An Elaboration on Computer Frauds from the Perspective of Iran's law and International Instruments

By

Dr Abbas ASGHAR
Faculty of Law
University of Tehran
Tehran Province
Tehran
Enghelab Square، Iran
Iran

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 settlement 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.

Key Words: fraud, computer fraud, computer crimes, cyber crimes, classic fraud

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. 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. 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 cybercrimes 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 cybercrime 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.

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 (UNCGIN, 2016b). 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 (UNCGIN, 2016a).

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 (Alipour, 2004).

B. Although some countries have not enacted a new regulation for computer fraud, by adopting a general regulation they have 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 (Alipour, 2004).

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.

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 (Dezyani, 1996).

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 (Goldouzian, 2005).

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 (Khorramabad, 2005). 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 (Ulrich, 2004).

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 (Ulrich, 2004). 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 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 (Wilding, 2000).

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. 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 (Goldouzian, 2005).

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" 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", 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 whole 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 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 be 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 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 (Khorramabadi, 2005). 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 to 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, 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 (Habibzadeh,1995) Article 26-In the cases below, the offender will be sentenced to more than two-third of at most one or two penalties appointed: When the crime is committed at a broad level. 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. Computer 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 aforementioned law can be criticized in this regard.

VIII. Computer Crime Act is not an Absolute computer law; rather, the crime committed by telecommunications systems is also included in this law; however, 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 these laws, 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.

REFERENCES

Alipour H. (2004). conceptual relativity of terrorism from the perspective of jurisprudence. J Stracts stud. *Journal of Legal Studies*. pp.6.

Bay H, Pourqahremani B. A *Jurisprudential and legal review of cybercrime*. Publications of Institute of Islamic Science and Culture, Qom.

Budapest, (2001) Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States

Dezyani MH (1996). *Cybercrime in terms of specific criminal law.* Informatics Newsletter. 1996;(64).

Goldouzian I (2005). *Specific criminal law*. University of Tehran Publications. 11th ed.

Habibzadeh MJ (1995). *Specific criminal law, 3rd ed*. Samt Publications, Tehran;

Hasan B. (2005). *Rights and security in cyberspace*. Tehran, Abrar International Research Institute for Contemporary Studies.

Khorramabadi A (2005). Cybercrime from an international perspective and the situation of Iran, Law Quarterly. *Journal of Faculty of Law and Political Science*.;2.

Kshetri N. (2010). Diffusion and effects of cyber crime in developing Economices. *Third World Quartely*.;3(7):1057-1079.

Mirmohammad Sadeqi H (2005). *Crimes against property and ownership*. 12 ed. Tehran: Mizan Publications;

OECD. Org. (2016). *Development Co-operation Report:* The Sustainable Development Goals as Business Opportunities. Available at https://www.oecd.org/dac/development-co-operation-report-2016.htm

Ulrich's Z. (2004). *The Legal Aspects of Computer Crime*. Report at The Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Havana, Cuba, p.16.

Wilding E. (2000) fraud and the computer. *The white papers, association of certified fraud examiners,* 19, 43-47.