Italy

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 01 May 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	No legislative measures of adoption have been made with respect to the mere carrying out of the relevant definitions under the Convention, as said normative definitions are already known in legislation in force (cf. article 4 of legislative decree no. 196 of 30 June 2003, with the code regarding the protection of personal data). It has however been decided to maintain for the crimes of false representation as accepted by law in 1993 which, by considering the computer document equal to public acts and to private contracts, had permitted traditional criminal cases to be extended to cases in which a computer document was the object.
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	**art. 615-*ter* Penal Code**. Illegal access to a computer or computer-related system.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to establish as criminal offences under its domestic law, when 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.	The formulation of the criminal offence is in keeping with the requisites foreseen by the Convention, because, as required, it occurs with the violation of a security measure. In addition the offence of the illicit maintaining of the agent in the system is also foreseen. From the standpoint of sanctions, in conformity with art. 9, paragraph 2 of the subsequent *cybercrime directive*, the maximum punishment is fixed as three years' imprisonment, against the forecast in the directive of a custodial punishment of not less than two years at least for cases that are not of minor gravity, and, with reference to more serious cases as per paragraph 3, not less than 3 years.
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.	**art. 617-*quater* *Penal Code.*** Interception, impediment or illegal interruption of computer or computer-related systems. Article 617-*quater* satisfies both the substantive requirements of article 3 of the Convention, from the standpoint of the offence, which is elastic in form, including any means of interception whatsoever between computer or computer-related systems. The requisites of punishment as per article 9, paragraph two, of the mentioned cybercrime directive are also safeguarded.
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.	**art. 635-*bis* Penal Code.** Damaging of computer information, data and programmes. The crime as per article 635-*bis of the Penal Code*, inserted in implementation of the Budapest Convention, exists in subsidiary form, even when the cancelled data can be recovered thanks to the intervention of a skilled technician. Article 635-ter foresees the more serious case of damage, caused by a number of alternative offences, of computer data and programmes **art. 635-*quater* Penal Code.** Damaging of computer or computer-related systems. This article concerns the case of illegal interference with computer or computer-related systems, moreover foreseeing more severe punishment than that imposed by article 9, paragraph two, of the mentioned directive, and, with reference to the more serious cases as per the successive paragraph, of not less than 3 years. The offence of illegal interference is described, listing a series of alternative modalities.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 635-*quinques* Penal Code foresees the more serious case of causing damage by a number of alternative means, to information and computer-related systems of public utility.
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	The offence as per **article 635-quater Penal Code** introduced by the Budapest Convention, punishes as a subsidiary measure the damaging of computer information systems, which occurs even when the system may be repaired following the intervention of a skilled technician.
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, 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,	**art. 615-*quater*** of the Penal Code. Illicit possession and distribution of access codes to computer or computer-related systems. **art. 615-*quinquies*** of the Penal Code. Distribution of apparatuses, devices or computer programmes for the purpose of damaging or interrupting an information or computer-related system. Article 615 *quater* of the Penal Code considers an action to be an offence when it is preliminary to the crime of the illegal interception or distribution of access codes to information or computer-related systems. According to case law the offence of illegal access may contribute towards the crime as per article 615 *quinqiues* of the Penal Code, namely the distribution of apparatuses for the purpose of interrupting computer devices or programmes. The necessary sanction as per article 9, paragraph 2, is achieved by increasing the punishment foreseen for the aggravating circumstances as per paragraph 2. With regard to article 615 *quinquies*, relating to the possession or distribution of *maleware*, the latter is considered to be an offence with specific intent, which appears compatible with the directive, which requires there to be a definite intention in the action of utilization, for the purpose of committing the offences from 3 to 6.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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.	Such a case was foreseen by **article 491-bis** of the Penal Code, as introduced by law no. 547 of 1993, entitled: "Computer-related documents". The article in question inserted, in Chapter III of Title II of Book II of the Penal Code, relating to forgery in official acts, a new case that extended to the cases of falseness regarding a computer-related document, the provisions regarding forgery in a public act or a private contract (arts. 476 to 491 Penal Code). The second part of the article concerned contained the definition of a computer-related document valid in the penal sector: this was "any computer-related support containing data or information having a probative effect or programmes specifically intended to produce them". For a clearer understanding of the amendments made in article 3 of the law ratifying said article, it is necessary to reproduce the original text, namely: 491-bis. (Computer-related documents).- If any of the forgeries foreseen in the present chapter regards a public or private computer-related document, the provisions contained in the chapter concerning public acts and private documents, respectively, shall be applied. For this purpose by computer-related document is understood "any computer-related support containing data or information having a probative effect or programmes specifically intended to produce them". Article 3 of the law concerned amended in part the aforesaid article. More precisely in the first period, after the word "private" the words "having a probative effect" were added, while the second period was suppressed up to the words "intended to produce them"… This took place, as stated in the report on the original bill (no. 2807). "…in consideration of the evident inadequacy of the definition of computer-related document, understood as "a computer support containing data or information having a probative effect or programmes intended to produce them", it was decided to adopt, also for penal purposes, the broader and more correct notion of a computer-related document, already contained in the regulation in Decree no. 513 of the President of the Republic dated 10 November 1997, as a "computer-related representation of legally relevant documents, facts or data"

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	The introduction to article 495-bis of the Penal Code has the same standpoint, stating: "False declaration or statement to the certifier of an electronic signature of the identity or the state or one's own personal qualities or those of other persons. – Any person who falsely declares or attests to the person performing the service of certification of electronic signatures one's own identity or state or other qualities or those of another person shall be punished with a term of imprisonment of up to one year".
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 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.	***Art. 640-ter*** of the Penal Code***.*** *"Computer-related fraud",* as follows*:* Any person who, by altering in any way the operation of a computer or computer-related system, or who acts without right and in any way on data, information or programmes contained in a computer or computer-related system, or ones pertaining thereto, procures an economic benefit for himself or for others with detriment to other persons, shall be punished with a term of imprisonment of 6 months to 3 years and with a fine of 51 to 1,032 euro. The punishment shall be a term of imprisonment of one to five years and a fine of 309 to 1,549 euro if one of the circumstances applies as listed in number 1) of the second paragraph of article 640, or if the fact is committed abusing the quality of system operator. The punishment shall be a term of imprisonment of two to six years with a fine of 600 to 3,000 euro if the offence is committed with the theft or unauthorized use of the digital identity to the detriment of one or more subjects. The offence is liable to punishment upon request (« querela ») by the offended person, unless any of the circumstances as per the second and third paragraph, or another aggravating circumstance, should apply. ***Art. 640-quinquies*** of the Penal Code***.*** "Computer-related fraud by the one performing services of certifying electronic signatures", states as follows: "The person performing the service of certifying electronic signatures, who, in order to procure, without right, an economic benefit for himself or for others, or to cause detriment to others, violates the obligations foreseen by law for the issue of a qualified certificate, shall be punished with a term of imprisonment of up to three years and with a fine of 51 to 1,032 euro".

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	This provision appears necessary because, although article 640-ter of the Penal Code already punishes computer-related fraud, for this specific offence to apply, it appears necessary for actions to be carried out altering the operation of a computer-related system or of acting unrightfully on data, information or programmes, which do not apply in the case of certification. However, the new offence appears centred not only on the mere violation of the obligations of the qualified and accredited certifier (already sanctioned civilly by letter d) of paragraph 1 of article 30 of the cited Code of Digital Administration), but also on the actual occurrence of an unrightful benefit with detriment to others.
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 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-	These provisions have already been carried out following the introduction into Italian legislation of article 4 of law no. 38 of 6 February 2006. In particular, apart from the amendment of the criminal offences, said law entrusts to the National Centre for the Prevention of Child Pornography on Internet, established in the Police postal and communications service of the POLICE Department the measures against this criminal phenomenon. The Centre is engaged in the prevention and repression of offences of this type. The primary objective is the defence of adolescents on Internet, by means of monitoring services which seek virtual clandestine spaces where images and films of abused minors are offered. More in general, continuous monitoring focuses attention on discovering sites and situations that could represent a source of danger in the navigation carried out by the very young. With regard to child pornography sites, this law identifies the Centre as the assembly point for dealing with reports sent in both by other police forces, including foreign ones, and by citizens, voluntary associations and providers. From all this activity the Centre makes provision to draw up a list of the child pornography sites on the Network (termed the "black list"), which is made available to Internet Service Providers, so that they may inhibit navigation by means of technical filtering systems. If while navigating any such banned site is encountered, even unintentionally, a specific "stop page" appears, containing the notice of prohibition. National banking and financial systems also contribute towards preventing such offences, via the Bank of Italy, which enables information to be acquired relating to illicit transactions and spending on the online market aimed at purchasing photographs and films of abuses against minors.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	This law (no. 38 of 6 February 2006) establishes, in the Prime Minister's Office, the Observatory to prevent paedophilia and pornography of minors, with tasks of monitoring the phenomenon, with the connection of all the Institutions concerned with questions regarding minors, including judicial bodies and the social services. The Centre, as the organ of operative assembly, conducts a constant dialogue with the Observatory, the organ of institutional assembly, for which it provides its own data for the analysis and prevention of the abuse of minors. A world coalition under the guidance of Interpol, with the participation of Europol, implements International police collaboration, on a daily basis, for the identification of the victims of child pornography, wherever they may live. An Office for Minors is set up in every Police Headquarters, headed by a police officer with specific competences in identifying minors at risk and in gaining their confidence, in order to prevent the risk of abuse. In 2014 three training courses were held at the Police Department, General Directorate of State Police, for Postal Police operators, with a total of 120 trained operators. In the course of 2015 two such courses were held and in all further 70 operators were trained.
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-	Copyright is safeguarded in Italy by law no. 633 of 22 April 1941: Protection of copyright and other related rights for the exercising thereof (text coordinated with the latest amendments introduced by law no. 248 of 18 August 2000). The following are in addition to this law: Law no. 39 of 1 March 2002: Provisions for the implementation of obligations deriving from Italy's membership of the European Communities – Community Law of 2001, published in the Gazzetta Ufficiale no. 72 of 26 March 2002 – Ordinary Supplement no. 54, Art. 30 (Implementation of Directive 2001/29/CE, on harmonizing certain aspects of copyright and of related rights in the information society). Law no. 137 of 6 July 2002: Delegated mandate for reform of the organization of the Government and of the Prime Minister's Office, as well as of public entities, published in the Gazzetta Ufficiale no. 158 of 8 July 2002. Art. 10 (Mandate for reorganization and codification of in the sphere of cultural property

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	and environmental assets, entertainment, sport, literary property and copyright). Law no. 248 of 18 August 2000: New regulations for safeguarding copyright (published in the Gazzetta Ufficiale no. 206 of 4 September 2000) Regulation of the implementation of provisions regarding the mark of the Italian Society of Authors and Editors (SIAE) as per article 181-bis of law no. 633 of 22 April 1941, as introduced by article 10 of law no. 248 of 18 August 2000, containing new regulations for the safeguarding of copyright (G. U. no. 194 of 22 August 2001) Royal Decree no. 1369 of 18 May 1942, with approval of the regulations for implementing law no. 633 of 22 April 1941, for the protection of copyright and of other rights related to its enforcement. Law no. 159 of 22 May 1993 regarding the unauthorized reproduction of books. Law no. 747 of 20 December 1994: Adoption of TRIP agreements regarding intellectual property. The following should also be considered a) Laws by Parliamentary delegation: Provisions for the implementation of obligations deriving from Italy's membership of the European Communities – Community law of 1995-1997, published in the Gazzetta Ufficiale no. 104 of 7 May 1998 – Ordinary Supplement no. 88. Delegated law no. 128 of 24 April 1998, "Community law for the adoption of European directives" b) Legislative decrees for implementation of Community directives: Legislative decree no. 68 of 9 April 2003 regarding the implementation of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Directive 2001/29/CE on harmonizing certain aspects of copyright and of related rights in the information society. Published in the Gazzetta Ufficiale no. 87 of 14 April 2003 – Ordinary Supplement no. 61. Legislative decree no. 518 of 29 December 1992: Implementation of Directive 91/250/CEE relating to the legal safeguarding of computer programmes Legislative decree no. 685 of 16 November 1994: Implementation of Directive 92/100/CEE concerning the right of lending and hiring and of certain related rights Legislative decree no. 581 of 23 October 1996,: Implementation of Directive 93/83/CEE for the coordination of some regulations regarding copyright and related rights, applicable to radio broadcasting and to retransmission by cable Legislative decree no. 154 of 26 May 1997: Implementation of Directive 93/98/CEE concerning the duration of copyright protection and of certain related rights. Legislative decree no. 169 of 6 May 1999: Implementation of Directive 96/9/CE relating to the legal safeguarding of databanks.
Title 5 – Ancillary liability and sanctions	
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.	The provisions of art. 11 of the Convention are fully covered by current Italian law as follows: a) **art. 414** of the Penal Code**.** (Instigation to commit a crime) sanctioning the conduct of any person who instigates another person to commit a crime. b) **art. 378** of the Penal Code**.** (Personal aiding and abetting).- Any person who, after a crime has been committed for which the law establishes life or another term of imprisonment, and apart from cases of complicity therein, assists another person to elude the investigations of the Authorities, including those conducted by organs of the International Criminal Court, or to elude the searches made by said subjects, shall be punished with imprisonment of up to four years. When the crime committed is that foreseen by art. 416 bis, the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	punishment of not less than two years shall in any case be applied. If the crimes concerned are ones for which establishes a different punishment, or of infractions, the punishment shall be a fine of up to 516 euro. The provisions of this article shall also apply when the person assisted is not indictable or when it results that he has not committed the crime. c) **art. 379** of the Penal Code. (Real aiding and abetting). – Any person who, apart from cases of complicity in the crime and of the cases foreseen by articles 648, 648 bis and 648 ter assists another person in securing the product or the benefit or the price of a crime, shall be punished with imprisonment of up to five years if a crime is concerned, and with a fine of 51 euro up to 1,032 euro if an infraction is concerned. The provisions of the first and the last paragraph of the preceding article shall apply. d) **art. 110** of the Penal Code**.** (Punishment for those who participate in an offence). – When more than one person participates in the same offence, each of them shall be subject to the punishment prescribed for such offence, except as provided in the following articles. In the Italian Penal Code, article 110 which disciplines the institution of the concurrence of persons in an offence, has an extensive incrimination function in the punishability of a penally relevant offence, in that by being linked with other special articles it opens up to that number of incriminating offences.
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	Legislative decree no. 231 of 08/06/2001, regulates the administrative liability of legal persons, of companies and of associations, even those without a legal personality, as per article 11 of law no. 300 of 29 September 2000. Art. 24-bis. Computer crimes and illicit data processing, sanctions the cases foreseen in the Convention**:** 1. In relation to the commission of the offences as per articles 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater and 635-quinquies of the Penal Code, the pecuniary sanction of one hundred to five hundred shares shall be applied to the entity. 2. In relation to the commission of the offences as per articles 615-quater and 615-quinquies of the Penal Code, the pecuniary sanction of up to three hundred shares shall be applied to the entity.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	3. In relation to the commission of the offences as per articles 491-bis and 640-quinquies of the Penal Code, except as foreseen in article 24 of the present decree for the cases of computer-related fraud to the detriment of the State or of another public entity, the pecuniary sanction of up to four hundred shares shall be applied to the entity. 4. In cases of conviction for one of the offences indicated in paragraph 1, the interdictory sanctions foreseen in article 9, paragraph 2, letters a), b) and e) shall be applied In the event of conviction for one of the offences indicated in article 9, paragraph 2, letters b) and e) shall be applied. In cases of conviction for one of the offences indicated in paragraph 3 the interdictory sanctions foreseen in article 9, paragraph 2, letters c), d) and e) shall be applied.
Article 13 – Sanctions and measures 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.	For the adequacy of the sanctions foreseen, reference is made to the preceding paragraphs.
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	Given that the stipulation of the Convention on cybercrime by the Member States is aimed at achieving a "minimum common level" of capacity to counter the criminal phenomena that are the object thereof, but does not exclude that each State may continue to have even more incisive and/or restrictive measures available than those required under the Convention, the criterion followed in drawing up the regulations to implement the Convention under Italian law has been that of limiting ourselves to the measures strictly necessary and ensuring that in the system of criminal proceedings all the measures listed above, as foreseen by the provisions of the Convention, are available, with the accompanying institutions of guarantee. Consequently, action has been taken at two converging levels: 1) the integration of certain provisions of the Code of Criminal Procedure

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	– which already govern measures of investigation corresponding to those foreseen by the Convention – through explicit and specific references to the computer and computer-related situation, in order to bring the textual formulation of the procedural provisions into line with applicative requirements in the computer field; 2) the insertion *ex novo* of procedural provisions that regulate measures requested by the Convention but not now present in the domestic system, with the accompanying institutions of guarantee; such is the case of article 9 of the bill, which introduces paragraphs 4 *ter, quater* and *quinquies* of article 132 of legislative decree no. 196 of 30 June 2003 with which the conservation "on an urgent basis" of data relating to computer-related traffic is introduced, among other things, into the Italian system. It appears useful to point out that while the order of intervention as per 2) innovates the system from the standpoint of its legislative contents, the modifications as per point 1) consist in a mainly "lexical" update of the procedural provisions in force, for the purpose of making explicit the applicative potentials in the computer field, which already today, moreover, have been recognized by both jurisprudence and case law for the procedural institutions concerned. The integrations made by the following articles, at this second level of intervention, mainly of a formal nature, are: - in art. 244, paragraph 2: the insertion of an express reference to the computer and computer-related systems with regard to the possibility for the judicial authority to order, at the level of inspections, surveys and other technical operations; - in art. 247: the introduction of paragraph 1-*bis*, which explicitly foresees that searches may have computer and computer-related systems as their object, even though protected by security measures; - in art. 248, paragraph 2: a statement that computer data, information and programmes are included among the items that may be the object of examination in banks, by the judicial authority or by Judicial Police officers, without the need to have recourse to forms of searches; - in art. 254, paragraphs 1 and 2: a partial reformulation of paragraph 1, aimed at updating notions and expressions recurring therein in the light of the changes that have occurred in the past decade or so in the organizational and functional forms of the correspondence services and with the advent of the electronic mail; in paragraph 2, also, in view above all of the different material structure of computer correspondence as opposed to that on paper, a statement aimed at guaranteeing that this should not only not be opened or known, but not even simply altered; - in art. 256, paragraph 1: a statement that computer data, information

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	and programmes are also included among the items having to be handed over upon request to the Judicial Authority by persons subject to professional secrecy, as well as by public officials, public employees and those commissioned to perform a public service; - in art. 259, paragraph 2: a statement of the contents of the obligation of custody when the things seized consist of computer data, information and programmes; - in art. 260, paragraphs 1 and 2: a statement, in paragraph 1, that the imposition of seizure may be evidenced, in relation to the nature of the things seized, also with electronic or computer-related means; and an indication, in paragraph 2, of the ways in which to make a copy and in which to conserve the originals when it is a question of the seizure of computer data, information and programmes; - in art. 352: the introduction of a paragraph, no. 1-bis, which explicitly foresees that the search at the initiative of Judicial Police officers may have as its object computer and computer-related systems, even though protected by security measures; - in art. 353, paragraphs 2 and 3: a modification in the formulation of regulations in relation to the same requirements already stated with regard to article 254 and so as to maintain the parallel nature of the two articles; - in art. 354, paragraph 2: a statement of the activities that Judicial Police officers are empowered to carry out, within the context of the urgent investigations as a consequence of the commission of an offence, in order to ensure the conservation of computer data, information and programmes and of computer and computer-related systems, and so as to prevent any alteration or access, in any case subject to the power of seizure. For the same purpose, moreover, the insertion is ordered of an article 254-*bis*, intended to regulate the ways of acquiring data under seizure with providers of computer and computer-related or telecommunications services, in order to prevent any disturbance or upsets in the regular provision of said services. Then, with the introduction of the new paragraphs 4 *ter, quater* and *quinquies* in article 132 of legislative decree no. 196 of 30 June 2003, it is intended to foresee, as already observed, a measure which, in compliance with what is required by the Convention, will permit the temporary and urgent "freezing" of data. Lastly, with article 10 the insertion is made of paragraph *quinquies* in article 51 of the Code of Criminal Procedure so as to concentrate competence for computer and computer-related offences in the district prosecution offices. This in order to facilitate the coordination of the investigations and the formation of work groups specialized in the matter.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	The safeguarding of human rights is ensured in the State by the reservation of jurisdiction, which covers all the cases of sanctions indicated in the preceding paragraphs. As furthermore the regulations on *cybercrime* are largely inserted in the Penal Code and in the Code of Criminal Procedure or in other acts having the force of law, all the guarantees are applicable that safeguard human rights, as foreseen in general by the Italian Constitution and, in particular, among others, the articles regarding personal freedom (article 13), inviolability of the home (article 14) and the confidential nature of correspondence (article 15), as well as the provisions of International conventions on the subject of human rights, in force in Italy, which are recognized a higher status than that of ordinary laws.
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	Full attention has been given in article 16 of domestic law through article 2 of law no. 48 of 18 March 2008, according to which "full and entire execution is provided for the Convention, as from the date of its coming force, in conformity with the provisions of article 26 of the Convention". It has not been necessary to introduce any further legislative amendments, as said instruments are already foreseen in the present Code of Criminal Procedure or in the Code of Protection of Personal Data (regarding the data possessed by the providers).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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 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.	See sub art. 16
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	It has not been necessary to introduce any further legislative amendments, as article 96 of legislative decree no. 259 of 2003 already foresees this obligation for providers; in particular this provision foresees that "services for the purpose of justice, provided in the case of requests for interceptions and for information by the competent judicial authorities are obligatory for operators".

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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;	The legislative provisions relating to inspections, searches and orders to disclose have been modified in such a way as to make them clearly applicable also in relation to computer data. In particular: 1. Added to article 244, paragraph 2, second period, of the Code of Criminal Procedure, relating to inspections, are the words «also in relation to computer or computer-related systems, adopting technical measures aimed at ensuring the conservation of the original data and at preventing their alteration». 2. Paragraph 1-bis has been added to article 247 of the Code of Criminal Procedure, relating to searches, as follows. «*1*-bis. When there is good reason to believe that computer data, information and programmes or in any case traces thereof pertinent to the offence can be found in a computer or computer-related system even if protected by security measures, the search thereof shall be ordered, adopting technical measures aimed at ensuring the conservation of the original data and at preventing their alteration». 3. Paragraph 1 of article 254 of the Code of Criminal Procedure, relating to the seizure of correspondence, has been substituted, as follows: *1.* On the premises of those supplying postal, telegraphic, computer or telecommunications services the seizure is permitted of letters, folders, packages, securities, telegrams and other objects of correspondence, even if sent by electronic means, which the judicial authority has good reason to believe to have been sent by or to the accused, even under a different name or via a different person, or which could in any case be in relation with the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	offence»; 4. Furthermore, Art. 254-bis has been introduced as follows: «Art. 254-*bis*. - *(Seizure of computer data from providers of computer, computer-related and telecommunications services) - 1*.The judicial authority, when ordering the seizure from providers of computer, computer-related or telecommunications services, of data possessed by them, including those of traffic or of location, may establish, for necessities linked to the regular provision of said services, that their acquisition shall take place by copying them on a suitable support, by a procedure that ensures the conformity of the data acquired with the original ones and the impossibility of modifying them. In this case however the provider of the services shall be ordered to conserve and to protect adequately the original data». Amendments have also been made in the provisions relating to orders to exhibit (article 256) and to other procedural measures, in order to extend them also to computer data and to guarantee the custody thereof. Powers of acquisition have also been given to the police forces. In particular the updated article 352 of the Code of Criminal Procedure foresees, in paragraph *1*-bis: At the moment of the offence, or in the cases as per paragraph 2 when the assumptions and the other conditions therein are present, Judicial Police officers, adopting such technical measures as to ensure the conservation of the original data and to prevent the alteration thereof, moreover carry out a search of computer or computer-related systems even though they may be protected by security measures, when they have good reason to believe that computer data, information and programmes may be concealed therein, or traces in any case pertinent to the crime, which might be cancelled or dispersed. With regard to the conservation of data, article 354, paragraph 2, of the Code of Criminal Procedure, as renewed, foresees that: In relation to computer data, information and programmes or to computer or computer-related systems, Judicial Police officers shall adopt, furthermore, the technical measures or shall give instructions as necessary to ensure the conservation and to prevent the alteration and access thereof and thereto and shall make provision, when possible, for their immediate duplication on suitable supports, by means of a procedure that ensures the conformity of the copy to the original and makes it impossible to modify it.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be	No specific provisions have been introduced, as this possibility is already ensured by domestic legislation.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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: 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.	No specific provisions have been introduced, as this possibility had already been foreseen with the preceding legislative action (Law no. 547 of 23 December 1993), which introduced article 266 bis of the Code of Criminal Procedure, pursuant to which "in proceedings relating to the crimes indicated in article 266 (namely limits of admissibility of interceptions of conversations or communications) and to those committed with the use of computer or computer-related technologies, the interception is permitted of the flow of communications relating to computer or computer-related systems or taking place between a number of systems".

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	As already stated, providers are obliged by law to give assistance and to treat as confidential the carrying out of interception operations.
Section 3 – Jurisdiction	
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	Art. 22,1, a) of the Convention is implemented by art. 6 of the Penal Code; article 22,1 c) is implemented by arts. 7,8 and 9 of the Penal Code; article 22, 3 by article 9, last paragraph, and 10 no. 3 of the Penal Code.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
Chapter III – International co-operation	
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. 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,	Article 24 was implemented in Italian law by means of article 2 of law no. 48 of 18 March 2008, according to which "full and entire implementation has been made of the Convention, as from the date of its coming into force, in conformity with the provisions of article 26 of the Convention". It has not been necessary to adopt any amendment in Italian law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	In implementation of article 24 § 7 of the Convention, article 13 of the law authorizing ratification foresaw the Minister of Justice as the competent authority. By declaration deposited at the same time as the act ratifying the Convention, on 5.6.2008, the competent authority was indicated as: MINISTRY OF JUSTICE DEPARTMENT FOR AFFAIRS OF JUSTICE OFFICE II (INTERNATIONAL JUDICIAL COOPERATION)
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 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	Article 25 was implemented in Italian law by means of article 2 law no. 48 of 18 March 2008, according to which "full and entire implementation has been made of the Convention as from the date of its coming into force, in conformity with the provisions of article 26 of the Convention". It has not been necessary to adopt any further amendment to Italian law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 26 has been fully implemented in Italian law by means of article 2 of law no. 48 of 18 March 2008, according to which "full and entire implementation has been made of the Convention as from the date of its coming into force, in conformity with the provisions of article 26 of the Convention". According to this provision no further legislative measure was necessary.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 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.	Article 27 has been implemented by means of article 2 of law no. 48 of 18 March 2008, according to which "full and entire implementation has been made of the Convention, as from the date of its coming into force, in conformity with the provisions of article 26 of the Convention". In the event that no International conventions exist, the procedure applicable is that envisaged in Book XI of the Italian Code of Criminal Procedure.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	In implementation of article 27 § 2 of the Convention, article 13 of the Italian law authorizing ratification foresaw the Minister of Justice as the competent authority. By declaration deposited at the same time as the act ratifying the Convention, on 5.6.2008, the competent authority was indicated as: MINISTRY OF JUSTICE DEPARTMENT FOR AFFAIRS OF JUSTICE OFFICE II (INTERNATIONAL JUDICIAL COOPERATION).
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 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	Italy has not submitted any declaration as per § 9 letter a)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	Article 28 has been implemented by means of article 2 of law no. 48 of 18 March 2008, according to which "full and entire implementation has been made of the Convention, as from the date of its coming into force, in conformity with the provisions of article 26 of the Convention". It has not been necessary to take any further legislative measure.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	Article 29 has been implemented by means of article 2 of law no. 48 of 18 March 2008, according to which "full and entire implementation has been made of the Convention, as from the date of its coming into force, in conformity with the provisions of article 26 of the Convention". To make this provision executive under Italian law, no further legislative measure was necessary, with the exception of those necessary to enable this type of request to be executed. See articles 16 and 17.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	Article 132, paragraph 4 ter of the Penal Code, regarding the protection of personal data, as per legislative decree no. 196 of 30 June 2003 foresees that: «*4*-ter. The Minister of the Interior or, with his authorization, the heads of the central offices specialized in computer or electronic matters of the State Police, of the Carabinieri Corps or of the Finance Corps, as well as the other subjects indicated in paragraph 1 of article 226 of the provisions of implementation, coordination and temporary actions of the Code of Criminal Procedure, as per legislative decree no. 271 of 28 July 1989, may order, also in relation to any requests made by foreign investigating authorities, providers and operators of computer or computer-related services to conserve and protect, in accordance with the modalities indicated, and for a period of not greater than ninety days, the data relating to computer-related traffic, but excluding the contents of communications, for the purpose of conducting preventive investigations as foreseen in the mentioned article 226 of the provisions as per legislative decree no. 271 of 1989, namely for purposes of ascertaining and repressing specific offences. This provision, which may be extended for justified requirements for a

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	total duration of not more than six months, may foresee special modalities of the custody of the data and the possible unavailability of said data by the providers and operators of computer or computer-related services or of third parties.. Paragraph *4*-quater of the same article states as follows: «The provider or the operator of computer or computer-related services to whom the order foreseen in paragraph 4-ter is given shall carry it out without any delay, immediately giving to the requesting authority his assurance of compliance. The provider or the operator of computer or computer-related services shall maintain secrecy relating to the order received and to the activities consequently carried out for the period indicated by the authority. In the event of any violation of this obligation the provisions as per article 326 of the Penal Code shall apply, unless the fact constitutes a more serious offence". Paragraph *4*-quinquies, lastly, foresees as follows: « The measures adopted as per paragraph 4-*ter* shall be communicated in writing, without delay and in any case within forty-eight hours of the notification to the receiver, to the Public Prosecutor of the place of enforcement who, if the requisite assumptions exist, confirms them. In the event of non-confirmation, the measures assumed shall lose their effect».
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 31 has been implemented by means of article 2 of law no. 48 of 18 March 2008, according to which "full and entire implementation has been made of the Convention, as from the date of its coming into force, in conformity with the provisions of article 26 of the Convention". To make this provision executive under Italian law, no further legislative measure was necessary, with the exception of those necessary to enable this type of request to be executed. See articles 16 et seq.
Article 32 – Trans-border access to stored computer data with	Article 32 has been implemented by means of article 2 of law no. 48 of 18 March

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	2008, according to which "full and entire implementation has been made of the Convention, as from the date of its coming into force, in conformity with the provisions of article 26 of the Convention". To make this provision executive under Italian law, no further legislative measure was necessary, with the exception of those necessary to enable this type of request to be executed. See article 16 et seq.
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.	Article 33 has been implemented by means of article 2 of law no. 48 of 18 March 2008, according to which "full and entire implementation has been made of the Convention, as from the date of its coming into force, in conformity with the provisions of article 26 of the Convention". To make this provision executive under Italian law, no further legislative measure was necessary. See article 20.
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 34 has been implemented by means of article 2 of law no. 48 of 18 March 2008, according to which "full and entire implementation has been made of the Convention, as from the date of its coming into force, in conformity with the provisions of article 26 of the Convention". To make this provision executive under Italian law, no further legislative measure was necessary. See article 21.
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	In compliance with article 35 of the Convention, article 13, paragraph 2 of law no. 48 of 18 March 2008, "Ratification and execution of the Convention of the Council of Europe on Cybercrime, held at Budapest on 23 November 2001 and measures to update national legislation" has foreseen that it is the responsibility of the Minister of Justice, in concert with the Minister of the Interior, to identify the point of contact.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	With its declaration dated 19.06.2009 Italy indicated as its point of contact as per article 35 § 1 of the Convention: SERVIZIO POLIZIA POSTALE E DELLE COMUNICAZIONI (POLICE POSTAL AND COMMUNICATIONS SERVICE) Via Tuscolana no. 1548 Email: htemergency@interno.it
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 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.	Italy has not yet submitted any of the reservations foreseen in article 42.

Back to the Table of Contents