The Iranian Criminal Policy about the Crimes against the Authenticity and Integrity of Computer and Telecommunications Data and Systems

Seyed Milad Alizadeh Javaheri and Elham Fariborzi

Protecting the authenticity and integrity of the computer data and systems is among the objectives of criminal politics of the countries in the legislation and criminalization within the scope of information technology. These two principles are among the essential principles governing the protection of data and systems. The crimes occurring against the authenticity and integrity of data in the electronic environment are categorized in two categories one of them is computer forgery against the authenticity of data and the other one is computer impairment that includes the crimes against the integrity of data and systems. It covers four domains including data damage, system interference, access prevention and cyber terrorism. The main objective of this study was acquaintance with each of these crimes and identification of different reactive responses and interactive actions in social and legislative prevention and depiction of the model of the Iranian criminal policy against this kind of crimes. The research method is descriptive, analytical and library-oriented. The findings of this research indicate that, firstly, the nature of these crimes created by the modern computer technology is different from the traditional ones; secondly, the Iranian criminal policy model against such crimes benefits from the governmental models instead of social patterns in which the responses are given based on criminal system; thirdly, the Iranian legislative criminal policy, due to the lack of supporting the traditional criminal laws from computer data and system and in parallel with the rules of the Cyber Crimes Convention, has criminalized this kind of the crimes, and fourthly, the determined responses in statute laws, mostly are suppressive and they are the same punishments common in the classic criminal law such as imprisonment and cash penalty.

Keywords: Cyber crimes, Data integrity, Data authenticity, Computer forgery, Impairment

Introduction

After the computer invention, emerged computer crimes were inevitable because of the common usage of computer in personal life and social relations; therefore, crimes and breaching rules in using computer became unavoidable. The branch of criminal law about information technology is a newly-emerged field resulted from modern technology which has been created in two recent decades. As other new fields of study such as Environmental Criminal Law or Administrative Criminal Law, it analyzes computer crimes.

Seyed Milad Alizadeh Javaheri, Islamic Azad University - Mashhad Branch, Iran Email: milad Aj2001@yahoo.com
Prof. Dr. Elham Fariborzi, Islamic Azad University - Mashhad Branch, Iran. Email: elhamfariborzi@gmail.com,
In the classification done on the basis of amalgamated classification, the computer crimes have been classified in the four following categories¹:

1. The crimes against the authenticity and integrity of data and system such as computer forgery and impairment.
2. The crimes against privacy and confidentiality of the data and system such as unauthorized hearing.
3. The crimes against data or system accessibility such as unauthorized and illegal access.
4. The crimes commitable by computer which are classified in two categories including the crimes against individuals’ spiritual character and financial crimes such as degradation, publication of false statements, and fraud.

The abovementioned classification is the same categorization based on the computer role. Cyber Crimes Convention has used combined method. In addition to the mentioned convention, the Computer Criminal Law ratified in 2009 has also selected this method.

In cyberspace, we not only witness the routine crimes such as rubbery, fraud, spying and publication of false statements which occur in internet network similar to the actual environment but also we see new offences the subject of which is the actions against computer system and network security such as the crimes against confidentiality, authenticity and accessibility of the data and systems that are generally called cyber crimes².

To understand the computer crimes including the discussed crimes, at first, we should realize the values supported in cyber space.

Concerning the criminal policy of the cyber crimes including the crimes discussed in this text, in addition to criminalization, the criminal applicable cases find a great importance through legislating the criminal sanctions, resorting to interactive actions including social and legislative prevention by training the internet users in cyber space, promoting the technical approaches of system security, and recommending the users to employ protective and supervising actions.

Among the principals governing on the information technology and computer security is the data free-flow observing of which is possible in the light of respecting and supporting the confidentiality, integrity and accessibility of data and information. Therefore, the computer data in Cyberspace should be supported in the light of this principle. So, nobody can obstruct data free-flow without permission.

The authenticity and integrity of data and system are considered as the subordinate of the principles supervising data protection. The authenticity principle is among the fundamental principles dominating on data in Cyberspace which is a qualitative principle and supervises the data content. Lack of data authenticity is always considered as risk for computer users’ information and personal privacy.

Concerning data integrity, the most important crime is forgery and use of the forged data. Because of insufficiency of the regulations of traditional criminal law about classic forgery that only supported the written documents, the Iranian new

regulations for protecting electronic data and documents were legislated based on the regulations of electronic trade law and computer crimes law. Among other principles supervising the data support is the principle of data massage integrity and documentation. This principle is concerned with the data and system integrity and nature and protects from the data entity (Aalipour, 2011, 198). Computer impairment includes data damage; interfere in system, computer sabotage which are more important than other ones due to their novelty. With respect to this fact that the former regulations were legislated in order to support the materialized and tangible things and were not enforceable in the field of information technology, many countries such as Iran have legislated criminal laws in this area.

Lack of specific studies and researches about these computer crimes and studying them only in some books generally as well as no access to a complete collection for usage, the novelty of the subject, lacking the former researches to which may be relied on, close correlation with the topics within the scope of information technology, and specialized communications and literature of this kind of crimes are among the problems and obstacles of this research.

The purpose of writing the present article is studying the crimes against the authenticity and integrity of the computerized data and systems such as computer forgery and impairment in the statute laws, depicting the model of the Iranian criminal policy in the field of cyber crimes, presenting the preventive approaches against this kind of the crimes and describing the suppressive responses in the form of legislators' policy making which can serve as an important source for the lawyers, judges, technicians and computer users.

Research Review Historical Survey International Documents:

Various forms of computer crimes especially data and system forgery and impairment which are among the crimes against the authenticity and integrity of data have international dimensions and attack information interests throughout the world, therefore, the international organizations have rendered wide attempts to classify this kind of crimes in order to get international consensus for identifying the abovementioned crimes and preventive procedures; in addition to the fact that each of different countries have taken measures for classification according to their social, economical and cultural characteristics and their legal infrastructures (Pakzad, 2005, 81).

In the beginning, the inter-governmental and regional societies and organizations consisting of developed countries such as America, Germany has studied this classification. After wide usage of the computer systems all over the world, more important societies such as United Nations have published some documents the evident characteristic of which is focusing on wide misuse of computer systems and attempting in taking uniform measures against such misuse by the member and non-member countries. (Jalali Farahani, 2010, 148).

Economical Cooperation & Development Organization, European Council, International Society of Criminal Law, and International Criminal Police Organization have presented recommendations about entering, changing, deleting, and stopping data as well as spreading virus which are the components of the computer forgery and impairment (Bay and Poorghahremani, 2009, 82-86). With respect to the wide aggression in the electronic environment and computer network, the European
Council ratified the Cyber Crime Convention which is reflected in the Article 4, interference in data, Article 5, interference in system and Article 7, forgery concerned with computer in compliance with the necessity of taking a public criminal policies against cyber invasions such as ratifying suitable rules.

The Iranian Laws

The first legal reaction concerning this kind of cyber crimes was enforced by ratifying E-business Law on Seven, January, 2004 in which the legislator considers computer forgery as a crime only within area of E-business and trading exchanges. The second legislator's reaction and the most comprehensive rules against cyber crimes were ratified in 2009. In a separate chapter, in supporting two principles of the authenticity and integrity of data and computer system, the legislator criminalized computer forgery, data destruction and computer systems, access prevention and cyber terrorism.

Criteria, Principles and Philosophy of Criminalization

With respect to the justification employed by criminal policy in using suppressive actions for campaigning against crimes with different natures the criminalization can be effective and may act as a pain sedative similar to surgery; although it may be harmful and inefficient in the same rate and it is the criminal policy which may act as a guidance. The direct relation between criminalization process with citizens' rights in a society demonstrates the strong need to this policy so that while preserving social values, the personal interests are also respected (Mahmoudi Janki, 2003, 22). If we consider criminal law as forcible regulation of social relations, the method of selecting moral rules by government relates to criminalization. This process requires:

1. Determining the criminalization principles including moral, religious and political principles for justifying punishment necessity. 2. Specifying the criminalization criteria in the form of the principles and rules for determining the manner of criminal reaction. 3. Variation of criminal subject and values regarded by the legislator, separating the material and mental elements regarding the intensity of crime traces and identifying the different types of offenders and victims for determining the type of punishment in the course of an integrated criminal policy. (Hassani, 2006, 22).

Criminalization in the cyber environment is different from criminalization in real one in different aspects. It is different because excluding the principles, criteria and fundamentals of criminalization in real space including loss, moral proposition and legal patriarchy, some other issues should also be regarded; without them, no suitable criminalization may be enforced.

General Criteria of Criminalization in Cyberspace

Professor Ulrich Sieber has described criteria for criminalization principles in Cyberspace in six paragraphs as follows:

The principles of criminal law as the last resort, accuracy in definition, transparency and no need to any reference, differentiation and distinction, intentional crime and crime forgiveness which have been emphasized in international documents including the Recommendation Letter No.R (89) 9, issued by the European Council.
Answering the question that in what extent the general criteria of criminalization in virtual space have been observed by the Iranian legislator for approving the regulations concerning this kind of crimes, it is mentioned that, firstly, about legislative prevention, using protective and supervising actions have been emphasized by the judicial authorities as the pioneer measures for protecting personal data and systems, secondly, this kind of crimes are prosecutable when they are committed intentionally, thirdly, with respect to the principle of crime unforgivable, it seems that this kind of crimes are being unforgivable and need no victim’s complaint, fourthly, in the regulations concerning the computer crimes, when the legislator uses the terms such as electromagnetic waves, optical waves and data cryptography without presenting any clear definition, he/she has ignored the principle of transparency, fifthly, the principle of crime typicality has also been observed by the legislator so that in the separate articles under the topic of the crimes against the authenticity and integrity of data, different criminal actions have been criminalized.

Special Criteria for Aggression to Personal Data and Systems

Special criteria for criminalization of the aggression to individual’s data and systems are not enforceable for all persons, sectors, and all data identically and the natural and legal entities’ data are not of the same importance and all data belonging to one person have not equal value. This principle of difference in criminal protection of data based on the data classification should be considered as one of the special criteria of criminalization (Hassani, 2005, 83). Careful study of the Computer Criminal Law, especially, the discussed crimes, indicates that the legislator makes no difference between ordinary and important data and has taken the same decision about all data and systems; in this regard, she/he has acted contrary to the principle of protecting data based on the data classification and paid more attention only to the computer and telecommunication systems which are used for more essential services and has intensified their punishment.

Criminalization Philosophy

Computer systems and Cyberspace have provided the facilities for committing common crimes more effectively. Although the tools and method of committing crime has no effect on the corpus delicti but sometimes the scope and rate of the damages resulted from employing computer systems in committing traditional crime are so extent that the legislator is obliged to enforce intensified punishment based on new criminalization against the crimes. (Sa’ dinegad, No.2, 36).

On the other side, computer systems have created new elements that have changed the corpus delicti in the field of crimes. From far past, whatever is considered as the property is the tangible and observable thing and the criminal laws have been ratified for protecting these things but today some other elements have found value which have not the same characteristics. The abovementioned factors encourage the legislator to legislate new regulations within the above scope.

In addition to the internal policy makers’ interests, the international considerations and obligations have also obliged the governments to consider some behaviors as the criminal actions; so, some criminalization have been created with inspiration from international conventions or due to joining them to the existing laws and accepting them by governments. (Mahmoudi Janki, 2003, 202).
Iran affected by European Convention for Cyber Crimes has also criminalized these crimes.
Whereas, nowadays, many human activities has transferred from ordinary to Cyberspace; this space have penetrated the private territory of individuals and has found more importance compared with the physical space because privacy is concerned with information and the role played by information in the Cyberspace is undeniable. So, what is concerned with the Cyberspace is included in communicative and informative private territory.
Informative private territory which has been studied in many legal systems under the title of data protection includes the rules for processing data and information related to the persons. Processing means any acquisition, maintenance, organization, saving, correction, and other similar actions about data (Noori and Nakhjavani 2004, 23). Informative private territory means immunization of personal life data and preventing acquisition, saving and processing personal data which is expected that other people have no access to them without the individual's permission. It is also called as data security (Aslani, 2005, 92).
Among other areas of the private territory which should be protected is communicative private territory. This area of private territory covers the individuals' rights for their secured and integrated correspondences and telecommunications. Nowadays, in addition to protecting letters from any damage, forgery, and inspection, following the emergence of new forms of correspondence such as e-mail and satellite communications, the communicative private territory includes the technology of all of correspondences within the digital networks such as undesirable internet and e-mail (Ibid.145).
-Modern computer technology facilitates and propagates criminal actions within computer environment, therefore, the Iranian legislators because of worry about the probable misuse of information and private relation between persons has criminalized the discussed crimes in order to protect the informative and communicative private territory.

Criminal Applicability

One kind of this sort of computer crimes is computer forgery. This offence has an extent relation with the progresses resulted from information technology and it is considered as a crime based on superior technology. Therefore, in the international documents it is included in the category of the crimes concerning with computer. In the phenomenology of computer forgery, this offence on the contrary to fraud which is committed in order to incur damages to the properties and acquire financial privileges, it often occurs for forging the judicial and electronic documents in order to change them and cheating (Bastani, 2004, 45).
Concerning this, Professor Susan Berner has said "the forgery nature is tampering with the documents in order to cheat; in the past this tamper was done in the paper documents but nowadays it occurs in both paper and electronic documents.(Talebi 2009, 55).
The first law that criminalizes computer forgery is Electronic Trade Law ratified in January 07, 2011. The application domain and context of this law is only concerned with the electronic trading exchanges and does not include outside this scope. According to the article 68 of this law, anybody who forges the messages with financial and documentary value in electronic exchanges through entry, change, removal, and stopping of the messages and intervention in processing of message
data and computer systems or using the applications employed in signature cryptography systems (such as a specific key) without the permission given by the signatory or signing without any record in registration book of electronic documents or inconformity of the applications with the holder’s name in the list as well as obtaining forged certificate, etc. will be considered as a forger and he/she will be convicted to 1 to 3 years of imprisonment and should pay a cash fine amounting to 50 millions Rials.

The second law that criminalizes the computer forgery is Computer Crimes Law. According to the article 6 of this law anybody who takes the following measures without any permission, will be considered as a forger and he will be convicted to 1-5 years of imprisonment or cash fine from 20 to 100 millions Rials or both sentences:

A. Changing or creating documentary data or adding other forged data to it.
B. Changing data or the signs existing in memory cards or the ones that may be processed in the computer and telecommunications systems or chips or creating and entering forged data and signs in them.

One of the other kinds of computer crimes is computer impairment. This crime occurs against the integrity of computer data and systems. Computer impairment covers any behavior which destroys data wholly or partially or disrupts the data or system efficiency. The term “sabotage” has a history in the Iranian criminal legislation and it is also included in the topic of the Punishment Law For Disruptors in Security of Airplane Flight for impairing air devices and installations ratified in 1970. If this term is used for individuals, society and security it includes destruction, vandalism and terrorism respectively (Hassan Beigi, 2005, 226).

This topic includes four criminal titles predicted in the Computer Crime Law: data impairment, system interference, access prevention and cyber terrorism.

**Data impairment:** The article 8 of Computer Criminal Law indicates that anybody who deletes, impairs or disrupts the other’s data through computer or telecommunication systems or data carrier or causes them not to be processed without any permission, he/she is convicted to 6 months to 2 years of imprisonment or cash fine of 10-40 millions Rials or both sentences.

**System Interference:** Anybody who disrupts the other's computer system through entering, conveying, spreading, deleting, stopping, forging, or impairing electromagnetic or optical waves of the computer systems belonging to others without any permission, he/she will be convicted to 6 months to 2 years of imprisonment or cash fine amounting to 10-40 millions Rials or both sentences.

**Access Prevention:** The article 10 of Computer Crimes Law indicates that anybody who commits unauthorized actions such as hiding data, alteration of password, or cryptography of data prevents the authorized persons to have access to the data or computer and telecommunications systems will be convicted to 91 days to 1 year of imprisonment or cash fine amounting to 5-20 millions Rials or both sentences.

**Cyber Terrorism:** The article 11 of Computer Crimes Law indicates that anybody, intending to endanger public security and convenience commits the actions mentioned in the articles 8, 9 and 10 of this law against telecommunications and computer systems which are used for necessary public services such as treatment, water, electricity, gas, telecommunication, transportation and banking, he/she will be convicted to 3 to 10 years of imprisonment.
Responses and Sanctions System

Criminal policy is defined as a series of methods which the legislators organize the reaction to criminal phenomenon by resorting to them (Delmas Marty, 2002, 23). According to the abovementioned definition, the criminal policy consists of different forms of social control among which criminal law is of special importance and position. But this doesn’t mean their exclusivity in the domain of criminal policy. Nowadays, the tools of social control are so various and include a wide spectrum of non-criminal methods such as preventive, social and legislative responses and other non-suppressive measures.

So, with respect to the fact that the criminal policy is studying epistemology of criminal phenomenon and analyzing that and the tools applied against crimes (lazerges 1996, 24), the main under-study subject in this text is “the tools for enforcing criminal law concerning with the crimes against the authenticity and integrity of computer data and systems in two areas of reactive and interactive actions.

Reactive Responses and Punishments

When the crimes and anti-social norm behaviors are committed, the criminal justice system, while preventing the crime commitment, is bound to alert the people about the necessity of observing regulations through resorting to the suitable and effective methods. This alert given by the public authorities of the society about preserving public systems has different forms the emphatic of which is punishing the law offenders.

For the most computer crimes including the discussed crimes, the determined punishments are the same as the common imprisonment and cash fine for which the judge, according to the kind of crime, offender’s record, and the rate of damage resulted from committing the crime, determines the suitable sentence.

In this law, contrary to the most criminal rules, it is attempted to establish a harmony among penalties. Considering the average salary of an Iranian and with regard to the rate of inflation, the sum of 2,500,000 Rials fine is determined in lieu of any three-month imprisonment and this is a half to one- fifth of the income earned by an ordinary man (Research Center of the Islamic Consultative Assembly, 5, 2005).

Considering the fact that the judge is authorized to take decision about penalties in the most cases, if the cash fine is not sufficient for repenting the offender, the judge may select imprisonment or he may add this to the cash fine. It is not justifiable to emphasize the increase of cash fine due to the offender's financial or spiritual situation, in one side, and for preventing the occurrence or repetition of computer crimes, on the other side without any reasonable basis.

Some legal experts believe that the legislator has no defendable reason raised from the nature of criminal law, characteristics of information technology domain, necessities of business in national and international domain, requirements, and circumstances in justifying the sanction legislation (Ibid.11).

The first law which has criminalized forgery as one type of the crimes occurred in Cyberspace is E-Business Law. According to the article 68 of this law, apart from the offender's position or the damaged profits, the punishment for computer forgery is form 1 to 3 years of imprisonment. With respect to the importance of offence and regarding the legal articles concerning traditional forgery, in Punishment Law, which has considered different punishments for different kinds of forgery in numerous
In the second reaction of the Iranian legislator against computer crime, the punishment determined for this crime, according to the article 6 of the Computer Crimes Law is from 1 to 5 years of imprisonment. Unfortunately, only in one article, the legislator has stated the applicable cases of forgery and subsequently has determined the punishment and has the same standing for different kinds of computer data forgery.

Among other computer crimes are the impairment and interference of data and systems, access prevention, and cyber terrorism for all of which the legislator has considered imprisonment. According to the articles 8, 9 and 10 of this law, the punishment determined for the abovementioned applicable criminal cases are as follows: the punishment for crime of impairment in computer data is from 6 months to 2 years, for interference in computer or telecommunication systems from 6 months to 2 years, for access prevention from 91 days to 1 year, for cyber terrorism from 3 to 10 years.

Among other reactive responses determined for this kind of crimes is cash fine. In E-Business Law, as the first substantive reaction against computer forgery and according to the article 68 of this law, for the committers of this crime, the cash fine of 50 millions Rials besides imprisonment has been determined. Not minimum and maximum rate determination causes that the judge can not consider suitable punishment with respect to the financial situation, precedence of the offender, and the type of committed crime that results in reducing its corrective and intimidating effects.

In the second reaction, the legislator has determined cash fine as follows in Computer Crimes Law for this kind of computer crimes:

- For computer forgery, the cash fine from 1 million to 100 millions Rials.
- For impairment of computer and telecommunications system and data, the cash fine from 10 to 40 millions Rials.
- For interference in data and disruption of computer systems, the cash fine from 10 to 40 millions Rials.
- For access prevention, the cash fine from 5 to 20 millions Rials.

With respect to this fact that computer user is not an ordinary offender and indeed he/she is a specialist in computer, it is better to use non-criminal responses such as depriving him/her of computer operation and of having access to telecommunications services such as phone, cell phone, e-mail and massage sending or preventing him/her from using informative and specialized sites relevant to his/her job or social obligations including helping the network security or anti-virus projects.

The sole civil response considered in Computer Crimes Law for the committers is stated in article no.27 of this law. If a crime is repeated for more than twice, the court is authorized to deprive the committer of electronic services such as internet subscription, cell phone and electronic banking. Unfortunately, except the mentioned response, the Iranian legislator has paid less attention to the civil responses and its position in the Iranian criminal policy against these crimes seems weak. There are no facilities for enforcing such responses practically.
Interactive and Preventive Responses

Interactive prevention is attributed to a case which is enforced through influencing the process of criminal intention and action. It will be discussed in two social and legislative domains (Niazpour 2003, 127).

Social prevention is one of the interactive prevention kinds (non-criminal) and includes those kinds of actions which prevents from crime occurrence through interfering in the process of persons’ growth, improving environment and immunizing social environment. (Niazpour, 2004, 171).

Based on the new approach, this prevention is divided in two kinds of community- and growth-oriented.

The objective of community-oriented prevention in computer crimes is prevention from the formation or occurrence of criminal intention in the society by encouraging dignified motivation and avoiding cyber abnormalities.

One of other kinds of social prevention is growth-oriented. This kind of prevention, while applying early social and psychological intervention, intends to prevent the increase of computer crimes through recognizing of risk factors, therefore, it is also known as early prevention or correction-oriented approach (Raijian Asli, 2004, 150).

Among the actions taken in institutionalizing the cyber ethics and its compliance with criminology in social prevention are warning people of online-environment risks and threads, presentation of the approaches and expectations from the procedure of people’s activity in the virtual space and suitable reactions to the risks of this environment, compiling behavior codes in compliance with more familiarity with their important jobs, removing the criminal motivations and subsequently, declining the crimes statistics in Cyberspace, training internet security and promotion of media knowledge. Successful implementation of the abovementioned measures necessitates the recognition about cyber-space users and legislation of the related moral norms (Jalai Farahani, 2004, 56).

As one of other kinds of interactive responses, legislative prevention includes a series of non-criminal measures which prevent committing crime through removing or reducing the chances for committing crime and visualization of the conditions unsuitable for committing cyber crime. In other words, these situational orientation prevent committing crime through interfering in situation before the crime occurrence in the future (Niazpour, 2003, 137).

This kind of prevention, because of the special qualification of information exchange which has a technical feature, is of special importance. These measures are more security-oriented and include the components of administrative, organizational, physical, staff, hardware and software security. Taking the measures for access prevention including filtering, proxy servers, and fire walls as well as supervising measures such as permit issuance, cryptography and protecting workers and operations prevent these offences. Also, emergence of cyber police caused another kind of the legislative prevention of these crimes which has been executed as one kind of preventive measures through modeling the positive results obtained by Police in real space. (Jalali Farahani, 2007, 145).
Research Method

Based on the literature review regarding to computer cyber crime, researchers have done a research for identifying crimes against the authenticity and integrity of computer and telecommunications data as one kind of the computer crimes and studying the interactive and reactive responses and depiction of the Iranian criminal policy. This study was a systematic review on identifying of this kind of crimes in the Iranian Law and describing the system of responses and sanctions against these crimes. A systematic review is literature review focused on a single question that tries to identify, apprise, select and synthesize all high quality research evidence relevant to that question. The research method is descriptive, comparative and analytical.

Findings

Studying the Iranian criminal policy against this kind of cyber crimes, the following findings have been obtained:

1. Studying the crimes against the authenticity and integrity of systems as one kind of cyber crimes and considering the existing discrepancy in legislative criminal policy, no integrated and purposeful criminal policy was observed. But the Iranian model of criminal law, concerning this kind of crimes, follows the governmental models of criminal policy vs. community-oriented models because the punishing responses determined for this kind of crimes are often the suppressive responses such as imprisonment and cash fine which is applied by criminal system. The type and rate of such responses to these crimes in substantive laws make the criminal system of Iran close to totalitarian government model.

2. Concerning prevention of this kind of crimes, training the measures for reducing bad consequences in internet environment, compiling behavioral codes by the information technologists, promoting the media knowledge by attracting people to social affairs, and employing technical and protective measures including those for access prevention and cryptography for preventing any change and interference (in system by internet users and employing non-governmental sector for providing security in information production and exchange) indicates the government determination in relative establishment of a cooperative criminal policy coordinated with the governmental model of a democratic society.

3. The crimes against the authenticity and integrity of data and systems have a nature different from the traditional crimes which have been created by modern computer technology.

4. The legislative criminal policy of Iran criminalized this kind of crimes due to not protecting the computer data and systems by traditional criminal law and in parallel with the Convention Regulations.

5. The responses determined against this kind of crimes in the substantive regulations are mostly suppressive; they are the same common punishments determined in classical criminal law such as imprisonment and cash fine. Since a computer user is not considered as an ordinary offender and he/she may be a computer genius, it is suggested that the non-criminal punishments, for example, deprivation of operating computer, deprivation of access to telecommunications services such as cell phone, e-mail, massage sending or social obligations such as helping network security and anti-virus projects are employed instead of criminal punishments.
The criminal responses determined for this kind of crimes especially computer forgery, contrary to similar traditional crimes, have been applied identically dispense with the offender's position, type of data, and the information on which the crime occurs. This application of criminal responses seems illogical considering the importance of crime in Cyberspace and its extensive losses in this environment and compared with the traditional state. It would better that the legislator makes a distinction among different forms of the crimes, or at least, considers intensified punishments for them.

**Conclusion**

Studying the Iranian criminal policy concerning this kind of cyber crimes in the relevant legal texts and studying the criminology of these crimes as one of the cyber crimes applicable cases, the following results are inferable.

Following the recommendation letters and the guidelines issued by different international and regional organizations about this kind of crimes and in compliance with the international necessities for coordinating the criminal elements in the substantial criminal law and inspired by International Cyber Convention, the Iranian legislator has criminalized this kind of crimes to which have been referred in different laws including E-Business Law and Computer Crime Law.

With respect to the fact that the regulations of the Iranian Classical Criminal Law, has only supported the written documents and objective and tangible things against forgery and destruction respectively; therefore, adaptation and application of traditional regulations for cyber crimes seem impossible. So, the problems such as deficiency of classical regulations, insufficiency of the former regulations, and the same obliged the legislator to criminalize this kind of the crimes in the Iranian Law System independently and determine some punishments for them. Concerning the criminal punishments and sanctions, the legislator has taken a relative united policy so that the punishments determined for this kind of crimes are the same common punishments such as imprisonment and cash fine. In this procedure, less attentions has been paid to the preventive and interactive responses.

One of the other important aspects of the criminal policy is preventing and inhibiting approach and resorting to the non-criminal responses in tandem with the corrective justice. In this approach, although the Iranian governmental and disciplinary authorities have always emphasized on the preventive and purposeful measures, but this criminal policy orientation was not very successful practically. Nowadays, these crimes have had a fairly high rate of growth. Considering the special features of Cyberspace and the motivations and reasons for committing these crimes as well as their committers' characteristics who are among intellectual computer users in various levels, a differential criminal policy is required, so punishing these crimes not only demands special responses from the criminal and reactive points of view but also needs special policies conformed with production and exchange of information concerning their prevention and reaction.
References

Hassani, Jafar, Criminal Support from Privacy in Cyberspace, Thesis for Ms. Program in the field of Criminal Law and Criminology, Shaid Beheshti University, Summer of 2006.
Jalali Farahani, Amir Hossein, Computer Crimes Prevention, Thesis for Bs Program in the field of Criminal Law and Criminology, Imam Sadegh University, 2010.
Sa'dinegad, Yasamin, Criminalization in Virtual Space, Ta'li Hagh Publication, No.2.