

Criminal Responsibility of Individuals in Cyberspace Law of Iran

Seyed Nematollah Mousavi

Department of Criminal Law and Criminology, Allameh Tabataba'i University, Faculty of Law and Politics (Judge of Tehran Province Justice Administration)

Behzad Razavifard

Department of Penal Law & Criminology, Allameh Tabataba'i University
*Author for Correspondence

Doi:10.5901/mjss.2016.v7n3s2p198

Abstract

Cyber space or virtual environment is one of the concepts that have been recently considered by criminologists and lawyers. At the same time with the creation of this environment, there are some crimes taking place in it and using it and therefore, the legal fight against these crimes requires taking some significant steps. The first crime was criminal behavior. However, the criminalization without creation and proof of criminal liability is deemed to be almost pointless. Perhaps it was on this basis that the legislator of the law in Iran has emphasized on the criminal liability of legal entities regarding the cybercrimes and explicitly targeted the criminal liability of legal persons for the first time Iran. However, the issue of criminal responsibility and explaining the scope of computer crime law has been of great importance. Many questions may be raised about the extent of the responsibility of individuals in a virtual environment. Legislator of Iran has allocated the sixth season of the computer crimes law to the subject of criminal liability and the most important changes that have been made in the above-mentioned law is to identify and establish criminal liability for legal persons in the virtual environment.

Keywords: Cyberspace, cybercrime, criminal liability, criminal liability shall agents

1. Introduction

Today, the use of modern means of electronic communication has created a lot of changes in all aspects of human life. It is obvious that the criminal law field have also been experiencing great changes in this regard. The most important impact that technology has had on criminal law has been creation of new opportunities for crime and thus supporting new horizons of criminal offenders, and establishing criminal responsibility. Various crimes may occur in the Internet environment and as a result many criminals may commit crimes on the Internet. Lack of coordination between criminal law and these types of phenomenon means lack of criminalization of offenses that occur in the Internet environment, lack of responsibility for the offenders who use the environment for their criminal behavior and interests which in turn certainly provides a great way to commit crimes on the Internet and cyberspace .

Accordingly, it should be noted that technological progress should be able to prevent and combat crime based on the criminal law. So the most important issue facing the criminal systems of law is to create and accept change in order to combat various offenses which are committed using the Internet or occur in a virtual environment. The issue of identifying the criminal responsibility for perpetrators who are committing the criminal behavior on the environment is one of the most important issues that should be considered after an act of crime is committed, the issue which will be explored following the purpose of the present research.

1.1 Part 1: Concept of cyberspace

One of the fundamental rights of individuals is to have privacy and the right to communicate such information to others. People, inevitably have to have a series of relationships in their private, public, familial and occupational lives, the nature of these relationships are typically not covered from someone and it is basically no fault to know these types of information, but everyone absolutely has their own personal issues and the necessary condition is to be secrecy and non-disclosure .

Non-disclosure of private and personal information on social issues is expressed as a right for everyone and

people are obliged to follow it. Entering to the private life of others in any way is morally reprehensible and legally under the responsibility. Today information technology developments have created a situation in which the issue of securing the personal and intelligence information of people is threatened more than ever. Computer science and information technology is not only threatening personal information or images of people's family but this knowledge may be used to violate other issues backed by legislation .

For example, insults and obscenities are the permanent process of all the communities and motivation of the person committing it is to humiliate others through crushing their cultural value. Article 31 of the Press Law asserts that vilification is not only worthy in personal relationships but it is also an expression of a decadent culture through the press and media. Similarly, disclosure and exposing the weaknesses of others are the other cases used in defamation and it can be committed through computer systems and the Internet .

In all these cases, using information technology and the Internet, will lead to the violation of the values supported by the legislator but what the cyber or virtual environment is and how it facilitates the committing of such crimes. So far, various definitions of virtual environments have been given and expressed. Some of these definitions have restricted the concept of virtual environment while the others have expanded it. According to one of the definitions of cyber space refers to the electronic information which is transferred through Internet (Davi D'Agostino, Greg Wilshusen, Defense Department Cyber Efforts: DoD Faces Challenges in Its Cyber Activities , DIANE Publishing, 2011 , p 28.)

However, other definitions have tried to express the distinction between the virtual and the network's cyber issues and from their point of view, the virtual environment is a data set that is stored in the computer storage and connected to other types through the Internet .(Ploug,Thomas, Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction , Ballerup Denmark , Springer pub : 2009 , p 70.) However, the network, or net has its own definition. Internet is a wide array of computers available in computer networks all around the world which are connected to each other through communication line and exchange information using certain protocols(Diana Holmes, familiarity with information technology, translation by Majid Azarakhsh and Jafar Mehrdad the publisher, Tehran, first edition, 1998, p).

Many computers have stored a lot of information available on the Internet and the huge volume of information is stored on the Internet. he information is stored on the Internet in different ways and therefore can be provided by a variety of methods and transmission.

Web or Webpage are one of the specific ways to save and store information in multiple ways and providing information on the Internet.

Unlike the old methods of storing and providing information which usually, store and transmit information in text format, Web page data storage is a graphical page for storing information working based on the system of "hypermedia". Hypermedia is a combination of "hypertext" and "multimedia". Now, if we mean that cybercrime happen, it indeed means that criminals Attempted to disrupt the information contained in the virtual environment using a computer or any other device that provides Internet access to them to obtain benefits for themselves. Therefore, all evidence of this crime can include various crimes; it could be unauthorized access.

Therefore, the article 1 of the computer crime law provides that: "Everyone has access to data or computer systems or telecommunications protected by the security access illegally, he is sentenced to the imprisonment of ninety-one days to one year or a fine of five to twenty million Rials or will be punished by both". The crime can also be falsified, as the above-mentioned Article 6 of the Law provides that: "Everyone who commits the following acts illegally is considered as a forger and is sentence to imprisonment from one to five years or a fine of twenty to one hundred million Rials or will be punished by both:

- A) To change of reliable data or create or insert fraudulent data,
- B) To change in the symptoms data or memory cards or processing in computer systems or telecommunications or chips or to create or to insert fraudulent data or their symptoms. Otherwise, it could be a crime against public morals

As Article 14 of the Computer Crimes Act provides: "Anyone who produces, uploads, publishes, distributes or deals with a computer or telecommunications systems or data carriers of pornographic content or writes or publishes or retains business or the production or storage will be sentenced to imprisonment of ninety-one days to two years or a fine from five to forty million Rials or by both."

Therefore, it should be noted that the majority of crimes can happen in cyberspaces and type of crime do not affect the cyber space and cyber-crime definition.

1.2 *Second Part: Definition and history of computer crimes*

1.2.1 *The history of the formation of cyber crimes*

The first computer was invented in 1937 in the United States. With the advancement of computer technology gradually some changes were made to the extent that different generations of computers term used to describe these changes. Today, communication with the computer will be possible via the audio and video. Information has been stored from the birth to be suitable for computers and will be used through the computer systems when necessary. The use of low-volume optical storage and memory capacity is the most inconceivable important characteristic of this generation.

The use of artificial intelligence and computer power of thought and inference are the other features of computers of the present generation and will not ended by changes in manufacturing computers but certainly will be followed by the changes in the technological and cultural changes also will follow, but what is cultural change and what effect will it have on human social life and finally what will be the impact it has on criminal law community?

In a general comment, it can be stated that computer crimes are considered as the twin to computer and crimes had also emerged with the use of computer. This definition is consistent with the definitions given by advocates of absolute justice school and sociological definition of cybercrimes but from the perspective of criminal law, a crime is an act that the legislator has been considered as crime. For example, after British police suspect a 23 year old young man who with a contact had suggested to a large computer company that instead of taking the funds to teach them how to get secret information from computers other institutions and his arrest was discovered as blackmail of an international gang robbery.

When the research was carried out, it was found that the young were familiar with a system that can obtain sensitive information from military and commercial computers. Moreover, this young man dealt with some information club in Germany and America and within a few years, has exchanged information with them in encrypted form. This young man using Kiel Ford computer system could obtain too much information from the information systems in the United Kingdom Ministry of Defence and NASA. The fundamental problem in the relationship with him was that his act despite considerable impact on national security of England was not considered as a crime at the time(Taheri Jebeli, M., "computer crime", Tehran, Justice Law Journal, Winter 1003, No. 9, p. 117.) and the young easily escaped punishment. Accordingly, regardless of the sociological definition of the crime at issue, we are going to see the background knowledge of computer crime.

From the international perspective, signing the conventions of cybercrimes by the Council of Europe's that took place on November 8, 2001 was the first step in the fight of international law against the phenomenon of cybercrimes. However, the former domestic legislation in the field of cybercrimes can be traced back to the period before 2001 in America which is considered as one of the pioneers in this field and between 1978 and 1986, 45 states of the country adopted computer crime laws .

The text of the law was consistent with the text of the proposed federal legislation(W. Brenner ,Susan , Cybercrime and the Law: Challenges, Issues, and Outcomes, University Press of New England, 2012 , p21.) . Finally, in relation to the legislative history of Iran with regard to cybercrimes, it should be stated that the history of law in the country in relation to computer crimes is related to the recent years that is 2009. The general computer crime bill was approved on 27 November 2008 with 176 votes in favor, 3 votes against and 2 abstentions. After resolving objections to this law by the Guardian Council, the Computer Crimes Act was approved by the Guardian Council in 17 August of 2009 (<http://www.itna.ir/vdcdsj0f.yt0xz6a22y.html>) .

Finally, the problem which can be considered in this regard is the effect of criminalization of cybercrimes in different countries regarding the development of computer science. As it was observed, the criminalization of cybercrimes in the United States of America which is the cradle of knowledge of computers has started much earlier than the rest of the world and is also crisscrossed gradually some other regions of the world such as Iran.

1.2.2 *The definition of computer crime*

In relation to the definition of cybercrimes, it should be said that the Iranian law has not provided a definition of computer crime, computer crime legislation has identified Iran has only defined in the domain extension while in the definition of computer crime provided by the federal police America, computer crime is any crime that it is committed by help of the computer(Nami, Mohsen, "an overview of computer crime", Tehran, correctional magazine, the third year, January 2004, No. 34, p. 53.).

It should be noted that definitions of computer crimes has changed due to misuse of computer-based definition and

today also encompasses other areas. It should be explained that the definition of computer crime at the beginning of the emergence of the crime was considered somehow as a white-collar crime that was committed only by certain people (McEwen, J. Thomas, *Dedicated Computer Crime Units*, DIANE Publishing, 1989, p1.). Finally, the definition based on computer-based definition was replaced by the above-mentioned definition and finally today it is believed that every crime that is committed using the knowledge and computer technology is considered to be a kind of computer crime. (op. cit.) The definition based on the use of computers cannot be valid while in the law of some other countries, some definitions have been provided for computer crimes which expand or limit the definition of this crime according to case depending on the policy makers in those countries against the criminal law offenses. In German criminal code section 202, legislation defines the offenses of computer crime that take place with the certificate number and password or to change in the system and software of a computer program. (Section 202c, Acts preparatory to data espionage and phishing, (1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible Page 95 of 157 1. passwords or other security codes enabling access to data (section 202a(2)), or 2. software for the purpose of the commission of such an offence, Criminal Code in the version promulgated on 13 November 1998, Federal Law Gazette [Bundesgesetzblatt].)

However, in German law as the law of our country, computer crime legislation has been defined in connection with the definition of the crime. For example, under section 263 A of the Act computer fraud has been defined or computer sabotage has been defined in Article 303 b. further, Article 1 of the Computer Misuse Act in the United Kingdom 1990 has provided full definition and interesting classification of computer crimes. By virtue of section one of this act, that is three raw articles, computer crimes are divided into three major categories:

- A) Unauthorized access to computer material.
- B) Unauthorized access with intent to commit or facilitate commission of further offences.
- C) Unauthorized modification of Computer material.

Paragraph one and two of article one have distinguished between a three alternatives among cybercrimes and unauthorized access to computer data that need to establish intent in criminal and absolute cybercrimes. (1.—(1) A person is guilty of an offence if—

- (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
- (b) the access he intends to secure is unauthorized; and
- (c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

- (a) any particular program or data;
- (b) a program or data of any particular kind; or
- (c) a program or data held in any particular computer. Computer Misuse Act 1990. Art 1.) Finally, with regard to the above-mentioned definitions, cybercrimes can be attributed to crimes which are committed using the knowledge of computer technology. This definition is the knowledge-based definition of computer crimes. (P. Madhava Soma, Umarhathab, Sundaram, Syed, *Cyber Crime and Digital Disorder*, New Delhi Tamil nadu, K. Jaishankar pub: 2011, p 21.) In other words, the need for specific knowledge of computer crimes has been emphasized because as it was said such crimes can be committed without using a computer.

1.3 Third Part: criminal responsibility in cyberspace

1.3.1 The concept of criminal responsibility

Criminal responsibility is one of the legal concepts that the authors have proposed many definition of it so far in criminal law. One of the authors of our criminal law has considered criminal responsibility as the general personal commitment to accountability for violations of the rights of others or violating the rights to freedom under Western and sometimes under the protection of collective rights and to protect the community .

Another authors, according to the definition of the word responsibility which means being obliged to work as a kind of sense of responsibility, has defined responsibility as a type of commitment and believes that in the realm of criminal law content of this obligation is to assume the effects of the actions Ardabili, Mohammed Ali, the rights of public crimes, vol. 2, Tehran, Mizan,, the nineteenth edition, 2008, p. 74. of the confidential, which more accurately means penalty which in the rules of the criminal justice system is to blame actions (Ardabili, Mohammed Ali, the rights of public crimes, vol. 2, Tehran, Mizan,, the nineteenth edition, 2008, p. 74.). It also means that criminal liability can be another view and

this is not to bind to assume the consequences of criminal activity that deserves to bear the consequences. (Rahmanpour, Abu Talib, the criminal liability of legal persons, Tehran, Imam Hossein University, 2013, p. 12.) Criminal liability in cyber space also means accepting the consequences of one's criminal act that occurred in the Internet environment so the concept of separation of responsibilities in cyber space has no other responsibility.

In relation to the criminal liability, legal entities have presented different opinions. Some authors have tried to deny it and others arguing that legal entities have real existence, crime committed against them is based capabilities and finally, some sentences can be used in relation to such persons, have believed that the legal entities have criminal liability (Rouholamini, Mahmoud, "the transformation of the criminal liability of legal entities in the French legal system", Tehran, Journal of Law and Jurisprudence, affiliated to the Institute of Islamic Thought and Culture, fourth, No. 16, Spring 2008, p. 133.) .

In many cases it can be noted that it presents the legislature's willingness to accept criminal responsibility for legal entities. Perhaps the Article 220 of the Commercial Code can be considered as a first step of taking responsibility by the legal entities whereby the partnership responsible for unregistered companies and action has been taken. Single article text on property owned by the parties dissolved is another example of accepting criminal responsibility of legal entities in the legal system Iran. (Damghani, Mohammad Taghi, "criminal liability of legal persons under Iranian law," the Tehran Bar Association Journal, June and July 1959, No. 65, p. 15 5)

And finally, computer crime law can be relied on in which criminal liability of legal entities is expressly accepted. From the perspective of the implementation of Article 10 of Palermo Convention which has been adopted by member states in connection with transnational organized crime, in this regard provides that: "1. Each State Party shall, in accordance with its legal principles, take necessary measures to establish the liability of legal persons participating in the commission of serious crimes in which an organized criminal group is involved. Further, the offenses 5, 6, 8 and 32 of the Convention will be considered. Liability of legal persons may be criminal, civil or administrative. These responsibilities do not undermine the criminal responsibility of individuals who commit these crimes (1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in serious crimes involving an organized criminal group and for the offences established in accordance with articles 5, 6, 8 and 23 of this Convention.) In Japan until 1932, only legal entities on behalf of its managers were responsible. Since 1932, the dual responsibility of the legal person shared responsibility was accepted. The most important penalties applicable in the legal system of the country against legal entities are fines (Kyoto, Ann "criminal liability of legal entities in Japan," Abdullahi Ismail, Tehran, Justice Law Journal, Winter 2003 No. 45, p. 180.) .

In America's criminal law, because of the complexity of social life, an industrial and commercial corporation has gained tremendous influence and importance and because of this criminal liability of legal persons has long been accepted (Glodouzian, Iraj, sacrifice, Abraham, "the criminal liability of legal persons in international conventions", Tehran, monthly hearing, August and September 2012, No. 93, p.). But what is the relationship between criminal liabilities as a legal concept with other responsibilities? The answer lies in the concept of criminal responsibility in addition to other responsibilities.

1.3.2 Criminal liability and civil liability

Responsibility is ranging from criminal and civil liability and is required to meet the person in charge and the responsibility is either due to fault or because of the loss of audience response into the community, or the injured and are intended to deter and punish the person responsible or to restore damaged items. However, the old legal system, and the purpose of the above-mentioned cases were not separated and the aim of deterrence and punishment of the responsible person is preventive and also causes compensation (Badini, H., Philosophy of civil responsibility, Enteshar Cp., 2005, p. 159)

And this shared past is only a milestone of the concepts of civil and criminal responsibility. From the late eighteenth century in most legal systems, the criminal and civil liability was separated both in terms of legislation and in terms of objectives and principles. For example, the most important basis for establishing criminal responsibility for the protection of collective rights was the rights of so-called adequate criminal liability happening in the relationship between people and the king (Wilson, Luke Andrew, Theaters of intention: drama and the law in early modern England, Stanford University Press, 2000, p 173.) .

However, the purpose of protection of the rights of civil liability is against the losses that may be noticed in the social relations of the actions of others. In addition, the responsibility of the mass of the population is due to the law and any harmful act cannot be considered as crime while the analogy is not permissible in Criminal Matters and the legality of sanctions against the government's guarantee of individual rights but the judge does not have civil liability for any liability of legal basis and acquired conditions (Katouzian, Nasser, requiring out-of-contract civil liability, vol. 1, Tehran, Tehran

University Press, Eighth Edition 2008, p 40) .

In addition, the scope of this responsibility is also different. Some of the crimes that have heavy penalties, because they do not cause damage to persons, are not associated with civil liability, so the existence and committing a crime does not lead to civil liability.

1.3.3 Criminal responsibility and international liability

According to Article 2 proposed by the International Law Commission in the field of states international responsibility, International violation of a state is established when an act or omission constituting the action is attributable to that State under international law and breach an international obligation of that State .

The international responsibility can be created only with the above two conditions. Therefore, that special groups to be described as a violation of international, they have to be attributable to the state and the second condition is that the act attributable to the state, it should be in violation of an international obligation. In contrast to deficit liability, the international responsibility has some major differences. First, unlike criminal liability that usually occurs for individuals, International responsibility is primarily for the states and is the most complete legal entity in to be created international law. On the other hand it is sufficient to establish the international responsibility or violation of rules of conduct contrary to international law and is not necessarily the existing treaties and international responsibility for governments .

However, the responsibility for your criminal responsibility should be according to legal provisions, or text reference of law. It should be noted that the issues surrounding the international responsibility of the state in the last twenty years has been debated more than anything else.

Committing some illegal activities that starters are applied to other categories of his international responsibilities. Such illegal acts, the government called international crimes. In fact, it should be noted that features international crimes in such a way that legal entities, particularly their states are more capable in but the Statute of the International Criminal Court do not block the way for the crime of these people and based on the traditional approach, only individuals have been responsible. However, the difference between the international and criminal responsibility is related to the person who is responsible in this case.

Fourth speech: criminal responsibility in computer crime law of Iran

Iranian legislator has devoted Chapter VI of the Computer Crimes Act to the issue of criminal responsibility. Perhaps the most important change that the above-mentioned law is established in relation to criminal liability is to identify and establish criminal liability for legal persons. Article 19 and 20 of the above-mentioned law are on the criminal liability of legal persons. Article 19 provides: "In the following, if computer crimes in the name of the legal person and in the interests of the offense, the legal person has criminal liability:

- A) If the director of a legal person commits an offense.
- B) If the director of the legal person issued the order computer crime, and the crime took place.
- C) If an employee of a legal person has committed a crime with the knowledge of the administrator or as a result of his lack of computer crime.
- D) If all or part of the legal person's activities is dedicated to computer crime

And Article 20 also stated: "legal persons referred to in Article above, according to the conditions and circumstances of the crime, the revenues and results of the crime, in addition to three to six times the maximum fine for the crime will be sentenced as follows:

- A) If the maximum sentence for the offense is five years imprisonment, temporary closure of the legal entity of one to nine months and in case of recidivism temporary closure of the legal person of one to five years.
- B) if the maximum sentence is of five years' imprisonment for the offense, the temporary closure of the legal entity of one to three years and in case of recidivism legal entity will be dissolved.

In this regard, a question may be raised that what do the Iranian legislators' emphasis on the criminal liability of legal persons entail? What will be the consequences of this emphasis?

One of the most important questions that may be raised in this area is in fact, the recognition of criminal liability for legal entities and its impact on the responsibility of individuals.

Is the legislative scheme of the principle of criminal liability to entail the legal entities? or to negate criminal responsibility of individuals in the cyber space?

Certainly the answer is negative given that the provisions of Article 19 that provides:

"Criminal liability of legal person will not prevent the punishment of the offender." That is, since, the legislator has devoted the first article of the sixth chapter of the computer crimes law to discussion of criminal responsibility; it does not

negate the criminal responsibility of individuals.

Another issue that must be considered in this category is the balance of responsibilities and accountability relationship for natural and legal persons. As we noted, the Article 19 did not consider criminal liability of legal entities as an obstacle to punish individuals but the text of the article is somewhat misleading, because it virtually does not mention the relationship between the two type of the responsibility. However, it should be acknowledged as long as someone does not take responsibility, it is impossible to impose penalties on them. The text of the aforementioned Note 2, at the same time means possible liability for legal persons and individual members of the set. Discussion of the relationship between individual responsibility and liability of legal persons, deals with various forms of the relationship between responsibilities. It should be noted that the responsibilities have shared history and their common roots. They are created due to serious breach of obligations generally against the society . (Bonafe.Beatric, *The Relationship Between State and Individual Responsibility for International Crimes* Hague ,martinus nijhoff pub : 2009 , p24.)

However, the two type of the responsibility have the same consequences. It should be mentioned that, the existence of common ground does not mean that the general rules of liability of natural persons are applicable in relation to the liability of legal persons. Here we can only point to the fact that the similarity of these two basic rules of responsibility means that both are created due to violation of the fundamental norms of community support. However, this relationship will fade secondary rules . (op. cit .p 24.)

However common understanding and communication among the responsible persons is the investigation of theoretical responsibility in this regard.

1.4 Fifth Part: The factors of disclaiming criminal responsibility in cyberspace

Criminal responsibility is the "commitment to undertake work or bear the consequences of criminal activity which is the punishment for blaming the actions of criminal justice; But to take offense at once, cannot bear the burden of his guilt, but before that, he deserves to be called to bear this heavy burden of the fault that has been committed, he had first considered and then he will be held accountable. The capability of accepting the blame on is called the lawyers' ability to assign and it has been defined as being subject to a perception of power and authority. So if criminal is not evident or authorized, he is not responsible for their actions. That there should be criminal liability in a strict sense of culpability of the offender commits a fault and the fault is attributable to him(Habibzade Mohammad Jafar, Fakhronab, Hussein, "comparing crime justified factors and factors preclude criminal responsibility", Tehran, professor of Humanities magazine, 2005, No. 40, pp. 41-42.) .

In these reasons, there is no criminal liability for the offender. In order to understand this concept the meaning of criminal responsibility must be understood. Criminal responsibility is defined as being responsible for crimes committed based on the crimes stipulated in the law and the person responsible to be one of the penalties provided by law, the victim of crime in the community. (Langroodi parsley, MJ, terminology of Law, Tehran, Treasure of Knowledge, 2007 p. 642, No. 5120.)

However, removal reasons of criminal liability would provide criminal Disclaimer

In these cases, despite the fact that the crime occurred but in that case the offenders person is not in charge of criminal and therefore the penalty will not be imposed on him. In relation to the substantive difference between the causes of the causes modal mass should be said:

Removal of criminal liability has a public and private, or internal aspect, and due to the physical or mental capacity and characteristics of the offense, and a manifestation of internal origin. While the causes of legitimacy due to external factors and conditions and perpendicular to describe an event that eliminates criminal act will be committed. Moreover, physical and mental characteristics of the offender have no role in it(Shambayati, H., former Page 314) .

The factor disclaiming the criminal responsibility includes the personal act whose scope is limited to the offense. That is, it would only be guilty of criminal responsibility and has no impact on the criminal liability of the partners while it is the causes of legitimacy to all the participants in mass actions. That is the legitimacy of the partners and also accessories. Regarding another difference between the two, it should be said that the spiritual element of responsibility shall have been met in the crime and thus a crime is primarily unrealized while the causes of disclaiming the crime is non-criminalization of crime due to legal element fix it by another text of the law, and from the point of view of the goal, it should be said that the reason for disclaiming the criminal responsibility does not eliminate the causes of the Civil Liabilit.

For the purpose of defining the rules of criminal liability as its title implies is to eliminate the Criminal liability for the loss of committing a crime which requires punishment that is subordinate to prove criminal liability in order to maintain order and social defense. And one cannot eliminate liability offense while Constitution not only causes deterioration of Criminal liability and civil liability to commit a crime and makes the criminal act legitimate; it also causes lack of criminal

liability and civil partners and also accessories . (Rahmanpour, A., former, Pages 92-91)

Iranian legislator pointed out in the cybercrimes law to the factors that shall not eliminate the criminal responsibility. Paragraph B of Article 19 refers to the order of the director's role in the crime agenda which actually refers to the causes of crime not the criminal liability. However, it should be noted that factors eliminating the responsibility in cyberspace are the functions if general factors shall be criminal liability. These factors can be found in subjects such as childhood, madness, spiritual force and others. Therefore, it should be noted that factors eliminating the responsibility in Cyberspace are the ones removing the criminal liability which is usually considered the general criminal law texts.

2. Conclusion

Using cyber tools and new means of communication, especially the Internet, has created new opportunities for crime offenders. In this regard, if the criminal law in any society fails to fit with these developments change, naturally there will be a lot of crime and delinquency which remain unpunished. Perhaps the most important new tools to fight crime against the criminal law, there are strategies such as crime, development of criminal responsibility, using new approaches to conflict resolution and new sanctions, etc.

In relation to criminal responsibility in Cybercrime legislation of Iran, an extension and expansion of criminal liability for legal persons has been done. Until the above-mentioned law the criminal liability of legal persons in question had not been considered in Iran's penal code and computer crime laws accepted the criminal liability of legal persons for the first time. It is known that many cybercrimes are usually located by legal entities and the legislator's action is perfectly normal in connection with establishing criminal responsibility for these individuals and in fact the use of new tools to fight crime is to expand criminal liability. However, it should be noted that :

- A) Criminal liability of legal persons does not mean the negation of the true person's responsibility.
- B) Criminal liability of legal persons does not create an obstacle to impose penalties on the individuals.

Finally, it should be noted that concerning the removal of criminal liability in cyber space, the causes are considered as the functions of the general factors removing the responsibility for factors such as childhood and the madness of these cases .

References

- Aalipour, H., "International Criminal Court and challenge the liability of legal persons", Proceedings of international criminal law theories and views, Tehran, 2011, Page 237
- Ardabili, Muhammad Ali, the rights of public crimes, vol. 2, Tehran, Mizan, the nineteenth edition, 1998, p. 74.
- Atul , Jain , Cyber Crime: Cyber crime : issues and threats , Gyan Publishing House, 2005 , p 121.
- Badini, Hassan, philosophy, civil liability, Tehran, Inc. Publishing, 2005, p. 159.
- Bonafe, Beatrice, The Relationship Between State and Individual Responsibility for International Crimes Hague ,martinus nijhoff pub : 2009 , p24.
- Davi D'Agostino , Greg Wilshusen , Defense Department Cyber Efforts: DoD Faces Challenges in Its Cyber Activities , DIANE Publishing, 2011 , p 28.
- Diana Holmes, familiarity with information technology, translation Azarakhsh Majid and Jafar Mehrdad, the publisher, Tehran, first edition, 1998, p. 5
- Habib Mohammad Jafar, Fakhrebab, Hussein, "comparing crime justified factors and factors preclude criminal responsibility", Tehran, professor of Humanities magazine, 2005, No. 40, pp. 41-42
- Hashemi Mohammad, human rights and fundamental freedoms, Tehran, The, 2005, pp. 286 -
- Helmy, N., international responsibility and political support, Tehran, amount, published in 2011, pp. 37-36
- <http://penology.blogfa.com/post-208.aspx>
- <http://www.itna.ir/vdcdsj0f.yt0xz6a22y.html>
- <http://www.modiryar.com>
- Jeff B. Zhang, Accusing the American Judicial System of Rampant Corruption ,Pittsburg Pennsylvania , Dorrance Publishing , 2011 , p 489.
- Katousian, Nasser, requiring out-of-contract civil liability, vol. 1, Tehran, Tehran University Press, Eighth Edition 2008, p 40
- Langroodi-Jafari, MJ, terminology of Law, Tehran, Treasure of Knowledge, 2007, p. 642, No. 5120.
- Maryna, Espidini "about possible crimes committed by the state and his criminal responsibility" Translator, Hanjy, Ali, Tehran, neighborhood legal research martyr Beheshti University, autumn and winter of 2006, No. 44 Page 77
- McEwen , J. Thomas, Dedicated Computer Crime Units, DIANE Publishing, 1989, p1.
- NamiMohsen, "an overview of computer crime", Tehran, correctional magazine, the third year, January 2004 No. 34, p. 53.
- P. Madhava Soma , Umarhathab, Sundaram , Syed , Cyber Crime and Digital Disorder , New Delhi Tamil nadu , , K. Jaishankar pub: 2011 , p 21.

- Ploug ,Thomas , Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction , Ballerup Denmark , Springer pub : 2009.
- Rahmanpour, Abu Talib, the criminal liability of legal persons, Tehran, Imam Hossein University, 2013, p. 12.
- Section 202c , Acts preparatory to data espionage and phishing, (1) Whosoever
- Shambayati, H., general criminal law, Tehran, again, fifteenth edition 2009, p. 22.
- Taheri-Jabali, M., "computer crime", Tehran, Justice Law Journal, Winter 1993, No. 9, p. 117.
- W. Brenner ,Susan , Cybercrime and the Law: Challenges, Issues, and Outcomes, University Press of New England, 2012 , p21.
- Wilson , Luke Andrew , Theaters of intention: drama and the law in early modern England, Stanford University Press, 2000 , p 173.