Iran

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 25 June 2020

Table of contents

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	

BUDAPEST CONVENTION	**DOMESTIC LEGISLATION**
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Computer Crimes Act** **Section 2- Procedural law** **Chapter 2- Collecting Digital Evidence** **Title 1- preservation of traffic data** 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.
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when	**Computer Crimes Act** **Chapter 1- Crimes against Confidentiality of Data and Computer and**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Telecommunication Systems** **Title 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 3- Computer Espionage 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 measurescause 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	from service.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Computer Crimes Act** **Chapter 1- Crimes against Confidentiality of Data and Computer and Telecommunication Systems** **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.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Computer Crimes Act** **Chapter 2- Crimes against Integrity and validity of Data and Computer and Telecommunication Systems** **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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Computer Crimes Act** **Chapter 2- Crimes against Integrity and validity of Data and Computer and Telecommunication Systems** **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.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,	**Computer Crimes Act** **Chapter 2- Crimes against Integrity and validity of Data and Computer and Telecommunication Systems** **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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	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).
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Computer Crimes Act** **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.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when	**Computer Crimes Act** **Chapter 2- Crimes against Integrity and validity of Data and Computer and Telecommunication Systems**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**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
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct	

Back to the Table of Contents

BUDAPEST CONVENTION	**DOMESTIC LEGISLATION**
3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 – Ancillary liability and sanctions	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Computer Crimes Act** **Chapter 2- Crimes against Integrity and validity of Data and Computer and Telecommunication Systems** **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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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.
Article 13 – Sanctions and measures	**Computer Crimes Act**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	**Chapter 2- Crimes against Integrity and validity of Data and Computer and Telecommunication Systems** **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	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and	**Computer Crimes Act** **Section 2- Procedural law** **Chapter 2- Collecting Digital Evidence** **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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	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.
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Computer Crimes Act** **Section 2- Procedural law** **Chapter 2- Collecting Digital Evidence** **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.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and	**Computer Crimes Act** **Section 2- Procedural law** **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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	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.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**Computer Crimes Act** **Section 2- Procedural law** **Chapter 2- Collecting Digital Evidence** **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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Computer Crimes Act** **Section 2- Procedural law** **Chapter 2- Collecting Digital Evidence** **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)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability:	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.	**Computer Crimes Act** **Section 2- Procedural law** **Chapter 2- Collecting Digital Evidence** **Title 3- Interception of 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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**Computer Crimes Act** **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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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.
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents