Search

Farsi

Computer Crimes Act

Section 1- Crimes and Punishments

Chapter 1- Crimes against Confidentiality of Data and Computer and Telecommunication Systems

Titel 1- Unauthorized Access

Art. 1- Every person who, without authority, gains access to data, or computer or telecommunication systems which are protected under security measures shall be punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.

Title 2- Unauthorized interception

Art. 2- Every person who, without authority, **intercept** the non-public transmissions of content by computer or telecommunication systems, or electromagnetic or optical waves shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Title 3- Computer Spy

Art. 3- Every person who, without authority, commits any of the following acts against stored or in transit secret data in storage media or computer or telecommunication systems shall be punished by the provided punishments:

A) Gaining access to the aforesaid data or acquisition of them, or interception the content of the secret data in transit; by a term of 1 to 3 years of imprisonment, or by a fine of 20,000,000 to 60,000,000 Rials, or by both the imprisonment and fine;

B) Making the aforesaid data accessible to unauthorized persons; by a term of 2 to 10 years of imprisonment;

C) Disclosure of the aforesaid data or making them accessible to a foreign government, organization, corporation, or group , or their agents , by a term of 5 to 15 years of imprisonment.

Note 1: The term "secret Data" refers to the data whose disclosure will affect the state security or national interests.

Note 2: the procedure of determination and identification of the secret data, and the method of classification and protection of them shall be drafted by the Ministry of intelligence with the cooperation of ministries of Justice, State, Information and Communication Technology (ICT), and Defense, and ratified by the Board of Ministers within 3 months from the date the present act is ratified.

Art. 4- Every person who, with the intent to access the secret data provided in article 3 of the present act, violates the security measures of the computer or telecommunication systems shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Art. 5- In the event that government officials who are responsible for protection of the secret data provided in article 3 of the present act or relevant systems are efficiently trained , and the mentioned data or systems have been put at their disposal -due to carelessness, negligence or nonobservance of the security measures- cause the access of unauthorized persons to the mentioned data, storage media, or systems, shall be punished by a term of 91 days to 2 years of imprisonment, or by a fine of 5,000,000 to 40,000,000 Rials, or by both the imprisonment and fine, in addition to a period of 6 months to 2 years dismissal from service.

Chapter 2- Crimes against Integrity and validity of Data and Computer and Telecommunication Systems

Title 1- Computer Forgery (& counterfeiting)

Art. 6- Every person who, without authority, commits the following acts shall be considered a counterfeiter and punished by a term of 1 to 5 years of imprisonment, or by a fine of 20,000,000 to 100,000,000 Rials, or by both the imprisonment and fine:

A) Alteration or creation of admissible data, or deceptional creation or entry of data to them;

B) Alteration of data or signals stored in memory cards or proccessable cards in computer or telecommunication systems or chipsets, or deceptional creation or entry of data to them.

Art. 7- Every person who, by knowing that the data or cards or chipsets are forged, uses them shall be sentenced to the punishments provided in the above article.

Title 2- Data or Computer or Telecommunication Systems interference

Art. 8- Every person who, without authority, deletes, destroys, or disturbs another person's data available in computer or telecommunication systems or storage media, or makes them unprocassable shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Art. 9- Every person who, without authority, disables another person's computer or telecommunication systems, or disturbs their function by inputting, transmitting, distribution, deleting, suppressing , manipulation, or deterioration of data or electromagnetic or optical waves shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Art. 10- Every person who, without authority, prevents authorized persons from access to data, or computer or telecommunication system by hiding data, changing passwords, and encrypting data shall be punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.

Art. 11- Every person, with intent to endanger the public security and tranquility, commits the acts mentioned in articles (8), (9), and (10) of the present act against computer and telecommunication systems which are use to provide (vitally) needed public services, including treatment services, water, power, gas, telecommunication, transportation, and banking shall be punished by a term of 3 to 10 years of imprisonment.

Chapter 3- Computer Related Theft and Fraud

Art. 12- Every person who, without authority, thieves data belonging to others, while the original data remains, shall be punished by a fine of 1,000,000 to 20,000,000 Rials, and otherwise, by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.

Art. 13- Every person who, without authority, obtains money, property, profits, services, or financial advantages for himself or another person, by committing acts, including entering, altering, deleting, creating, suppression data, or disturbing the system shall be punished by a term of 1 to 5 years of imprisonment, or by a fine of

20,000,000 to 100,000,000 Rials, or by both the imprisonment and fine, in addition to restitution of the property.

Chapter 4- Crimes against Public Morality and Chastity [Decency]

Art. 14- Every person who products, transmits, distributes, trades, or, with intent to transmission or distribution or trading , produces or stores pornographic contents by means of computer or telecommunication systems or storage media shall be punished by a term of 91 days to 2 years of imprisonment, or by a fine of 5,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Note 1: Committing the aforesaid acts with respect to non pornographic but immoral contents shall result in at least one of the above punishments.

Note 2: In case the pornographic contents are sent to less than 10 persons, the perpetrator shall be punished by a fine of 1,000,000 to 5,000,000 Rials.

Note 3: if the perpetrator has made the acts provided in this article his routine work or commits them in an organized way, in case that not being found guilty of corruption on the earth, shall be punished by the maximum amount of the both punishments.

Note 4: "Pornographic Contents" refer to real or unreal image, audio, or text indicating the whole nudity of a man or woman, or their sexual organs or sexual intercourse.

Art. 15- Every person who commits the following acts by means of computer or telecommunication systems or storage media shall be punished as follows:

A) In case of provocating, encouraging, threatening, bribing, alluring, deceiving people to access pornographic contents, or facilitating or training the methods of gaining access to them, punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine;

Committing such acts with respect to non pornographic but immoral contents shall result in a fine of 2,000,000 to 5,000,000 Rials.

B) In case of provocating, encouraging, threatening, inviting, deceiving people to commit crimes against chastity, using narcotic or psychedelic drugs, suicide, sexual deviations, or violation, or facilitating or training the means of commitment or use of them, punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.

Note: The provisions of this article and article 14 shall not refer to the group of contents which are produced , generated, keeped, represented, distributed, issued, or traded for scientific purposes or any other rational expedients.

Chapter 5- Aspersion of the Dignity and Issuing Lies

Art. 16- Every person who, by means of computer or telecommunication systems, alters or distorts the video, audio, or image of another person, and issues them; or being aware of such alteration or distort,and issues them- in such a way that conventionally results in aspersion of dignity of them- shall be punished by a term of 91 days to 2 years of imprisonment, or by a fine of 5,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Note: In the case that the mentioned alteration or distortion done is in a pornographic manner, the prepatrator shall be punished by the maximum extent of the both provided punishments.

Art. 17- Every person who, by means of computer or telecommunication systems, issues or makes the audio, image, private or family video, or secrets of another person accessible to others without permission –other than in legitimate instances- in such a way that conventionally results in aspersion of the dignity of them, or causes loss- shall be punished by a term of 91 days to 2 years of imprisonment, or by a fine of 5,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Art. 18- Every person, with intent to cause damage to another person or distress the public mind or official authorities; and by means of computer or telecommunication systems, issues or makes accessible any lies; or, with the very same intent, explicitly or implicitly, in person or by quotation attributes unreal acts to a legal or real person- whether any moral or economic loss is delivered to the committee or not- shall be punished by a term of 91 days to 2 years of imprisonment, or by a fine of 5,000,000 to 40,000,000 Rials, or by both the imprisonment and fine, in addition to re establishing their dignity, if possible.

Chapter 6- Corporate Liability

Art. 19- In following instances, in case computer cyber crimes are committed by the name of a legal entity and pursuant to its interests, the legal entity shall be criminally responsible [liable]:

A) When the computer crime is committed by the director of the legal entity;

B) When the director orders the computer crime and the crime has been committed

C) When any of the employees of the legal entity commits the computer crime with the director's awareness or due to director's lack of supervision;

D) When the entire activities of the legal entity or a part of them are allocated to computer crime.

Note 1: The term "Director" refers to the person who has the authority of representativeness, decision making, or supervision of the legal entity.

Note 2: The criminal liability of the legal person shall not exempt the prepatrator from punishment, and in case of lack of terms and conditions provided in the proceeding this article, or impossibility of attributing the crime to the legal entity, the sole real person shall be regarded responsible .

Art. 20- The legal entities provided in the above article, based on the circumstances of the committed crime, their income range, and the consequences of committing crime- in addition to payment of 3 to 6 times as much as the maximum extent of fine provided for the committed crime- shall be punished as follows:

A) In case the maximum punishment provided is is up to 5 years, temporary closure of the legal entity from 1 to 9 months, and in the event of repeating the crime, temporary closure of the legal entity from 1 to 5 years;

B) In case the maximum punishment provided is more than 5 years, temporary closure of the legal entity from 1 to 3 years, and in the event of repeating the crime, the legal entity shall be liquidate.

Note: The director of the legal entity which is liquidated based on paragraph (B) of this article shall not be allowed to found, represent, make decisions for, or supervise any other legal entity up to 3 years.

Art. 21- Access Service Providers (ISPs) are obligated to filter the criminal content which is regulated within the framework of laws, whether resulted from or used to commit computer crimes, based on the technical criteria and the list provided by the Filtering Committee subject to the following article. The ISP shall be liquidated, In case of willful refusal of filtering criminal content, and punished by a fine of 20,000,000 to 100, 000, 000 Rials, for the first time, by a fine of 100,000,000 to 1,000,000,000 Rials, for the second time, and by a three year temporary closure, for the third time, in case of carelessly or negligently causing access to the illegal content.

Note 1: In case that the criminal content belongs to the websites of the public institutions including entities under the supervision of the Supreme Leader, and the three legislative, executive, and judiciary branches of power of the government, and the non-governmental public institutions subject to the Law of the Index of Non-governmental Public Institutions and Entities, 19/4/1373, and its amendments, or to the parties, guild or political societies, Islamic societies, recognized religious minorities, or to other legal or real persons in Iran -identification and communicating to whom is possible- the websites shall not be filtered until the issue of the final decision based on the order of judicial authority examining the case, and immediate removal of the criminal content's effect.

Note 2: Filtering the criminal content which is the subject-matter of private plaintiff shall be carried out by the order of the judicial authority examining the case.

Art 22- The judiciary power is obligated to establish the Committee of Filtering (committee of determining the instances of criminal content), within one month from ratification of the present act, in the location of the Office of the State Prosecutor General. The ministers or representatives of the ministries of Training and Development, Information and Communication Technology (ICT), Information, Justice, Science, Research and Technology, Culture and Islamic Guidance, the president of the Islamic Propagation Organization, and the head of the Islamic Republic of Iran Broadcasting, the Commander-in-Chief of the Police, an expert in information and communication technology chosen by the Commission of Industries and Mines of the Islamic Consultive Assembly (Majis), and one of the members

of the Legal and Judicial Commission of the the Islamic Consultive Assembly chosen by the Legal and Judicial Commission and confirmed by the Islamic Consultive Assembly, constitute the members of the committee. The State Prosecutor General shall undertake the responsibility of chairmanship of the committee.

Note 1: The committee meetings shall be held every 15 days, and the quorum shall consist of 7 members. Decisions of the committee shall be effective by a relative majority of the votes of those present at the meeting.

Note 2: The committee is obligated examine and decide about the complaints regarding the filtered instances.

Note 3: The committee is obligated to present a report regarding the procedure of filtering the criminal content to the heads of the three powers of government (legislative, executive, and judiciary), and the Supreme National Security Council every 6 months.

Art 23: The Hosting Service Providers are obligated to, immediately after receiving the order of the Filtering Committee mentioned in above article or judicial authority examining the case concerning the existence of criminal content in computer systems, prevent the continuation of access to them. The Hosting Service Providers shall be liquidated, In case of willful refusal of executing the order of the committee or judicial authority. Otherwise, The Hosting Service Providers shall be punished by a fine of 20,000,000 to 100, 000, 000 Rials, for the first time, a fine of 100,000,000 to 1,000,000,000 Rials, for the second time, and by a three year temporary closure, for the third time, in case of carelessly or negligently causing access to the criminal content.

Note: The Hosting Service Providers are obligated to, immediately after becoming aware of the existence of the criminal content, inform the Filtering Committee of their existence.

Art 24- every person who, without authority makes use of the international (internet) bandwidth to establish international protocol-based telecommunication connections from abroad to Iran or visa versa shall be punished by a term of 1 to 3 years of imprisonment, by a fine of 100,000,000 to 1,000,000,000 Rials, or by both the imprisonment and fine.

Chapter 7- Miscellaneous Crimes

Art 25- Every person who commits the following acts shall be punished by a term of 91 days to one year of imprisonment, by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine:

A) Production, issue, distribution of and making accessible, or trading data, softwares, or any other electronic devices, which are exclusively used to commit computer crimes;

B) Sale, issue, distribution of, or making accessible passwords or any data makes the unauthorized access to data or computer or telecommunication systems belonging to others possible;

C) Issue of or making accessible the unauthorized-access-training contents, unauthorized sniff, computer spy, causing distortion or destruction of data or computer or telecommunication systems.

Note: In the event that the prepatrator has made the mentioned acts his routine occupation, he shall be punished by the maximum extent of both punishments provided (in this article).

Chapter 8- Aggravation of Punishment

Art 26- In following instances, the prepatrator shall be punished by more than two third of the maximum extent of one or both the punishments:

A) Any of the employees or staff of the governmental or government-related departments, organizations, and institutions, councils and municipals, revolutionary entities, foundations and institutions which are administered under the supervision of the supreme leader (of the Islamic Republic of Iran), the Supreme audit court, the Institutions which are administered by means of the constant subsidies subventions paid by the government, officials holding judicial ranks, and generally, members and staff of the three powers/ branches of the government, armed forces, and public service officers -whether official or unofficial- have committed computer crimes in the performance of their duties;

B) The operator or the legal possessor of the computer or telecommunications networks, have committed computer crimes in the performance of their duties;

C) Data or computer or telecommunication systems belong to the government or entities or centers providing public services;

D) The crime has been committed on a vast scale.

Art 27- in the event of more than two times repetition of the crime, the court is empowered to deprive the prepatrator of the public electronic services including internet or cell phone subscription, obtaining domain name registrations in national Top-Level Domains (ccTLDs), and electronic banking:

A) In case the imprisonment punishment provided for the crime is from 91 days to 2 years, deprivation from 1 month to 1 year;

B) In case the imprisonment punishment provided for the crime be from 2 to 5 years, deprivation from 1 to 3 years;

C) In case the imprisonment punishment provided for the crime be more than 5 years, deprivation from 3 to 5 years.

Section 2- Procedural law

Chapter 1- Jurisdiction

Art 28- Along with instances predicted by other Laws and regulations, The Iranian courts have jurisdiction over following instances:

A) Criminal data or data used in committing crimes has been anyhow stored in computer or telecommunication systems or data carries existing in Islamic Republic of Iran's land, air, and maritime territory;

B) The crime has been committed by means of the websites with country code Top-Level Domains of Iran;

C) The crime has been committed by any Iranian or non-Iranian person, outside Iran's borders, against computer or telecommunication systems, and websites used by or under control of the three powers/ branches of the government, Leadership Entity, official governmental agents , or any institution or entity providing public services, or against websites with national country code Top-Level Domains of Iran;

D) Computer crimes involve abuse of persons under the age of 18, whether the prepatrator or the victim is Iranian or non-Iranian.

Art 29- In the event that the computer crime is discovered or reported in a place, while the location it was committed in location of the commitment thereof is not obvious , the local prosecutor's office is obligated to initiate the preliminary investigations. In case that the location of commitment of crime does not become obvious, the prosecutor's office- by finishing the investigations- resorts to issue verdict, and the relevant court issues the appropriate order.

Art 30- The judiciary power is obligated to, based on necessity, allocate one or more branches of the prosecutor's office, the public and revolutionary courts, military courts, and appeal courts to try computer crimes.

Note: Judges of the aforesaid prosecution office branches and courts shall be chosen amongst judges who are well-acquainted with the computer affairs.

Art 31- In the event of any disputes arising over jurisdiction, the dispute resolution shall be done in accordance with the Civil Procedure Code of the Public and Revolutionary Courts.

Chapter 2- Collecting Digital Evidence

Title 1- preservation of traffic data

Art 32- Access service providers are obligated to preserv the traffic data at least until 6 month after the creation thereof and the users' information at least 6 months form termination of the subscription.

Note 1: The term "Traffic Data" refers to any data that computer systems generates in computer and chain of telecommunication chain make their trace from origin to destination possible. These data include information such as origin, path, date, time, duration, and volume [mass/ size] of communications and the type of the relevant services.

Note 2: The term "User Information" refers to any information related to user of access services including the type of services, technical facilities used, duration, identity, geographical or postal address or internet protocol (IP), telephone number, and other individual characteristics of the user.

Art 33- Domestic host service providers are obligated to retain their users' information at least until 6 months, and the stored content and traffic data resulted from the occurred changes at least until 15 days from termination of subscription.

Title 2- Expedited preservation of the Stored Computer Data

Art 34- Whenever **preservation** of stored computer data is necessary for doing investigations or judgments, the judicial authority is empowered to issue the **preservation** order addressed to any persons who, anyhow, have them under their control or possession. In urgent cases, including [such as] danger of damage, alteration, or destruction of data, judicial officers are empowered to, on their own initiative directly issue the **preservation** order, and then inform the judicial authority of the actions carried out within 24 hours. In the event that any of the governmental staffs, judicial officers, or other persons refuse to execute the order, disclose the **preserved** data, or inform the persons to whom the aforesaid data is related to the provisions of the issued order, governmental staffs and judicial officers shall be punished by refusal of executing the judicial authority's order, and other persons shall be punished by a term of 91 days to 6 months imprisonment, or by a fine of 5,000,000 to 10,000,000 Rials, or by both the imprisonment and fine.

Note 1: Data **preservation** is not equal to presentation or disclosure thereof, and demands necessitates observance of the relevant laws and regulations.

Note 2: the data protection duration is not to exceed 3 months, and in case of necessity, is extendable by means of the judicial authority's order.

Title 3- Data Presentation

Art 35- The judicial authority is empowered to issue the order of presentation of data mentioned in articles (32), (33), and (34) above addressed to aforesaid persons to put (the data) at the disposal of the officers. Refusal of executing the order shall be punished by the punishment provided in article (34) of the present act.

Title 4- Data and Computer and Telecommunication Systems' Search and Seizure

Art 36- Data or computer and telecommunications systems' search and seizure shall be performed by virtues of the judicial order, in cases there is a strong suspicion concerning discovering the crime, or identifying the criminal or crime evidences.

Art 37- Data or computer and telecommunications systems' search and seizure shall be performed at the presence of the legal possessors or persons, anyhow, have them under their control, including system operators. Otherwise, the judge shall issue the order of search and seizure without the presence of the mentioned persons.

Art 38- the search and seizure order must contain the information which aids the accurate execution thereof, including order execution in/out of the location, the qualifications and scopes [limits] of search and seizure, type and extent of the considered data, type and number of the hardware and software, the method of accessing the encrypted or deleted data, and the approximate time needed for accomplishment of search and seizure.

Art 39- Data or computer and telecommunication systems' search and seizure includes the following measures:

A) Gaining access to computer and telecommunication systems, in whole or in part;

B) Gaining access to data carriers including diskettes, compact discs, or memory discs;

C) Gaining access to encrypted or deleted data.

Art 40- In data seizure, proportionately considering the type, importance, and role of data in committing crime, methods including data printing, copying or imaging data -in whole or in part, making data inaccessible by means of techniques including changing passwords, encryption, and confiscation seizure of data carriers are practiced.

Art 41- in any of the following cases, the computer or telecommunication systems shall be seized:

A) The stored data is not conveniently accessible, or is in large volume

B) Search and analysis of data is not possible without having access to hardware system;

C) The legal possessor of data has given his/her consent;

D) Copying data is not technically possible;

E) In-place search causes damage to data.

Art 42- Seizure of the computer or telecommunication systems is performed proportionately considering their type, importance, and role in committing crime, and by means of methods including changing passwords to cause lack of access to the system, in-place plumping, and seizure of the system.

Art 43- in case of necessity of seizure of the data relevant to the committed crime existing in other computer or telecommunication systems which are)under control or possession of the accused, during seizure process, the officers –by the order of the judicial authority- shall expand the width of search and seizure to the mentioned systems, and take actions to search or seize the considered data.

Art 44- Seizure of the data, or computer or telecommunication systems, in the event of causing physical injury or severe economic damages to individuals, or disruption to public services provision, is forbidden.

Art 45- In cases that the original data is seized, the beneficiary is entitled to, after paying the cost, make a copy of them; provided that the presentation of the seized data is not concerned criminal or contrary to confidentiality of the investigations, and does not affect the procedure thereof.

Art 46- in cases that the original data or computer or telecommunication system are seized, the judge is obligated to, considering the type and volume of data, type and number of the considered hardware and software, and their role in committed action , make decisions about them within a reasonable period of time.

Art 47- The affected person is entitled to deliver his/her objection in writing with regard to the actions and measures taken by officers in search and seizure of data and computer and telecommunication systems, along with the reasons of the objection, to the judicial authority issuing the order. The mentioned objection shall be examined out of turn, and the decision shall be appealable.

Title 3- Interception the Content data

Art 48- intercepting the content of non-public communications in transit between computer or telecommunication systems shall be pursuant to the laws and regulations respecting interception of telephone conversations.

Note: Gaining access to the content of stored non-public communications, including e-mail or short message sevice, is tantamount to intercepting, and necessitates

observance of the relevant regulations and laws.

Chapter 3- Admissibility of Digital Evidence

Art 49- For the purpose of protection of the accuracy, integrity, validity, and admissibility of the collected digital evidence, it is necessary to protect hem pursuant to the relevant executive by-laws

Art 50- In the event that the computer data is created, processed, stored, or transferred by the parties of the suit or the third party which unaware of the existence of the suit, while the relevant computer or telecommunication system operates so properly that the accuracy , integrity, validity, and admissibility of data are not affected, the data shall be admissible.

Art 51- All the provisions of chapter (2) and (3) of this section, shall be applied to other crimes in which digital evidences are referred to, in addition to computer crimes.

Section 3- Miscellaneous Provisions

Art 52- In cases the computer or telecommunication system is used as a means of committing crime, and there is no punishment provided for the mentioned action, the relevant criminal laws and regulations shall be applicable.

Note: In cases there are no specific regulations provided in section (2) of the present act respecting the legal procedure of trial of computer crimes, the provisions of the criminal procedure act are applicable.

Art 53- The amounts of fines provided in this act are changeable every three years, based on the official annual inflation rate declared by the central bank, with the recommendation of the chief justice, and ratification of the Board of Ministers.

Art 54-Executive by-laws regarding to collection and admissibility of digital evidence shall be drafted within 6 months from ratification of the present act by the Ministry of justice, with the cooperation of Ministry of Information and Communication Technology (ICT), ratified by the Ministry of Justice.

Art 55- Articles (1) to (54) of the present act are considered as Articles (726) to (782) of the Iranian Penal Code (Ta'zirat and Deterrent Punishments Section), under the title "Computer Crimes Chapter", and the number of the article (729) of the Penal Code is corrected to (783).

Art 56- Laws and regulations contrary to the present act become invalid.

The above act, consisting of 56 articles and 25 notes, was ratified in the open session of the Islamic Consultive Assembly (Majis) [Parliament of the Islamic Republic of Iran], dated Thursday, Khordad 5, 1388, and confirmed by the Guardian Council on 20/3/1388.

Related Document

Comprehensive Study On Cybercrime

News Archive

News Archive

Related Websites

Interpol

Iran CERT

Netan South Korea

IC3

KISA

Contact Information

Address : Police Headquarter, Attar street, Vanak Sq, Tehran, Iran

E-mail : webmaster@cyberpolice.ir