operations in computer fraud crime refers to the appropriation of money or property through providing unlicensed and secret computer programs or through fraud in the computer system. The second condition in which there is also a basic conflict is the problem of deception of the victim, and in Article 1 of the Law of Resonance this condition has been mentioned. However, in the law related to computer crime, this condition is not mentioned. In this instance, it is believed that the deception of the victim of the fraud crime requires the commitment of this crime only against a human and therefore machines may not be deceived.[2] Moreover, in computer fraud people are not in contact with one another so as to be able to deceive or trick one another, and, due to the lack of this condition in computer fraud, it has also been argued that perpetration of fraud is ruled out, and only it may be proposed in the law related to fraud.[8]

The final condition that is proposed in traditional fraud is the appropriation of the property of others. At this point it is appropriate to ask: Is the existence of this condition also necessary in computer fraud? In traditional and classic fraud there is no vacuum regarding the E-commerce Law since the relevant laws have stated the explicit sentence but, with regard to computer fraud, in the specific sense of the word, it seems that such a stipulation does not exist as is deduced from Article 13 of the Computer Crime that states: "…appropriates money or property or benefits or services or financial advantages for oneself or others, in addition to returning the property to its owner…" (page 12) that the fraudulent person does not need to appropriate anyone's property; yet simply when the offender appropriates property for themselves or others (even though it does not belong to anyone) by actions such as input, alteration, deletion, creation or suppression of data or any form of deliberate interference with the system, computer fraud is committed. For instance, if by entering a centralized system of bank accounts that the offender receives money from a blocked bank account or transfers it to their other account, in this example, no one's property is taken, yet they have appropriated property for themselves or others. Such an action should not be considered as fraud since in the existence and basis of fraud "appropriation of another person's property" is a prerequisite for fraud to happen. Yet maybe the term "rejecting the property to its owner" can be used by which the legislator has meant appropriation of the property of "another person"; in other words, property must have an owner for which to become the subject of computer fraud; otherwise, the aforementioned crime cannot be committed. Nevertheless, Article 13 of the Computer Crime Act is ambiguous in this regard. Therefore, in order to eliminate the defect and ambiguity, the phrase "appropriation of another person's property" must be added to the context of the aforementioned Article.

Obtaining criminal results

In fraud, the mere resort to the fraudulent devices is not adequate for perpetration of crime; rather, the aforementioned crime is among the conditioned crimes and obtaining a specific result is necessary for its perpetration. The result in which, based on the stipulation of the law, refers to the "appropriation of money or property or benefits or services or financial advantages" (page 11), and therefore, the appropriation of another person's property requires two things; one is to cause financial damage to a victim (whether the actual or legal person) and the other is the financial gain of the fraudulent person or the person considered by them. This condition has been explicitly cited in the regulations related to computer fraud; for instance, in Article 13 of the Computer Crime Act it is stated that "they should appropriate money or property or benefits or services or financial advantages for oneself or others"; this statement is greatly influenced by Article 1 of the Law of Resonance. The cases mentioned in Article 13 have a wholey financial aspect; therefore, if by taking the aforesaid measures in the Article someone enters the computer system of the university and succeeds to obtain an academic certificate for themselves or others, charging such a person with the computer fraud will be impossible; although, other crimes might happen in these cases or the offender might ensure to compensate for the civil damage.

A point can be mentioned in this section; that is, obtaining another person's property must be the result of interferences that are conducted in the computer system; in other words, there must be a causality between fraudulent actions and the appropriation of another person's property. Thus, if the offender conducts their fraudulent actions but cannot appropriate any property but the property is entered the bank account of the offender for example though another way, the offender

Citation: Pourghahramani B. An elaboration on computer frauds from the perspective of Iran's law and international instruments. *Forensic Res Criminol Int J.* 2018;6(2):107–114. DOI: 10.15406/frcij.2018.06.00192

cannot be charged with the computer fraud; also, if by penetrating into the bank system of the bank account of a person in order to damage them, a person just decreases their money as the offender has not appropriated any property for themselves or others, they cannot be considered as fraudulent.

The crime commitment device

Crime of fraud is one of the crimes that are committed by the computer. The device (computer) in this crime is one of the constituents of the material element, and the statement "…computer or telecommunications systems…" set forth in Article 13 confirms this. A point worth to mentioned here is that the legislator has also considered commitment of the actions set forth in Article 13 by "telecommunications systems" as part of computer crime. However, this case cannot be considered as the Absolute computer crime; for instance, when a person takes the aforesaid measures by the mobile phone. The title of the third chapter that is "computer-related frauds".

Intellectual element

Computer fraud, like traditional fraud, is among the deliberate crimes that ensure the existence of a general and specific ill will. General ill will refers to deliberation in committing fraudulent actions, or in other words, the intention to resort to fraudulent devices including input, alteration, creation or suppression of data or any interference with a system, etc., as it was formerly said that the aforementioned actions are indicative of fraud. Hence, due to the awareness of the offender regarding the "illegal" and "fraudulent" nature of the actions, as a result, it is a prerequisite for the perpetration of computer fraud crime; if the offender by mistake comes to think that they have the right to take actions and access the result, although they take the aforementioned measures on purpose, crime will not be committed.[7] Also, specific ill will refers to the will to appropriate money or property or services or financial advantages; in other words, it is the will for the result of crime. Therefore, if someone does not want the aforementioned result, the person's action is not considered as computer fraud.

Computer fraud penalty

The penalty determined for computer frauds depends on how it is looked at:

As was observed, regarding computer fraud, in its general sense, there are some different regulatory elements, each of which, can be investigated; yet, what is considered here is fraud in the specific sense of the word or fraud set forth in the Computer Crime Act. According Article 13 of the aforementioned law: "anyone who appropriates money or property for themselves or others illegally via computer or telecommunications systems, in addition to returning the money to its owner they will be sentenced to one to five years' imprisonment or to twenty million RLS' fine or both". Compared with traditional fraud, as computer fraud takes place mostly in cyber-space, its main penalty is low; however, in Article 26 of the aforementioned law[5], this defect has been to some extent resolved. The prescribed penalty for the computer fraud crime is specific to real persons and when this crime is committed by actual persons, the penalty for crime will be aggravated based on Article 19 and Article 20 of the aforementioned, Law of Resonance. Finally, it should also be noted that compared with the traditional fraud law, this law is specific, and therefore, unlike traditional fraud there is no obstacle for the reduction, conversion or suspension of the penalty.

Conclusion and suggestions

i. Computer fraud, in its general sense, has emerged in today's law in three forms: 1: fraud in which the computer is merely a crime commitment device which is in fact based on Article 1 of the Law of Resonance. In other words, such a case is traditional and not computer fraud. 2: Computer fraud in the context of electronic exchanges, which is considered as a specific law and is based on Article 67 of the E-commerce Law; and 3: Absolute computer fraud set forth in the Computer Crime Act.

ii. Computer fraud, in the specific sense of the word, which refers to the fraudulent use of a computer system by taking fraudulent actions set forth in the law and by the appropriation of another person's property by appealing to previous outlined methods or intentions.

iii. Computer Crime Act Policy that is derived from international documents and recommendations corresponds to the concept set forth in the Computer Crime Act.

iv. Compuer fraud is substantively different from the classic fraud in some cases. For instance, in classic (traditional) fraud, deception of the victim is the main prerequisite for committing the crime; but in computer fraud, appropriation of property is conducted through deception in the data and deceiving the victim is not a prerequisite. However, the fraudulent nature of the devices used and also appropriation of property and money is common in both types of fraud.

v. Article 13 of the Computer Crime Act has not referred to computer fraud and has referred to "computer-related fraud" only in the title of the chapter. According to the legislation method, the point argued in determining the criminal title cannot be [computer fraud] and therefore the court cannot charge the accused with computer fraud.

vi. Article 13 of the Computer Crime Act does not explicitly refer to the prerequisite of "deception", which is ambiguous, and thus, amendment of the Article seems necessary in this regard.

vii. Article 13 of the discussed law does not refer to the "appropriation of another person's property" and has merely referred to the appropriation of money or property, while the basis and the nature of fraud appropriation of another person's property is considered as a basic prerequisite. Therefore, the aforemtentioned law can be criticized in this regard.

viii. Computer Crime Act is not a Absolute computer law; rather, the crime committed by telecommunications systems is also included in this law; howver, the title of the law does not express this.

ix. Article 13 of the Computer Crime Act can include all frauds and it seems that due to existence of this las, Article 67 of the E-commerce Law is not required; however, Article 13 of the discussed law cannot exclude Article 67 of the E-commerce Law.

5 Article 26-In the cases below, the offender will be sentenced to more than two-third of at most one or two penalties appointed:

A)……

H) When the crime is committed at a broad level.

Citation: Pourghahramani B. An elaboration on computer frauds from the perspective of Iran's law and international instruments. *Forensic Res Criminol Int J.* 2018;6(2):107–114. DOI: 10.15406/frcij.2018.06.00192

Acknowledgement

None.

Conflict of interset

None.

References

1. Ulrich's Z. Cybercrime. 2004.
2. Alipour H. Cybercrime. *Journal of Legal Studies*. 2004;6.
3. Dezyani MH. Cybercrime. *Informatics Newsletter*. 1995;62.
4. Mirmohammad Sadeqi H. Crimes against property and ownership. 12 ed. Tehran: Mizan Publications; 2005.
5. Habibzadeh MJ. Specific criminal law, 3rd ed. Samt Publications, Tehran; 1995.
6. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
7. Khorramabadi A. Cybercrime from an international perspective and the situation of Iran, Law Quarterly. *Journal of Faculty of Law and Political Science*. 2005;2.
8. Goldouzian I. Specific criminal law. University of Tehran Publications. 11th ed. 2005.
9. Kshetri N. Diffusion and effects of cyber crime in developing Economices. *Third World Quartely*. 2010;3(7):1057-1079.
10. Bay H, Pourqahremani B. A jurisprudential and legal review of cybercrime. Publications of Institute of Islamic Science and Culture, Qom.
11. OECD. Org. (2016).
12. Hasan BI. Rights and security in cyberspace. Tehran, Abrar International Research Institute for Contemporary Studies. 2005.
13. UNCGIN.org. (2016a).
14. UNCJIN.org (2016b).
15. Dezyani MH. Cybercrime in terms of specific criminal law. *Informatics Newsletter*. 1996;(64).
16. Wilding E. Cybercrime. 2000.

Citation: Pourghahramani B. An elaboration on computer frauds from the perspective of Iran's law and international instruments. *Forensic Res Criminol Int J.* 2018;6(2):107–114. DOI: 10.15406/frcij.2018.06.00192