Cybercrime Law
No. 71863
10/4/1388
Ministry of Justice
The Law on Computer Crimes, which was presented at a public hearing on Tuesday, June 25, 2009
Two hundred and eighty-eight of the Islamic Consultative Assembly was approved and approved by the Council on 3/20/2009.
The guard arrived and submitted it through letter No. 16360/121 dated 3/4/2009 of the Islamic Consultative Assembly
Has been notified to the appendix for implementation
President - Mahmoud Ahmadinejad
Chapter One - General
Part One - Crimes and Punishments
Chapter One - Crimes against Data Confidentiality and Computer and Telecommunication Systems
Title 1 - Unauthorized access
Article 1- Anyone who unauthorized access to data or computer or telecommunication systems that
Access is protected by security measures, up to ninety-one days in prison
One year or a fine of five million (5,000,000 Rials to twenty million) 20,000,000
Rials or both will be punished
Topic 2 - Unauthorized eavesdropping
Article 2- Anyone who illegally listens to private contents in non-public communication
Listen to computer or telecommunication systems or electromagnetic or optical waves
Imprisonment from six months to two years or a fine of ten million) (10,000,000 Rials to forty
Million) (40,000,000 Rials or both will be punished
Topic 3 - Computer espionage
Article 3 - Anyone illegally transferring or storing secret data
Computer or telecommunication systems or data carriers to commit the following acts, to
The following sentences are punishments will be condemned
, A) access to or study of such data or eavesdropping on the content of the series being transmitted
Imprisonment from one to three years or a fine of twenty million) (20,000,000 Rials to sixty
Million) (60,000,000 Rials or both penalties
B) Making the said data available to unqualified persons, from imprisonment for two to ten
years
C) Disclosing or making available such data to a government, organization, company or group
Aliens or their perpetrators, to imprisonment from five to fifteen years
Note 1- Data is a series of data whose disclosure is to the security of the country or national interests
Harm
Note 2: By-laws on how to determine and identify secret data and how to classify and protect them
Within three months from the date of approval of this law by the Ministry of Information in cooperation with the Ministries
Judiciary, country, communications and information technology and defense and support of the armed forces
Prepared and approved by the Council
Topic 4 - Anyone with the intention of accessing the secret data subject to Article 3 (3 of this law, measures)
Violate the security of computer or telecommunications systems, to imprisonment from six months to two years
Or a fine of ten million) (10,000,000 Rials to forty million) (40,000,000 Rials or
Both punishments will be punished
Article 5 - If government officials who are responsible for maintaining confidential data specified in Article (3)

Are law or related systems and have been trained or required data or
The mentioned systems have been provided to them due to carelessness, bimbalit or
Non-compliance with security measures causes unauthorized persons to have access to data, data carriers
The mentioned systems, to imprisonment from one hundred days to two years or a fine of five
Million) (5,000,000 Rials to twenty million) (20,000,000 Rials or both penalties and
Dismissal will be punished by six months to two years
Chapter 2 - Crimes against the accuracy and integrity of data and computer and telecommunication systems
Topic 1 - Computer forgery
Article 6- Whoever commits the following acts without permission, is considered a forger and shall be imprisoned from one to
Five years or a fine of twenty million) (20,000,000 Rials to one hundred million
) Rials or both will be sentenced) (100,000,000
A) Modifying or creating credible data or creating or entering fraudulent data into
a
B) Changing data or symbols on memory cards or processable systems
Computers or telecommunications or chips or the creation or importation of fraudulent data or
Signs to them
Article 7- Anyone with the knowledge of the falsity of data or cards or chips to use them
Will be sentenced to the punishment mentioned in the above article
The second issue is the destruction and disruption of data or computer and telecommunication systems
Article 8- Anyone illegally downloads other data from computer systems or
Telecommunications or data carriers deleted or destroyed or disrupted or unprocessed to be imprisoned
Six months to two years or a fine of ten million) (10,000,000 Rials to forty million
Rials or both will be sentenced) (40,000,000
Article 9- Any person unauthorized acts such as importing, transferring, distributing or deleting
Data, blocking and destroying electronic or mechanical or optical waves
Stop or disrupt other computer or telecommunication systems
Slow, to imprisonment from six months to two years or a fine of ten million) (10,000,000 Rials
To forty million (40,000,000 Rials or both will be punished
Article 10- Anyone unauthorized by acts such as hiding data, changing the password
Or data encryption prevents authorized persons from accessing data or computer systems
Or be telecommunicated, to imprisonment from ninety-one days to one year or a fine of five million
Rials up to twenty million) (5,000,000 Rials or both will be punished) (20,000,000
,
Article 11- Anyone with the intention of endangering the security, comfort and public safety of the acts mentioned in the articles
Article (5), (6) and (9) against computer and telecommunication systems to be submitted) (8), (9
, Essential public services are used, such as medical services, water, electricity, gas, telecommunications
If the commit transportation and banking, he will be sentenced to three to ten years in prison
Chapter 3 - Computer-related theft and fraud
Article 12- Anyone illegally steals data belonging to another, if the same
The data is at the disposal of the owner, for a cash of one million) (1,000,000 Rials to
Twenty million) (20,000,000 Rials and otherwise imprisonment from ninety-one days to one
Year or a fine of five million) (5,000,000 Rials to twenty million) 20,000,000
Rials or both will be punished
Article 13- Anyone committing unauthorized use of computer or telecommunication systems
Actions such as entering, modifying, erasing, creating or stopping data, or disrupting it
Money, money or property, benefits or services or financial benefits for yourself or another student
In addition to rejecting the property, the owner is sentenced to imprisonment for one to five years or a fine of twenty
Million) (20,000,000 Rials to one hundred million) (100,000,000 Rials or both penalties
Will be condemned
Chapter 4 - Crimes against public chastity and morality

,
Article 14- Everyone by means of computer or telecommunication systems or data carriers of contents
Publish, distribute or trade in pornography, or produce or store it for the purpose of trade or corruption
Hold, to imprisonment from ninety-one days to two years or a fine of five million
Rials up to forty million) (40,000,000 Rials or both will be punished) (5,000,000
,
Note 1- Committing the above acts regarding vulgar contents will result in a sentence of at least one
The above punishments will be
Content and vulgar works belong to works that have ugly scenes and images.
Note 2: Whenever obscene contents are sent to less than ten people, the perpetrator shall be one million
Rials up to five million) (5,000,000 Rials will be fined) (1,000,000
Note 3- If the perpetrator has made the acts mentioned in this article his profession or to
Corruption, the maximum of the punishment mentioned in this article will be the maximum of both
The punishments provided in this article will be condemned
Note 4- Pornographic contents belong to a real or unreal image, sound or text or text
It indicates the complete nudity of a woman or a man or the genitals or intercourse or sexual intercourse
Is human
Article 15- Everyone commits through computer or telecommunication systems or data carriers
If the following acts are committed, they will be punished in the following order
(A) If, in order to gain access to obscene content, it incites, persuades
Threaten or entice or deceive or facilitate access to education or training
) To imprisonment from ninety-one days to one year or a fine of five million) 5,000,000
Rials up to twenty million) (20,000,000 Rials or both will be punished
B) Producing, publishing or facilitating vulgar content will result in a fine of 2,000,000
Up to five million) (5,000,000 Rials
B) If people commit crimes against chastity or use drugs or psychotropic substances
Suicide or sexual perversion or violent acts of incitement or persuasion or threat or invitation
To deceive or facilitate or teach them how to commit or use them
Imprisonment from ninety-one days to one year or a fine of five million) (5,000,000 Rials up to
Twenty million (20,000,000 Rials or both) is sentenced
Note - The provisions of this article (14) will not include those contents that for
Scientific purposes or any other intellectual interest in the preparation or production or maintenance or presentation or distribution
Or it is stored or is available.
Chapter 5 - Crime - Defamation and Spreading Lies
Article 16- Everyone by computer or telecommunication systems, film or audio or video
Change or distort another and publish it or publish it with the knowledge of change or distortion
In such a way that the mystics - cause him to be tarnished, to imprisonment from ninety-one days to two years or
A fine of five million (5,000,000 Rials to forty million) (40,000,000 Rials or any
Two punishments will be sentenced
Note: If the change or distortion is obscene, the perpetrator will be punished with a maximum of both
The order will be condemned
Article 17- Anyone by means of computer or telecommunication systems of audio, video or video
Publish private or family or other secrets without his consent except in legal cases
, Or make it available to others, in a way that leads to harm or mystics - cause him to be tarnished
Imprisonment from ninety-one days to two years or a fine of five million) (5,000,000 Rials to
Forty million (40,000,000 Rials or both will be punished
Article 18- Anyone with the intention of harming others or disturbing the public mind or official authorities by means of
Publish or make available lies to others on a computer or telecommunications system
Or with the same intention to act against the truth, directly - or as a quote, to the person
Explicitly or implicitly attribute real or legal, whether through the aforesaid to
Whether or not any form of material or moral damage is inflicted on another, in addition to restoring prestige

If possible (imprisonment for ninety-one days to two years or a fine of five million (
Rials up to forty million) (40,000,000 Rials or both will be sentenced) (5,000,000
Chapter Six - Criminal Liability of Persons
Article 19- In the following cases, if computer crimes in the name of a legal person and in the interests of the interests
If it is committed, the legal entity will be criminally liable
A) Whenever the manager of a legal entity commits a computer crime
B) Whenever the manager of a legal entity issues an order to commit a computer crime and the crime occurs

C) Whenever one of the employees of a legal entity commits it with the knowledge of the manager or due to his lack of supervision
The crime has been committed
D) When all or part of the activity of a legal entity is dedicated to committing a computer crime
.This is found
Note 1- The manager means a person who has the authority to represent or decide or supervise a person
Has rights
Note 2: The criminal liability of a legal person shall not preclude the punishment of the perpetrator and if it did not exist
The conditions of the beginning of the article and the non-attribution of the crime to a private person, only the natural person will be responsible
Article 20- The legal entities subject to the above article, according to the circumstances and circumstances of the crime
Commitment, the amount of income and the results of committing a crime, in addition to three to six times
The maximum fine, one to three times the maximum fine for the crime
, Temporary suspension of the legal entity for a period of one to five years Implementation of the legal entity
From one to nine months and in case of recurrence of the crime of temporary closure of a legal entity from one to five years
For the time duration of one to three years and in the case of recurrence of the permanent closure of the legal entity
Legal from one to three years and in case of recurrence of the crime, the legal entity will be dissolved
Note - The closure of a legal entity that is dissolved according to paragraph (d) of this article, up to three years of establishment right
Or will not represent or decide or supervise another legal entity
Otherwise, if the access service providers are obliged to comply with the technical rules and the list prescribed by
Working group (Committee) to determine the instances of the subject of the following article of criminal content within the framework of the law
Filter it to include content from cybercrime contents to commit
Filter or block the content of crimes that are not enforceable, or from
Refrain (filter) from the content of crimes that will be dissolved and if from
Carelessness and negligence provide access to illegal content, in
The first order of fines from twenty million) (20,000,000 Rials to one hundred million)
) Rials and in the second place to a fine of one hundred million (100,000,000) 200,000,000
Rials up to one billion) (1,000,000,000 Rials and in the third place to one to three years of
Temporary suspension of the business
Note 1- If the criminal content goes to the websites of public institutions, including
Institutions under the supervision of the Supreme Leader and the three branches of the legislature, the executive and the judiciary and public institutions
The subject of the law on the List of Public Non-Governmental Institutions approved on 4/19/1373 and
Commercial companies and institutions in which the shares of the above-mentioned institutions are more than 50%
Or recognized religious minorities or other natural or legal persons present in Iran who
It is possible to authenticate and communicate with them to belong, by order of the authority
Judicial review of the case and removal of the immediate effect of the criminal content by holders
The website will not be filtered until the final refinement order is issued
Note 2: Filtering (criminal) content of the subject of a private complaint by order of a judicial authority
The case will be reviewed
Article 22- The Judiciary is obliged to work within one month from the date of approval of this law.
Determining instances of criminal content in the place of the Attorney General's Office
, Representatives of the Ministries of Education, Culture and Islamic Guidance, Information Technology, Information
Justice, Science, Research and Technology, Culture and Islamic Guidance, Head of the Propaganda Organization
Islamic, Heads of Media and Telecommunications, Commander-in-Chief of the Police, an expert in technology

Information and communication selected by the Industries and Mines Commission of the Islamic Consultative Assembly and one person
Form the working group (committee) with the Judicial and Legal Commission to be elected by the Judicial and Legal Commission and approved
The Islamic Consultative Assembly will form the members of the working group (committee). The working group will chair
The Committee will be in charge of the Attorney General.
Note 1- Meetings of the working group (committee) at least once every fifteen days and with the presence of seven members
The decisions of the working group (committee) will be valid by a relative majority of those present.
Note 2- The working group (committee) is obliged to filter the complaints regarding the examples of polishing.
Consider and decision-making
Note 3- The working group (committee) is obliged to report every six months on the refining process) filtering
Submit criminal content to the heads of the three forces and the Supreme National Security Council
Article 23- The service providers are obliged as soon as they receive the order of the working group) Committee
Determining the cases mentioned in the above article or the judicial authority handling the case based on
Filter the criminal content in your computer systems prevents you from continuing to access it
If they deliberately refuse to carry out the order of the working group (committee) or judicial authority
Otherwise, if due to carelessness and carelessness
Provide access to such criminal content, first and foremost criminal
Article 24- Anyone who commits the crime of fraud in the amount of two million) 2,000,000 Rials and in
Criminal time to one million) (100,000,000 Rials to one billion) 1,000,000,000
Rials and in the third place will be sentenced to one to three years of temporary suspension
Note: Internet service providers are obliged as soon as they are aware of the existence of criminal content
Inform the working group (committee) to determine the cases
Article 24- Any person without legal permission from the international bandwidth to establish communications
, Use telecommunications based on Internet protocol from outside Iran to inside or vice versa
Connection, in the first place to a fine of one to five hundred million) (100,000,000 Rials to one
(Billion) (1,000,000,000 Rials or both will be punished
Chapter Seven - Jurisdiction
Article 25- Any criminal who commits the following acts shall be imprisoned from ninety-one days to one year or
Fine from five million (5,000,000 Rials to twenty million) (20,000,000 Rials or any
Two punishments will be sentenced
(A) the production or dissemination or distribution and making available or traded of data; or
Or make any electronic device intended solely for the purpose of committing computer crimes
.To be used
B) Selling or publishing or making available passwords or any data that is accessible
Unauthorized data or computer or telecommunications systems belonging to another without
Their permission
C) publishing or making available the contents of unauthorized access training, unauthorized eavesdropping
Computer spying and destruction and disruption of data or computer and telecommunication systems
Note: If the perpetrator has made the above-mentioned acts his profession, to a maximum of both
The punishments provided in this article will be condemned
Chapter 8 - Investigation and Jurisdiction
Article 26- In the following cases, as the case may be, the perpetrator shall be punished by more than two thirds with a maximum of one or two
Will be imprisoned
A) Any employee and staff of departments and organizations, councils or municipalities and
Government institutions and companies affiliated with the government or revolutionary institutions and foundations and
Institutions that are managed under the supervision of the Supreme Leader and the Court of Justice and institutions that
Government-dominated companies and institutions and the Supreme Court and the Prosecutor's Office and the General
Law enforcement and armed forces as well as the Armed Forces and public service officers, including officials
And unofficially committed a computer crime on the occasion of performing their duty
B) Operator or lawful possessor of computer or telecommunication networks for the occasion of his job
Has committed a computer crime

C) data or computer or telecommunication systems, owned by the government or institutions and centers
Be a public service provider
D. The crime was committed in an organized manner
E) The crime has disturbed the public order and security
Article 27- In case of repeating the crime for more than two times, the court can remove the perpetrator from the services
Public electronics such as Internet sharing, mobile, Bali domain name registration
: Ban national and e-banking
A) If the punishment for imprisonment is ninety-two days to two years imprisonment, deprivation of one month
Up to one year
B) If the punishment for imprisonment is two to five years imprisonment, deprivation of one to three years
(C) If the punishment for that crime is more than five years imprisonment, deprivation of three to five years
Part 2 - Evidence)
Chapter One - Jurisdiction
Article 28- In addition to the cases provided for in other laws, the courts of Iran in cases
The following will also be competent to handle
(A) criminal data or data used to commit a crime in any way
, In computer and telecommunication systems or data carriers in the realm of terrestrial sovereignty
The sea and air of the Islamic Republic of Iran are stored
B) (crime through websites) websites (with the highest rank domain of the country code of Iran
.Completed
C) a crime committed by any Iranian or non-Iranian outside Iran against computer systems; and
Telecommunications and data carriers located or under the control of the three powers or
Against the government or official representative of the government or any institution or institution that provides public services
Offers or against websites (website) with a Bali-level domain code
C) Iran has been committed on a large scale
(D) Computer offenses involving the abuse of persons under the age of eighteen, including
Be an Iranian or non-Iranian perpetrator or victim
Article 29- If a computer crime is discovered or reported in a place, but its place is known
Otherwise, the court of the place where the discovery is obliged to conduct a preliminary investigation, if the place of occurrence
If the crime is not identified, the prosecutor's office will issue a verdict after the investigation is completed and the court
The relevant order will be transferred within 24 hours.
Article 30- The Judiciary is obliged, in proportion to the necessity of a branch or branches of courts, tribunals
Establish one or more branches of the prosecutor's office and investigate cybercrime
Special judges of the above-mentioned courts and tribunals are among the judges who are familiar with computer and telecommunications affairs.
Computers are being selected
Article 31- In the event of a breach of jurisdiction, the breach shall be resolved in accordance with the provisions of law
The future of the general and revolutionary courts will be in civil matters
Chapter Two - Gathering Electronic Evidence
Topic 1 - Data maintenance
Article 32- Internet service providers are obliged to provide traffic data for at least six months
Keep user creation and information for at least six months after the end of the subscription
Or the last time the user is in the service provider's system is kept.
Internet provider computer and telecommunications communications so that they can be traced from source to
, The destination exists. This data includes information such as origin, route, date
Time, duration and volume of communication and the type of services are relevant
Note 2- User information Any information about the user of access services such as type
Subscriber, technical facilities used and its duration, identity, geographical or postal address or
His telephone number and other personal details (IP), Internet Protocol
Note 3- Domestic hosting service providers are obliged to keep their users' information to a minimum
Up to six months after the end of the subscription and the saved content and traffic data resulting from the changes

Keep the created for at least fifteen days
Topic 2 - Immediate protection of stored computer data
Article 33- The storage of stored computer data is necessary for investigation or trial
The judicial authority may order their protection for persons who are in some way occupied or
They have control to issue. In urgent situations, such as the risk of injury or change or destruction
Data, judicial officers can directly issue a protection order and maximize
Inform the judiciary within 24 hours, as any government employee or officer
Judicial or other persons refuse to comply with this order or disclose protected data
Or the persons to whom the said data relates from the provisions of the order
Inform judicial officers and government employees of the punishment for refusing to comply with a judicial authority order
Disclosure of protected data shall be imprisoned for ninety-one days to two years or a fine of five
Rials up to ten million) (10,000,000 Rials or both will be sentenced) (5,000,000
,
Note 1- Data protection does not constitute the presentation or disclosure of them and requires compliance with the regulations
is related
Note 2- The maximum period of data protection is three months and if necessary by order
Judicial status can be extended
Topic 3 - Data presentation
Article 35- The judicial authority may order the presentation of the protected data mentioned in Articles 32
Article 34 to the owner of the computer or telecommunications system to be provided to the judiciary
Anyone who does not comply with the order will be sentenced to the punishment provided in Article 34 of this law
Topic 4 - Audit and seizure of data and computer and telecommunication systems
Article 36- Inspection and seizure of data or computer and telecommunication systems in accordance with the order
Judicial and in cases where there is a strong suspicion of discovering a crime or identifying the accused or evidence
Performs a crime
Article 37- Inspection and seizure of data or computer and telecommunication systems in the presence
Legal occupiers or persons who somehow have legal control over them, e.g.
System operators will be done. Otherwise, the judge will state the reason for the order
Article 38- The search and seizure order must be issued to the mentioned persons
Include the search and seizure order shall contain information that will assist in its proper execution
Including the examination of the place or off-site, the information sought, the scope of the inspection and
Seizure, type and amount of data, type and number of hardware and software
How to access the encrypted or deleted data and the approximate time of the search and seizure
How to do the Audit of data or computer and telecommunication systems including the following measures
: May
A. Access to all or part of computer or telecommunication systems
B) Access to data carriers such as floppy disks or compact discs or memory cards
Access to deleted or encrypted data
Article 40- In confiscating the data, observing their operational, type, importance and role in committing a crime
Prevention of damage to other data and computer and telecommunication systems
Make data inaccessible by methods such as password changes or
, C (the legal occupier of the system has consented
D (imaging) copying (of the data is not technically possible
(E) On-site inspections cause damage
Article 41- Confiscation of data or telecommunication systems in accordance with the type, importance and role
They commit crimes by changing passwords in order not to gain access to the system

The system is sealed at the location and recording of the system
Article 43- If during the execution of the search and seizure order, the search of the data related to the crime
Other data or computer or telecommunication systems that are under the control or possession of the accused
If necessary, the officers shall, by order of the judicial authority, extend the scope of the search and seizure
Order and the protected data and the data will be searched or seized
Article 44- If the seizure of data or computer or telecommunication systems causes a problem
To personal or financial loss to persons or disruption of the provision of public services is prohibited

,
Article 45- In cases where the original data is confiscated, the beneficiary has the right after payment
Request a copy of them, provided that the provision of confiscated data is criminal
Or does not contradict the confidentiality of the investigation and does not harm the investigation process
Article 46- In cases where the original data or computer or telecommunication systems are confiscated
The judge is obliged in terms of the type and amount of data and the type and number of hardware and
Software and the nature of the crime and their role in the crime, within a reasonable time
Assign tasks to them
Article 47- The victim may be informed about the operations and actions of the agents in confiscating the data and
Computer and telecommunications systems to submit their written objection along with the reason within ten days
Submit to the judge of the judicial system. The said request is out of turn
Examine the case and the judge can be challenged
Topic 5 - Listening to the content of computer communications
Article 48- Listening to the content being transmitted by non-public communications in computer systems
Or telecommunications will be in accordance with the regulations regarding the interception of telephone conversations
Note - Access to stored non-public communication content, such as e-mail or
SMS is a wiretapping order and requires compliance with relevant regulations
Chapter 3 - Citation of electronic evidence
Article 49- In order to maintain the accuracy and integrity, validity and undeniability of electronic evidence
Collected, it is necessary to maintain and take care of them in accordance with the relevant regulations
,
Article 50- If the computer data is provided by the litigant or a third party who is aware of the litigation
Do not been created or processed or stored or transferred and the computer system or
Telecommunications operates in a way that is accurate, complete, credible and undeniable
If the data is not damaged, it can be cited
Article 51- All the provisions mentioned in the second and third chapters of this section, in addition to the crimes
Computers include other crimes in which electronic evidence is involved
It also becomes
Chapter 4 - Other regulations
Article 52- In cases where the computer or telecommunication system as a means of committing a crime
This law does not provide for a penalty for this act, in accordance with the law
Relevant details will be acted upon
Note: In the cases mentioned in the second part of this law for the investigation of computer crimes
The rules of the specific procedure according to the procedure according to the provisions of the Code of Criminal Procedure
Will be implemented
Article 53- The amount of fines of this law based on the official inflation rate according to the bank
Central once every three years on the proposal of the head of the judiciary and the approval of the Cabinet
Will be
Article 54- Regulations related to the collection and citation of electronic evidence
Within six months of the date of the ratification of this law by the Ministry of Justice in cooperation with the Ministry
Information and information technology will be prepared and approved by the head of the judiciary
Article 55- Number of articles (1 to) (54 of this law as articles) (270 to) (782 law
Islamic Punishment (Punishment Section) with the title of Chapter on Computer Crimes and Article Number

,
Islamic Penal Code No. (783 to be amended) (729
Article 56- Laws and regulations contrary to this law are repealed
The above law consists of 56 articles and 25 notes in the public session on Tuesday, the fifth
/ In June, one thousand three hundred and eighty-eight, the Islamic Consultative Assembly approved and on
Approved by the Guardian Council in 2009
Speaker of the Islamic Consultative Assembly - Ali Larijani