Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.47, 2016

Electronic Data & Information Espionage: Civil or Criminal Liability?

Dr. Abdolrasoul DAYYANI
Assistant Professor of Private Law, Department of Law, Islamic Azad University of Tehran

Abstract
From time immemorial, every country has had some crucial and vital information regarding its national security and interests. If the information was revealed to the unqualified, the subject would have been penalized as a criminal and called as a spy. Today by entering into the electronic government environment, significant amount of information about the country, protection of which is directly linked to the national security, is being exchanged or kept in cyberspace. With regards to the significance of the issue, according to the Islamic Penal Code (computer crime chapter) approved in 2009, any act in the cyberspace environment for the purpose of computer spying is considered as an illegal act and the same would be considered as the material evidence of the committed crime in the court of law and will be dealt with accordingly. Hence some new regulatory measures are necessary in IPC in order to have common grounds for the terms of dealing with the electronic espionage.
Keywords: National Security - National interests - Computer crime - Cyberspace - Computer spy

Introduction

Sovereignty has always been one the most important values of a nation through history of the world. So, all countries, regardless of their governance system, answered the threats to their territorial unitary with the most severe types of punishments in order to protect their sovereignty.

One of the most obvious dangers and crimes against the national security and interests is espionage, because by committing this crime the vital information of one country will be in possession of another country or the enemies (Mirmohamma Sadeghi, 2006,75).

In the current era and with the improvement of the process of becoming electronic, governments have converted their vital national information into electronic data. As a result, spies, with different motivations such as financial incentives or opposition to the regime etc. try to use this information through computers and information technology in the cyberspace environment to serve their purpose.

With regards to the significance of this issue, articles 731 and 732 of Islamic Penal Code (computer crime chapter), an attempt is made to consider espionage in cyberspace; hence, the subject of this article.

1) General topics

In the penal codes, there is no definition of espionage, while jurists have given various definitions to explain it. Some of them consider the spy as the one who under secret or false titles tries to gain secret information or classified materials (Goldouzian, 2004, 462).

Some define the term spy as someone who collects information and news secretly and illegally with the aim of sending them to foreign countries or giving them to enemy agents, an act against the National Interests by ignoring the security laws of his own country (Rostami, 2009, 318).

Others consider espionage as a crime which consists of searching for documents, information, materials and giving them to unauthorized and unqualified people (Yari, 2004, 81).

One of the new methods of committing this crime is applying the cyberspace. Using information technology and computer systems that provide access to secret information has made this crime a cyber crime (Khodagholi, 2004, 117).

Cyber espionage, like classic espionage, deals with gaining professional, commercial, political, and military secrets and revealing, transferring, accessing and using the information. The concept of espionage in the beginning was limited to military and political spying, but in its evolution, it has changed a lot in terms of the objectives and the manner of conduct. In terms of objectives, commercial, financial, economical and industrial categories and their secrets are added to the above mentioned two categories. In terms of manner of conduct, some tools such as replicating devices, imaging equipment, eavesdropping apparatus, telecommunication systems, advanced electronic devices, satellite and IT are added to the previous information gathering tools (Hassan Beigi, 2005, 220).

Due to the increase in data processing in all disciplines, valuable economical, official and government data in big volumes are stored in data processing systems and data carriers (Khodagholi, 2004, 116).

With the aim of cyber espionage, some people try to gather classified secret government information or data documents the importance of which is linked to the national security. The prerequisite of such an act could be different motivations such as financial incentives or opposition to the current government.

2) Cyber espionage crime

In order to reprehend the person of such crime, the elements of the crime must be proved and cyber espionage crime is no exception. In this section, these elements will be investigated separately.

2-1) Legal foundation

With regards to the Criminal Laws of Iran, it is observed that articles 731 and 732 (computer crime chapters) have explained the legal foundation of espionage in cyberspace for non-military persons as:

According to article 731: anyone who illegally commits the following acts in the realm of secret data in telecommunications, computer systems during transfer phase, saved or from data carriers will be penalized:

A) Having ,obtaining or eavesdropping to secret data when being transferred will have the imprisonment of one to three years or a fine of Rls. twenty million (20/000/000) to sixty million (60/000/000) or both the punishments.

B) Giving the data to unauthorized people will have the imprisonment of two to twenty years.

C) Revealing or giving the aforementioned data to governments, organizations, companies or foreign groups or their agents will have the imprisonment of five to fifteen years.

Note 1: Secret data are the data disclosure of which harms National Interests or Homeland Security.

According to article 732: Anyone who violates the policies adopted for telecommunication or computer security systems with the purpose of accessing secret data which is the topic of the article 3 of this law [currently 731] will have the imprisonment of six month to two years or a fine of Rls. ten million (10/000/000) to forty million (40/000/000) or both the punishments.

Basic concepts

Before investigating the material and immaterial elements of the crime, it is necessary to explain the cyberspace and some of the terms used in these articles such as data, computer or telecommunication system, data transfer, data transmission and saved data.

According to the definitions given by experts, cyberspace can be defined as follows:

It is a virtual and intangible environment in the international network space (these networks are connected together via information superhighways like the Internet) where all the information about relationships among people, cultures, nations, countries and generally every tangible and physical occurrence on earth (written, audio visual, or signs) that exist in a virtual space in digital forms and are applicable and accessible by the users. All elements and international networks are interconnected with one another (Bastani, 2004, 59).

Data: According to the universal encyclopedia of Oxford, data is the information which is provided in a special form and for a specific purpose (Noori and Nakhjavani, 2004, 59).

According to the Cybercrime Convention, data is defined as follows: "any symbolic fact/ reality, information or concept which is in a sense worthy of being processed with a suitable program to make a computer system to perform a task" (Javidnia, 2008, 599).

In the second article of E-commerce Law, Data is defined as follows: "any sign of reality, information or concept which is produced, sent, received, saved or processed by electronic or optical devices of the information technology".

Computer system:

computer is defined as a device which has memory and is programmable and capable of performing mathematical and rational operations with high accuracy (Javidnia, 2008, 53). The term Computer System is defined in the second article of E-commerce Law as "any device or a set of connected hardware- software devices that operate through executing automatic message data processing programs".

Telecommunication system:

The Computer Crime Punishment Law defines this system as: "any device or a set of devices used for the electronic transmission of data between a source (optical source transmitter) and the receiver or an optical detector through one or several communicative routs through agreements which are understandable and interpretable for the receiver".

Data carrier:

This term refers to a device which contains data like memory cards, disks, floppies and CDs (Ebrahimzadeh Gholzom, 2001, 181).

Transferring data:

According to Microsoft encyclopedia, data transfer is a process from one source like a data bank to another source which is performed usually through automatic processors and programs. This process often contains data transfer from one computer system to another (Microsoft board of authors and editors publication, 2002, 203).

Saved data:

Saved data is defined as the transferred information from the main memory of computers to subordinate reserves, for the purpose of saving the information from being destroyed when the computer is turned off.

If the information in the computer memory is not saved, it would be destroyed as a result of power cut-

off or the computer turn off (Arya, 1993, 154).

2-2) Material element in cyber espionage

The material element of most of the crimes contains three parts which are categorized as the physical behavior, a group of conditions and senses. Their existence or non-existence according to the law constitutes the materialization of the crime committed.

2-2-1) Physical behavior

The physical behavior contains access to and obtaining data, unpacking the/ eavesdropping on the content being transmitted, revealing and violating the systems' security policies.

Access:

The first physical behavior in cyber espionage, the subject of our investigation, is the access. Unauthorized access to data or telecommunication or computer systems is a part of certain specific computer crimes which occurs in cyberspace; therefore, they are categorized as sub branches of absolute computer crimes. Unauthorized access is thought of as the main crime because it contributes to the commitment of other cyber crimes. In some cases, the unauthorized access has a facilitating role in the commitment of other computer crimes and in some other cases it is considered as an introduction to committing a crime. This is ranked high based on the incidence and the extent of the inflicted damage (Zandi, 2010, 179).

The term, access, conceptually is a general term since in a sense it contains definitions like gaining and influence.

In computer science, access is referred to reading data from or writing data in the memory or in other words, entering the memory in order to read or write data (Microsoft board of authors and editors publication, 2002, 20).

In note 6, article 2 of the privacy protection law, access is defined as: access to information means observing documents or anything where data is held or saved and being informed about its content through studying, transcribing or taking copies of the parts or the whole.

Some have defined unauthorized access as obtaining any kind of classified information outside the security regulatory norms (Yari, 2004, 92).

The reason for considering the unauthorized access as a crime is the invasion of privacy and security of data in a computer system. The privacy of data and computer systems means their protection from being revealed, informed about, observed, violated, investigated or analyzed. The security of data and computer system is their complete protection from any kind of obstruction (Zandi, 2010, 172).

In order to access the information in a computer, the criminals make some attacks to get the information that he or she must not observe. This attack might involve static (reserved) data in a location or data being transferred (transmitted) (Miwald, 2004, 19)

By static data and data being transferred, it is meant saved data or data being transferred which is mentioned in article 731of I.P.C.

Unauthorized access to telecommunication and computer systems must be accompanied with violations of security policies; otherwise, it would not be considered as a crime. In fact, unprotected systems are excluded from crime protection. Article 729 and note 2 of article 731 express this condition. By security and protection, it is meant that all technical and engineering methods, including hardware and software, must prevent unauthorized access.

The first step in every attack and act of violence is penetrating into the system. This work often involves obtaining the desired password. Most computer networks and web sites need password as a key to enter others domain (Mansfield, 2003, 26)

Among the experts, technical and legal, there is no consent on the concept of illegal access. Technical experts use the term hacking and define it as any kind of attack made to the security systems. Some others define hacking in a more limited range as penetrating or penetration (Shahidi, 1995, 88).

Some others consider hacking as a synonym for illegal access, but it should be stated that hacking cannot be considered as a synonym for illegal access because hacking is different from illegal access as far as the title, the target or whether it is secure or non-secure and the range of applying physical acts are concerned (Zandi, 2010, 174).

Although the attempt to illegal access is sometimes with no material purpose and the objective is to create chaos in the prey's computer system and have fun, it must be said that there are different motivations that promote this type of crime (Zibr, 2004, 46). Instances of these motivations and purposes are the revealment of the secret and protected security data for political purposes or for violating homeland security.

It should be mentioned that if access leads to transfer and abuse of the obtained information, a computer espionage has taken place; while, some believe that if this act is conducted to challenge the security system or inflict damages to the system, the crime would be labeled as a computer sabotage (Khodagholi, 2004, 119).

It seems that whenever someone obtains the data illegally and then destroys it, he can be penalized for both the espionage and sabotage because if the requirement of every sabotage was access, we could point out

that illegal access is an introduction for committing sabotage but it is not so in reality because the necessity of every sabotage is not accessing the data. For instance, a person can introduce a computer virus to a system and destroy the data without having access to the data.

Some have stated that if crimes like illegal access, unpacking and computer espionage happen simultaneously, for instance if someone tries to obtain data by having illegal access to computer system, it must be acted upon according to the spiritual multiplicity rule (Javidnia, 2008, 276).

Obtaining the data:

Obtaining data is inheres to crimes like illegal access and illegal unpacking/eavesdropping, regardless of the opinion by some that illegal access in article 75 of E-commerce which contains all these titles (Javidnia, 2008, 276).

It must be mentioned that obtaining data or any kind of information is usually the phase after illegal access, in a sense that if someone wants to obtain data illegally, he or she must have access to it first and then acquire or obtain it. According to this rational it is expressed that obtaining data is inheres of illegal access.

Unpacking/eavesdropping the data being transferred:

This behavior is considered as a part of cyber espionage material elements. Illegal Eavesdropping/unpacking is a common crime in cyberspace. In some cases, the legislators allow the law enforcement agents to unpack electronic information in a limited range for investigating some crime because crucial national security issues are involved.

In the field of electronics, eavesdropping/ unpacking for the purpose of interruption or access to any data have equivalences. Eavesdropping is an equivalent for and parallel with unpacking in the real world that can happen on telephone lines. These two terms may be used incorrectly for the same conveyance. Eavesdropping is the auditory form of accessing others' information and its usage is in the case of telephone conversations, microphones and receivers. But in case that accessing and obtaining information occurs in a digital environment and on communication lines, on the telecommunication and data transfer are attacked where that the criminal can have access to the information and data, unpacking is accomplished (Hassanbeigi, 2005, 255).

Eavesdropping is about illegal listening to conversations and even recording them. Although illegal unpacking is referred to controlling, supervising, protecting or any kind of tracking, investigating, analyzing data or electromagnetic waves that are being transferred with the purpose of understanding the content and similar acts, while eavesdropping particularly refers to sounds and the sound waves. (Zandi, 2010,169).

Although the concept of unpacking means hearing, but in article 731 of the IPC it is an expression where no hearing takes place but the knowledge of the content of the data is revealed (Hassanbeigi, 2005, 255).

As unauthorized people have no right to enter and access the systems without permission, they also do not have the right to disturb the communication which is taking place through the systems. Illegal eavesdropping can endanger the safety of data transfer, because it is assumed that there will be no security breach in data transfer from the source to the destination, as an important aspect of transferring data security is their protection from any kind of disturbance. Illegal unpacking happen when data is being transferred. So if data is not being transferred or not available or ready to be transferred in the system, it is not a case of unpacking; thus, no illegal act has taken place (Zandi, 2010, 170).

Unpacking the available data on waves is also mentioned in article 731 of the IPC. In fact, unpacking the radio waves containing data is subject to this law; otherwise, if they contain sound, it will be a case of eavesdropping. If the perpetrator is a government employee, he is subject to the article 582 of the IPC. Unpacking electromagnetic waves may occur in a computer or telecommunication system or between two or several systems.

It is notable that interrupting the data being transferred is not subject to article 731 of the IPC because illegal unpacking does not include the data being interrupted or violated (Zandi, 2010, 171).

Disclosure:

According to article 731 of I.P.C. revealing data is considered as disclosure.

In section 10, article 2 of the protection of privacy bill, it is stated that disclosure in general means releasing, transmitting, transferring of any kind of expression and presentation of information about privacy to anyone other than the subject.

According to this definition, it can be stated that by revealing the secret data in article 731 of the IPC, it is meant releasing, transmitting, transferring and in general, any kind of expressing and presenting the information about secret data mentioned in the note 1 of the same article to any government, organization, company or foreign groups or their agents.

Violation of system security:

Another physical bearing which exists in cyber espionage and is mentioned in the article 732 of the IPC is the violation of computer or telecommunication system security. Security measures which are mentioned in this article are any activities predicted for the prevention of illegal access to the systems.

According to this definition (article 732 of the I.P.C.) the measures' violation stage is an illegal stage

before accessing the data illegally. Among these measures, putting password on the system or firewall is an instance. The legislator has considered the activities which result in the violation of security measures as crime.

2-2-2) Provisions and circumstances of the crime

To accomplish an act of espionage in the cyber space which is the topic of the articles 731 and 732 of the IPC requires conditions and circumstances without which the person cannot be condemned to the related articles. In this section, we will define these provisions.

Perpetrator:

A question that might rise is that whether the person who reveals the data is really a competent person to have access to the data or he/she needs not be a competent person to have access to the data?

If we accept the first provision, the article should just include the government agents who are informed about the data with regards to their occupation. But by accepting the second provision, even if someone is informed and has access to the data that is considered as classified and has obtained the information through manners like illegal access or eavesdropping/unpacking, revealing this information to other unqualified people will be considered accomplishment of the subject crime the topic of the mentioned articles.

By referring to the articles and the usage of the term anyone at the beginning of the articles, it seems that anyone who somehow can have access to the information and data and give them to unqualified people would be subject to the above mentioned articles. Although it might be stated that with regards to the fact that basically, these types of information is not available to every person and the fact that there is access authority, the perpetrator must have the access authority to the mentioned information. But the first theory with regards to the application of the first law of the article is preferred, especially in the topics of computer and cyber crime. The non- competent people can easily have access to the secret data if they have the necessary skills and can reveal the data and give them to other unqualified people. According to the basic definition given about disclosure, it seems that disclosure is a more general expression than making available and between disclosure and making available there is the absolute common and restricted relation. Accordingly, the difference between sections B and C of article 731 regarding unqualified people who are given the data and the general conception that disclosure has to do with making the data available, it must be stated that making available might be just for one person but by data closure, with regards to the term release, policies would provide the grounds for more unqualified people to have access to the data.

In addition, according to section C, the data receivers are groups, organizations, the government etc. and the harm which might occur on their part is much more than the harm which might be inflicted by giving the information to a normal person in the society.

A notable point in the material element of espionage is that some have stated that espionage involves two levels: the elementary level and the implementation and it is mentioned that the first level is not always considered as an espionage because by preparing the information a person tries to obtain secret information with the purpose of patriotism or just by being curious and this elementary level is not a part of the espionage crime (Shambiati, 1998, 113).

But in computer espionage according to section A of article 731 of IPC, it must be stated that accessing, obtaining or unpacking the content of the data is considered as a crime and the perpetrator will be punished through the prescribed penalties in this article and his or her motivation and purpose in accessing, obtaining and unpacking the content of the data will not drop charges against him.

Secret data

It is the topic of articles 731and 732 of the IPC. Data, as documents, have their own specific classes.

Classification means evaluation of a news/issue/document with regards to the level of its secrecy, illegal disclosure, danger potential that are of four classes: Top Secret, Secret, Completely Confidential, Confidential, for the purpose of saving the information and determining on the necessary restrictions for accessing the already classified information and preventing illegal access to them (Rostami, 1999, 551).

Article 2 of the regulations states the manner in which these classified information are identified according to their degree of importance. Information Act 1975 states that each document class is determined according to its content.

Note 1, article 731 of IPC states the purpose of the secret data. This article considers any data the disclosure of which may harm the homeland security or national interests is a secret data.

In section 2 of the same article, the legislator has specified the Ministry of National Security, Ministry of Justice, Ministry of Interior, Ministry of Communications and Information Technology, Ministry of Defense and Armed Forces Logistics, to prepare regulations about determining and identifying the secret information and the manner of their classification and protection within three months from the approval date of the Computer Crime Acts in 2009 and pass the regulations to the Council of Ministries.

With regards to section 1 of this article, the legislator has given the same definition about secret data that laws and lawyers have. Article 1 of the release and disclosure of secret and confidential government documents law approved in 1974 states that the secret government documents are the documents disclosure of

which contradicts the interests of the state and the country.

In defining the classified documents, it is stated that their illegal disclosure causes major losses to the country and leads to strained political affairs and endangers the national defense program (Malmir, 2004, 72).

Others have pointed out that secret documents are those that their illegal disclosure endangers the public interest and national security (Bari, 2004, 94).

The exact title of the classified, documents is essential as far as the time of its revealing or handing to another person is concerned. The legal procedure afterwards is not that important (Malmir, 2004, 73).

The reason that the data value at the time of disclosure is the criterion is that it is possible that some classifications are constant and others lose their credit after sometime. In addition, if the judge doubts the data and information and is not sure whether they are top-secret, secret or total confidential and cannot make sure by investigation, attention must be paid to certitude, so if there is doubt between being secret or top secret of the data, it is considered as top secret (Malmir, 2004, 74).

Homeland or National Security

National security or homeland security has various concepts and has two internal and external dimensions. The internal phase of homeland security supervises on the order, peace, the public interest, development, social, cultural, civil, economic and ideological aspects of a given country, while the external phase supervises the position of the given country in the international arena and contains factors such as political ability, economic ability, military ability, cultural ability and sovereignty, integrity, defense against foreign aggression etc. (Malmir, 2004, 68).

Some have considered National Security as the capability of maintaining the national, material, and political values against any foreign aggression (Malmir, 2004, 68). Some have defined the National Security as the ability of a country in maintaining its values against external threats. Many realistic thinkers consider National Security as a synonym for Military Security and state that a country's National Security is guaranteed by its Military Security (Malmir, 2004, 69).

Some others have declared that in the contemporary discourse, security means achieving a level of assurance where the National Interests' protection is accomplished. According to Robert Mondel, National Security contains physical and mental pursuit of security and basically it is within the responsibilities of the state and the pivot point of this definition is more on pursuing and keeping the security rather than obtaining it (Nasri, 2001, 35).

Unqualified people or the enemy:

The proposed question here is that when someone obtains the information, whom should it be revealed to or given in order for the act to be labeled as cyber espionage?

According to Article 731 of IPC the addressees are in two groups. Section B of this article states the unqualified people and section C states, the governments, organizations, companies and foreign groups or their agents.

In section B the unqualified are listed and if somebody wants to overthrow the government or gives the data to the ones who want to do the same; they are subject to this section. Naturally this list is of the Iranian citizens.

Section C here, covers the foreigners- a real or legal entity- who are not Iranian citizens. The same is true for the term" their agents". The perpetrators would be subject to penalty measures mentioned in section C.

In section C, the phrase "their agents" has also been mentioned in addition to the term foreign and it seems that this term includes foreigners who are citizens of a foreign country or members of organizations, companies, or foreign groups mentioned in the article (citizens of a third country), but it only includes the ones who work for that government, company or group and might receive wages and vantages for the illegal act and this can include Iranian citizens who spy for a government, organization, company or a foreign group with different purposes like overthrowing the government.

Apart from these issues, the evidences show that the foreign constraint refers to the group evolved from government, organization, company etc. because the reason in the difference between sections B and C punishment is that the people who receive the data are foreigners, otherwise, there will be no difference between sections B and C and the punishment differences of these two sections will have no sense.

2-2-3) The results

The material behavior, mentioned above, must reach conclusions so that we can consider the occurrence of the material element of cyber espionage as a complete act. Cyber espionage through non-military individuals, with regards to the outcomes of their behavior is subject to specific punishments speculated in article 371and is of three classes. Article 732 of the IPC points to the particular crimes that in a sense are the initiators of the crimes stipulated in article 731.

Material behavior of the article 731 is divided into three sections.

In section A, the perpetrator's acts must result in accessing, obtaining or unpacking the secret data in order to be condemned to the determined punishments in this section.

In section B of the same article, the perpetrator must give the data to the unqualified people and upon doing this he or she would be condemned to the determined punishments in section B.

In section C, the perpetrator must reveal the data for governments, organizations, companies or foreign groups or their agents or give the data to them. With regards to the definitions given about disclosure, it seems that just by publishing or providing the data to governments, organizations, companies or foreign groups or their agents, the perpetrator would be sentenced according to the punishments of section C and it is not necessary to have the material evidence. In addition, the word "or", mentioned in the beginning of this section, indicates the same fact.

In order to be sentenced under article 732 of the IPC, if the perpetrator's acts result in the violation of the security procedures by breaking the firewall suffices for being condemned.

2-3) Beginning to commit the crime

Regarding espionage, it must be stated that the beginning of the political cyber crime through non-military people is not considered as a crime, since there is no clear statement on the legislator's part that does not consider this act as a crime.

2-4) Behavioral elements

Spying is an intentional crime unless it is possible to sentence the person through the legislator's explicitness and by blaming the perpetrator under article 733 of the IPC.

The general malice of the cyber espionage, committed by non-military individuals, is an intentional and conscious act recognized by articles of 731 and 732 of IPC and it seems that this malice is enough for the section A of articles 731 and 732 of the IPC and there is no need to have the intention to give the data to foreigners or unqualified people. But in sections B and C of article 731, in addition to general malice a specific malice is needed and both the sections point to the purpose of espionage.

2-5) Imposed punishments on cyber espionage

The penal code regarding non-military peoples' espionage imposes admonished sentences. Articles 731 and 732 of IPC have considered various punishments in concert with the acts and the outcomes of the committed crime.
According to section A, article 731, whenever an individual's actions lead to access to secret data, obtaining, or unpacking the data being transferred, the perpetrator will be sentenced to imprisonment from one to three years or the fine from Rls. twenty million to sixty million or both, imprisonment and cash fine.

Anyone who provides the secret data, the theme of article 731, to the unqualified people he or she will be sentenced to the punishment of the section B of the article 731 and will be sentenced to imprisonment from two to ten years. If the person reveals or gives the secret data stipulated in this article to the governments, organizations, foreign groups or their agents, he/she will be sentenced to punishment under sections C of article 731 that is imprisonment from five to fifteen years.

Whenever a person violates the security procedures of computer or telecommunication systems with the purpose of having access to the secret data, the theme of article 731, he or she will be sentenced under article 732 of the same law and will be sentenced to imprisonment from six to two years or cash fine from Rls. ten million to forty million or both imprisonment and cash fine.

Conclusion

From time immemorial, the vital national information in every country and government has been protected since this information is directly linked to the National Security. Therefore, whenever a person reveals the classified information to unqualified people, he or she faces severe punishments. With the entrance of human in the realm of computer technology, a new space is created called the cyber space where the governments' transferred or saved classified secret information is stored. With regard to the significance of this subject, the legislator of Iran, by passing the articles 731 and 732 of the IPC in 2009, considered some penal codes for crimes like having access to or obtaining secret data, unpacking the secret data being transferred, revealing and giving the data to unqualified people or the governments, organizations, companies, foreign groups or their agents and or violating the computer system's security measures with the purpose of accessing the data and has considered admonished sentences for the perpetrators of such crimes. Note 1 in article 731consideres secret data the data the disclosure of which harms the Homeland Security or National Interests.

Note 2 in the same article has made the Ministry of Information with help of some other ministries to introduce a secret data classification system as a regulation to be implemented through IPC.

Recommendations

1) With regards to the significance of the electronic data and their connection with the national security, it is recommended that the legislator, just like the penal Code Offenses of the armed forces crimes in espionage

related to classified information consider the same as a crime with less severe punishment for non- military perpetrators.
2) It seems that it would have been better if the legislator did not omit some basic technical terms which were mentioned in the cyber crime bill when it was being approved to become a law, because by stating the initial explanations, the lawyers could face a uniform definition and unique explanation about these terms and would have stopped the various interpretations and explanations of these terms.

References

Arya, Naser, 1372(1993), Computer Terminology and Computer Networks Dictionary, first edition, Tehran, specialized research center for accountancy and auditing of the Auditing Organization.
Ebrahimzadeh Ghalzam, Hosein, 1380(2001), Ghalzam Computer and Mathematics Dictionary, first edition, Tehran,Simaye Danesh publications.
Bari, Mojtaba, 1383(2004), MilitaryCriminal Justice, first edition, Tehran, Misaghe Edalat publications.
Bastani, Boroumand, 1383(2004), Computer oriented and Internet Crimes; a modern display of delinquency, first edition, Tehran, Behnami publications.
Javidniya, Javad,1387(2008), Electronic Commerce Crimes, first edition, Tehran, Khorsandi publications.
Hasan Beigi, Ebrahim, 1384(2005), Cyber Space Security and Rights, first edition, Tehran, Abrare Moaser Cultural Institute of International study and Research, Tehran.
Khodagholi, Zahra, 1383(2004), Computer Oriented Crimes, first edition, Tehran, Aryan publication.
Rostami, Mahmoud, 1378(1999), Dictionary for Military Terminology, first edition, Tehran, I.R.Iran Army publications.
Zeraat, Abbas, 1382(2003), Description of Islamic Penal Code; Section 1, first edition, Tehran, Ghoghnoos publiaton.
Zandi , Mohammad Reza, 1389(2010), Preliminary Research on Cyber Crimes, first edition, Tehran, Jangal publication.
Ziber, Olrisch, 1383(2004), Computer Oriented Crimes, translators; Mohammad Ali Nouri- Reza Nakhjavani- Mostafa Bakhtiari- Ahmad Rahimi Moghadam, first edition, Tehran, Ganje Danesh publications.
Shambayati, Houshang, 1377(1998), Proprietary Criminal Laws, third volume, second edition, Tehran, Joubin publication.
Shahidi, Farzad, 1374(1995), Unauthorised Access; A Modern Display of Modern Computer Oriented Crimes, a collection of articles on conferences for discussion on the legal aspects of information technology, Tehran Selsebil publication.
Golduzian, Iraj, 1383(2004), Proprietary Penal Code, tenth edition, Tehran University Press
Malmir, Mahmoud, 1383(2004), Description of Military Crimes Penal Code, first edition, Tehran, Dadgostar publication.
Mortazavi, Saeed, 1385(2006), Crimes Against Social Security and Welfare, first edition, Tehran, Majd publication.
Mansfield, Richard, 1382(2003), Hacker, translated by Hamid Eshagh Beigi, 5th edition, Tehran, Khalij Fars publication.
Mir Mohammad Sadeghi, Hosein, 1385(2006), Crimes Against Social Security and Welfare, 6th edition, Tehran, Mizan publication.
Mivaled, Eric, 1383(2004), A complete Book on Network Security, translated by Seyed Ahmad Safaee, first edition, Tehran, Daneshparvar publication.
Nasri, Ghadeer, 1380(2001), Petroleum and National Security of I.R.Iran, first edition, Tehran, Strategic Research and Studies publication.
Nouri, Mohammad Ali—Nakhjavani, Reza, 1383(2004), Data Protection Rights, first edition, Tehran, Ganje Danesh publication.
Microsoft publications' panel of authors and editors, 1381(2002), Microsoft Descriptive Dictionary for Computer Terminology (first edition), translated by Farhad Gholizadeh Nouri, first edition, Tehran, Sina Tasvir. Scientific Publishing Association.