Spain

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.

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	Concept of "traffic data": Article 588 ter b) Code of Criminal Procedure "Electronic data", of traffic or associated, means all data generated as a result of the communication transmission through a network of electronic communications, the availability to the user, as well as through the provision of a similar service from the company of information or telematic communication of similar kind.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	***Article 197 bis, paragraph 1 Criminal Code:*** 1. Whoever, by any means or procedure, in breach of the security measures established to prevent it, and without being duly authorised, obtains or provides another person with access to a computer system or part thereof, or who remains within it against the will of whoever has the lawful right to exclude him or her, shall be punished with a prison sentence of six months to two 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.	***Article 197 bis paragraph 2 Criminal Code:*** 2. Any person using technical devices or means to intercept non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions therefrom, and who is not duly authorised, shall be punishable by imprisonment of three months to two years or a fine of three to twelve months.
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.	***Article 264 CC*** 1. Whoever, by any means, without authorisation and in a serious way, were to erase, damage, deteriorate, alter, suppress, or make computer data, computer programs or electronic documents pertaining to others inaccessible, when the result produced is serious, shall be punished with a sentence of imprisonment of six months to three years.
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	***Article 264 bis CC*** 1. Punishment of six months to three years imprisonment, shall be imposed on any person who, without being authorised and in a serious way, hinders or interrupts operation of a computer system pertaining to another by: (a) any of the actions referred to in the preceding Article; (b) adding or transmitting data; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) destroying, damaging, disabling, removing or replacing a computer, telematics or electronic data storage system.
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, 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.	It should be noted that in our Criminal Code, due to systematic reasons, this specific provision of the Budapest Convention is regulated by two different articles: A.- On the one hand, Article 197 ter CC misuse of devices related to Article 197 bis 1º CC, referred to “Illegal Access to a computer system” and to Article 197 bis 2º CC, referred to “Illegal interception”: Any person who, with the intention of facilitating the commission of one of the offences referred to in Article 197(1) and (2) and Article 197bis (i.e. illegal system interference under Article 197(1) CC, illegal data interference under Article 197(2) CC, illegal access to a computer system under Article 197bis(1) CC or illegal interception of computer data under Article 197bis(2) CC), produces, procures, imports or otherwise makes available, without being duly authorised: a) a computer program designed or adapted principally to commit such offences; or b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.' Penalties: imprisonment of six months to two years or a fine of three to eighteen months B.- On the other, Article 264 ter, misuse of devices related to Article 264 CP “Data Interference” and Article 264 bis “System interference”: Imprisonment of six months to two years or a fine of three to eighteen months shall be imposed on any person who, with the intention of facilitating the commission of one of the offences referred to in the two Articles above, produces, procures, imports, or otherwise makes

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	available, without being duly authorised, one of the following tools: a) a computer program designed or adapted principally to commit one of the offences referred to in the two above Articles; or b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.
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.	The conduct described in Article 7 can be punished according to the Criminal Code, applying different precepts. Thus, concerning input, alteration, deletion, or suppression of computer data, it would imply the perpetration of the conduct already described in Article 264.1 CC. And such conduct might be considered concurring with the crime coinciding with the perpetrator's intent. Article 7 refers to the fact that the manipulation of computer data must have the intention of generating other data different from the original ones (forged data/not authentic) "with the intention that they be considered or used, to legal purposes, as authentic (…)" which could lead to consider the previous conduct concurring with an offence of documentary forgery. Regarding the alteration of electronic documents "with the intention that they be considered or used, to legal purposes, as authentic (…)", its criminal prosecution can be carried out through the application of any of the criminal figures that sanction, in generic terms, of the documentary forgery and that are specified in articles 390 to 399 of the CC In this context, it should be recalled that article 26 of the Spanish CC defines a document as "any material support that expresses or incorporates data, facts or narratives with evidential effectiveness or any other type of legal relevance", a concept that the case law of the Second

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Chamber of the Supreme Court has understood in the meaning of including any electronic document , a concept that the case law of the Second Chamber of the Supreme Court has understood to include any electronic document, as set out in the judgments handed down by the aforementioned Second Chamber of the Supreme Court on 19 May, 1991 ; 15 March, 1994 and 18 November, 1998 among others. However, this offence will be usually intended to produce an economic damage, which would be a fraud being the conduct as a whole contained in Article 248.2 a) of the CC. (See answer related to article 8, computer-related fraud).
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.	***Under Article 248(2) CC*** 1. In general, fraud is committed when, for profit, a person uses sufficient deceit to cause another person to commit an error, inducing them to carry out an act of disposal to their own detriment or that of another person. 2. The following persons shall also be found guilty of fraud: (a) Persons who, for profit, and by making use of a computer manipulation or similar scheme, bring about an unauthorised transfer of assets to the detriment of another person. (b) Persons who manufacture, upload, possess or supply computer programmes specifically aimed at committing the swindles provided for in this Article. (c) Persons who, by using credit or debit cards, or travellers' cheques, or the data contained in any of these, perform operations of any kind to the detriment of their holder or a third person. These conducts will be punished with six months three years imprisonment in case the amount of the fraud is 400€or more.(art. 249 CC).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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-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.	The conducts listed in Article 9.1 of the Budapest Convention have their appropriate correspondence in Article 189 of the Spanish Criminal Code. Thus, the conducts of Article 9.1 a), b) and c) of the Convention are included in Article 189.1 letter b) CC: b) produce, sell, distribute, display, offer or facilitate the production, sale, dissemination or display by any means of child pornography, or of pornography the production of which has involved a person with a disability requiring special protection, or possess such pornography for those purposes, even if the material is of foreign or unknown origin. Penalty: Prison from one to five years. And the conducts of Article 9.1 letters d) and e) of the Convention are covered by Article 189.5 paragraph 1 CC: - procurement for personal use or possession of child pornography or of pornography the production of which involved persons with a disability requiring special protection; Penalty: Prison from three months to one year or fine from six months to two years. On the other hand, the definitions of Article 9.2 of the Convention are contained in Article 189.1. 2nd paragraph of the CC: Child pornography or pornography the production of which has involved a person with a disability requiring special protection means: a) any material that visually depicts a child or a person with a disability

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	requiring special protection engaged in real or simulated sexually explicit conduct; b) any depiction, for primarily sexual purposes, of the sexual organs of a child or a person with disability requiring special protection; c) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes, unless the person appearing to be a child was in fact 18 years of age or older at the time of depiction; d) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes; According to article 183 CC the age for valid sexual consent is 16 years.
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,	Pursuant to Article 270 PC, any person who, for the purpose of obtaining a direct or indirect economic benefit and to the detriment of a third party, reproduces, plagiarises, distributes, publicly discloses or exploits economically in any other way all or part of a literary, artistic or scientific work or performance, or transforms, interprets or performs it artistically in any kind of support or medium, without the authorisation of the holders of the relevant intellectual property rights or their assignees, shall be punished by imprisonment of six months to four years and a fine of twelve to twenty-four months. 2. The same penalty shall be imposed on any person who, in the provision of information society services, for the purpose of obtaining a direct or indirect economic benefit and to the detriment of a third party, facilitates, in an active and non-neutral way and not limited to purely technical processing, access to, or placing on the internet of, works or performances that are the subject of intellectual property, without the permission of the holders or assignees of the corresponding rights, in particular by providing organised and classified lists of links to the works

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 content referred to above, even if those links had been initially supplied by the recipients of his or her services.
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. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	Under Spanish law, "those criminally responsible for offences are the principals and their accessories' (Article 27 CC). We find the definitions of 'perpetrator' and 'accessory' in Article 28 CC: Perpetrators are those who commit the act themselves, alone, jointly, or by means of another used as an instrument. The following shall also be deemed perpetrators: a) Whoever directly induces another or others to commit an offence; b) Whoever cooperates in committing an offence by carrying out an act without which there would have been no offence. And under Article 29 CC: 'Accessories are those who, not being included in the preceding Article, cooperate in carrying out the offence with prior or simultaneous acts.' In Spanish law, consummated offences and attempted offences are both punishable (Article 15 CC). Under Article 16 CC 1. An attempted offence takes place when a person begins to perpetrate an offence by direct action, perpetrating all or part of the acts that objectively should produce the intended result, and notwithstanding this, such is not attained due to causes beyond the control of the principal.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	2. Whoever voluntarily avoids the offence being consummated, either by going no further with its commission when already commenced, or by preventing the result from taking place, shall be exempt from criminal liability, without prejudice to the liability he may have incurred for the acts perpetrated, should these already have constituted another offence 3. When various subjects intervene in an act, the one or those who desist from execution thereof once already commenced, and who prevent or attempt to prevent consummation, in a serious, firm manner, shall be exempt from criminal liability, without prejudice to liability they may have incurred for the acts perpetrated, should these already have constituted another offence. In Spanish law, when the law establishes a punishment, it shall be considered that it is imposed on the perpetrators of the consummated crime (Article 61 CC). In general, the perpetrator in an attempted offence will be given a lower sentence by one or two degrees than that indicated by the law for the consummated offence, to the extent deemed appropriate taking account of the danger involved in the attempt and the degree of execution achieved (Article 62 CC) and accessories to a consummated or attempted offence will receive a punishment lesser in one degree than that established by the law for the principals in the same offence (Article 63 CC).
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.	***Article 31 bis.*** 1. In the cases referred to in this Code, legal persons shall be criminally liable for: a) The offences committed in the name or on behalf of them, and in their direct or indirect benefit, by their legal representatives or by those who acting individually or as part of a body of the legal person, are authorized to make decisions in the legal person's name, or have powers of organization and control within it.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	b) The offences committed, in the exercise of social activities and on behalf and in the direct or indirect benefit of them, by those who, being subject to the authority of the natural persons mentioned in the previous paragraph, could have carried out the facts for having seriously failed to supervise, watch and control their activity, taking into account the specific circumstances of the case. 2. If the offence was committed by the persons referred to in letter a) of the previous sub-section, the legal person shall be exempt from liability if the following requirements are met: 1st. The administration body has adopted and performed with efficiency, before the perpetration of the offence, organization and management models that include the suitable measures of surveillance and control in order to prevent offences of the same nature or to reduce significantly the risk of their perpetration; 2nd. The supervision of the performance and compliance of the prevention model introduced has been entrusted to a body of the legal person with independent powers of initiative and control or has legally entrusted the task of supervising the efficiency of the internal controls of the legal person; 3rd. The individual authors have committed the offence by fraudulently avoiding the models of organization and prevention and 4th. There has not been an omission or an insufficient exercise of their tasks of supervision, surveillance and control by the body referred to by the 2nd requirement. In cases where the previous circumstances can only be the object of partial accreditation, this circumstance will be considered in view of the mitigation of the penalty. 3. In small legal persons, the supervisory functions referred to in the 2nd requirement of paragraph 2 may be directly taken on by the board of directors. For that purpose, are legal persons of small dimensions,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	those which, according to the applicable legislation, are authorized to submit an abridged profit and loss account. 4. If the offence was committed by the individuals referred to in letter b) of sub-section 1, the legal person will be exempt from responsibility if, before the perpetration of the offence, it has adopted and performed successfully a model of organisation and management that proves to be appropriate to prevent offences of the kind of the one committed, or to reduce significantly the risk of its perpetration. In this case, the mitigation provided in the second paragraph, sub-section 2 of this article will also be applicable. 5. The models of organization and management referred to in the 1st requirement of sub-section 2 and the previous sub-section, shall meet the following requirements: 1st. They will identify the activities in the scope of which the offences to be prevented can be committed. 2nd. They will lay down the protocols or procedures that materialize the process of forming the will of the legal person, of decision making and of their performance in relation to those. 3rd. They will have models of financial resources management suitable to stop the perpetration of the offences to be prevented. 4th. They will impose the duty of informing about the possible risks and derelictions of duty to the body in charge of supervising the running and compliance with the prevention model. 5th. They will establish a disciplinary system that punishes adequately the failure to comply with the measures laid down by the model. 6th. They will carry out a periodical inspection of the model and of its possible modification when relevant infringement of its provisions are revealed, or when changes in the organization, control structure or the activity performed take place, making them necessary.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 31 ter. 1. The criminal liability of legal persons will be applicable whenever it is proved the perpetration of an offence that must have been committed by who holds the positions or functions referred to in the previous article, even when the specific liable individual has not been identified or it has not been possible to engage the procedure against him. When, as a consequence of the same facts, a fine would be imposed on both, the judges or courts will adjust the respective quantities, so that the resulting amount should not be disproportionate in relation with their seriousness. 2. The concurrence, in the individuals that have materially performed the facts or in the ones having made them possible for not having practised the due control, of circumstances affecting the defendant's guilt or that aggravate his liability, or the fact that the said individuals have died or have evaded justice, will neither rule out nor modify the criminal liability of the legal persons, without prejudice to the provisions of the following article.
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.	Regarding sanctions for natural persons they have been pointed out when describing each crime (articles 2 to 10, BC) Regarding legal persons see the scheme below Article 2 Convention Article 197 quinquies CC FINE FROM 6 MONTHS TO 2 YEARS POSSIBLITY OF IMPOSING ANY OF THE PENALTIES OF ARTICLE 33.7 letters b) to g) Article 3 Convention Article 197 quinquies CC FINE FROM 6 MONTHS TO 2 YEARS

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	POSSIBLITY OF IMPOSING ANY OF THE PENALTIES OF ARTICLE 33.7 letters b) to g) Article 4 Convention Article 197 quinquies CC FINE FROM 6 MONTHS TO 2 YEARS POSSIBLITY OF IMPOSING ANY OF THE PENALTIES OF ARTICLE 33.7 letters b) to g) Article 5 Convention Article 197 quinquies CC FINE FROM 6 MONTHS TO 2 YEARS POSSIBLITY OF IMPOSING ANY OF THE PENALTIES OF ARTICLE 33.7 letters b) to g) Article 6 Convention Article 197 quinquies CC FINE FROM 6 MONTHS TO 2 YEARS POSSIBLITY OF IMPOSING ANY OF THE PENALTIES OF ARTICLE 33.7 letters b) to g) Article 264 quater CC FINE (AMOUNT DEPENDS ON THE PRISON PENALTY ESTABLISHED FOR NATURAL PERSONS POSSIBLITY OF IMPOSING ANY OF THE PENALTIES OF ARTICLE 33.7 letters b) to g) Article 7 Convention PROPORTIONAL FINE POSSIBLITY OF IMPOSING ANY OF THE PENALTIES OF ARTICLE 33.7 letters b) to g)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 8 Convention Article 251 bis CC PROPORTIONAL FINE POSSIBLITY OF IMPOSING ANY OF THE PENALTIES OF ARTICLE 33.7 letters b) to g) Article 9 Convention Article 189 bis CC PROPORTIONAL FINE POSSIBLITY OF IMPOSING ANY OF THE PENALTIES OF ARTICLE 33.7 letters b) to g) Article 10 Convention Article 288 CC PROPORTIONAL FINE POSSIBLITY OF IMPOSING ANY OF THE PENALTIES OF ARTICLE 33.7 letters b) to g)
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 c the collection of evidence in electronic form of a criminal offence.	The measures foreseen n the Budapest Convention are governed in the Spanish legislation in the Chapters IV, V, IX and X of Title VIII, Book II, of the Code of Criminal Procedure. The application scope of these precepts is defined by articles 588 ter a) and 579.1, both of the Code of Criminal Procedure, jointly interpreted, and according to which:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	All measures about the interception of telephone or telematic communications and the access to the stored data shall apply to the following offences: Intentional crimes punished with a maximum of, at least, three years' imprisonment sentence. Offences committed within a criminal group or organisation. Terrorist offences. Offences committed through software tools or any other information or communication technology or communication service whichever the penalty is. In the case of remote recording of computer systems (not in the case of the usual recording of information massive storage devices), there are specific limitations provided for in Article 588 septies a) of the Code of Criminal Procedure, in the following terms: 1. The competent magistrate may authorise the use of identification data and codes, as well as the installation of software, allowing a remote and telematics examination, without the knowledge of the user or the owner, of the contents of a computer, electronic device, computer system, mass storage instrument or database, provided it is aimed at the investigation of any of the following criminal offences: a) Offences committed within criminal organisations b) Terrorist offences c) Offences committed against children or persons with legally modified capacity. d) Offences against the Constitution, treason and offences regarding national defence e) Offences committed through computer tools or by any other information technology, telecommunication or communication service. The assurance measure consisting in the specific preservation of computer data provided for in Article 588 octies of the Code of Criminal

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Procedure can be used in connection with the investigation of any criminal activity.
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.	All the inquiry measures established in the Code of Criminal Procedure and, in particular, the ones relating to the investigation of cybercrime are constitutionally subject to the provisions of Article 18 sub-sections 1,3 and 4 of the Spanish Constitution, namely: 1.-The right to honour, to personal and family privacy and to personal reputation is guaranteed. 3.-Secrecy of communications is guaranteed, particularly of postal, telegraphic and telephonic communications, except in the event of a court order to the contrary. 4.- The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights. Without prejudice to the specific rules concerning each of the measures provided for by the Code of Criminal Procedure, the general provisions about them – included in the above-mentioned Chapter IV - require judicial authorization for the adoption of nearly all of them except for the identification of holders or connectivity device terminals (art 578 ter m Code of Criminal Procedure). The assumptions on which the judicial authorization must be based are specified in Article 588 bis a), Code of Criminal Procedure, in the following terms: Article 588 bis a. Guiding principles. 1. During the pre-trial investigation, some of the inquiry measures provided for in this chapter can be applied as long as it is through a judicial authorization fully abiding by the principles of specialty, suitability, exceptionality, necessity and proportionality of the measure. 2. The principle of specialty requires that a measure should be related to the investigation of a specific crime. Measures of technological

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	investigation aiming at preventing or discovering offences or clearing up suspicions without an objective basis shall not be authorized. 3. The principle of suitability will define the objective and subjective scope and the duration of the measure according to its utility. 4. According to the principles of exceptionality and necessity, the measure can only be applied: a) when other measures less harmful for the human rights of the investigated or accused person but equally useful for the clarification of the fact are not available, or b) when the discovery or the verification of the investigated fact, the identification of its perpetrator or perpetrators and their whereabouts, or the location of the effects of crime could be seriously hampered without resorting to this measure. 5. The investigation measures provided for in this chapter will only be deemed as proportional when, having considered all the circumstances of the case, the sacrifice of the involved rights and interests does not exceed the benefit resulting from its adoption to the public and third party interest. For the weighting of the conflicting interests, the assessment of the public interest will be based on the seriousness of the fact, its social significance or the technological field of production, the intensity of the existing pieces of circumstantial evidence and the relevance of the results pursued with the restriction of the right Next, the Code of Criminal Procedure regulates in different articles aspects such as: -The specific content that the judicial decision must have (art 588 bis c) -The duration of the measure (article 588 bis e) explicitly stating that they will have the duration indicated for each of them without the possibility of exceeding the indispensable period of time to clarify the facts. -The control of the measure by the judicial authority (art 588 bis g) - Affecting a third party (art 588 bis h), referred to in the following terms: The investigation measures regulated in the following chapters can be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	granted even when they affect a third party in the cases and with the conditions laid down in the specific provisions of each of them. -The use, in other procedures, of the information obtained during an investigation and the discoveries by chance (art 588 bis i) -The destruction of registers once the judicial procedure has ended (article 588 bis k).
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.	***Article 588 octies. Data retention order*** The Public Prosecutor or the Judicial Police may request any natural or legal person to retain and protect specific data or information included in a storage computer system available to them until the corresponding judicial authorisation for their transfer is obtained in accordance with the provisions in the precedent articles. Data shall be retained for a maximum period of ninety days, which may be extended once, until the transfer is authorized or up to one hundred and eighty days. The person requested shall be obliged to cooperate and to maintain secrecy regarding the development of this measure, under liability described in Article 588 ter e., Subsection 3.
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:	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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.	Article 588 ter j) of the Code of Criminal Procedure is applicable. The precept refers to all kind of data and does not distinguish between content traffic data or subscriber's data. As it can be observed it refers both to the data stored under the law of data retention and to the data kept for commercial reasons or of another kind[1]. In addition, the Articles 588 ter k), with regard to identification by IP number and Article 588 ter m) allowing the identification of the holders of terminals or connectivity devices. These precepts do not limit its application to natural or legal persons having their domicile or registered office in Spain, therefore in can be understood that this order can refer to service providers settled in other States, in the terms and with the sense of Article 18 1 b) of the Budapest Convention. Supporting this standpoint, it is pertinent to mention the provisions of Articles 2 to 4 of the Law on services of the company of information and electronic trade 34/2002 of 11th July, namely Article 2. Service Providers settled in Spain. 1. This Law will apply to the service providers of the information company settled in Spain and to the services provided by them.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	A service provider will be considered to be settled in Spain when his residence or registered office is on Spanish territory, as long as these coincide with the place where the administrative management and their business direction are indeed centralized. Otherwise, the place where the said management or direction takes place will be taken into account. 2. Furthermore, this Law will be applicable to the services of the information company that the providers resident or living in another State offer through a permanent establishment located in Spain. A provider is considered to work through a permanent establishment located on the Spanish territory when he has, in a continuous or regular way, work facilities or premises, in which he carries out all or part of his activity. 3. For the purposes provided in this Article, the service provider is considered to be settled in Spain when the provider or some of his offices have been registered in the Trade Register or in another Spanish public register in which the registering is necessary to acquire the legal status. The use of technological means located in Spain, for the provision or access to the service, cannot be a criterion to determine, on its own, the establishment in Spain of the provider. 4. The service providers of the information company settled in Spain will be subject to the rest of provisions of the Spanish legal system applicable to them, depending on the activity that they develop, regardless of the use of electronic means for their execution. Article 4 Providers established in a Stated outside the European Union or the European Economic Area. The providers established in countries not belonging to the European

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Union or the European Economic Area will abide by the provisions of Articles 7.2 and 11.2. Paragraph 1 of Article 4 drawn by the sub-section one of Article 4 of the Law 56/2007, of 28th December, on Measures to Foster the Society of Information («O.J.» 29th December). Validity: 30 December2007. The providers specifically aiming their service at the Spanish territory will also be subject to the obligations provided by this Law, as long as this does not contravene the provisions of the applicable international treaties of conventions. Namely, Article 8 of the abovementioned rule lays down in this regard : Article 8. Restrictions on the service provision and procedure of cooperation within the European Community. 1. In case a certain service of the information company infringes or could infringe the principles listed below, the competent bodies for their protection, in the exercise of the tasks they have legally assigned, can adopt the necessary measures so that their provision is suspended or to withdraw the data that damage them. The principles referred to in this sub-section are the following: a) The safeguard of law and order, the criminal investigation, public security and national defence. b) The protection of public health of natural and legal persons having the status of consumers or users, or even acting as investors. c) The respect for the person's dignity and for the principle of non-discrimination on the grounds of race, sex, religion, opinion, nationality, disability or any other personal or social circumstance, and, d) The protection of the young and children. e) The safeguard of intellectual property rights. Finally and concerning the concept of the subscriber's data, there is no rule stating the scope of this precept in the criminal code or in the code of criminal procedure. Nonetheless, the appendix II of the General Law on Telecommunications 9/2014, defines the concept of subscriber in the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	following terms: any natural or legal person having concluded a contract with a provider of services of electronic communications available to the public, for providing those services According to the Circular 1/2013 of 20th March, of the Commission of Telecommunications Market on the supply procedure and the reception of the subscribers' data, the following will be considered as such: -Identification of the holder - natural person: name and surname, DNI, NIF, NIE or passport - legal person: registered office, NIF, trade name. -Identification of the user - similar data concerning natural or legal persons -Complete address (postal identification of the subscriber) -Numbers of subscribers (ranks and/or individual numbers) -list of numbers allocated to the postal address -consent for publishing the data or their use with commercial or advertising purposes -kind of terminal, if appropriate, - method of payment - operator . %
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	Search and seizure of stored computer data is regulated in Spanish Code of Criminal Procedure in Chapter VIII of Title VIII, Book II (Articles 588 sexies a) b) and c), which reads as follows: Article 588 sexies a. Need for individual justification 1. When, on the occasion of a house search, it can be expected that computers, telematics or telephone communication tools, mass storage digital devices are seized, or that access to telematics data repositories is produced, the decision issued by the Examining Magistrate shall extend the reasoning to justify, where appropriate, the reasons legitimating the access to the information contained in such devices on the part of the agents appointed.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	2. The mere seizure of any of the above mentioned devices, carried out during a house search, does not legitimate the access to its contents, without prejudice to the fact that access may be afterwards authorized by the competent magistrate. Article 588 sexies b. Access to the information contained in electronic devices seized outside the address of the investigated person The requirement under Subsection 1 of the previous article shall also be applicable when computers, communication tools or mass storage devices, or the access to data telematics repositories, are seized independently of a house search. In such circumstances, officers shall inform the magistrate on the seizure of these items. Should the magistrate consider indispensable to have access to the information hosted in them, the corresponding authorization shall be granted. Article 588 sexies c. Judicial authorisation. 1. The decision of the Examining Magistrate by which access to the information contained in the above-mentioned devices is authorized shall establish the terms and the extent of the search and may authorise making copies of computer data. It shall also set out the conditions required to ensure the integrity of data and guarantee their safekeeping in order to allow, where appropriate, the practice of an expert examination. 2. Unless they constitute the object or the instrument of the offence or there are other substantive reasons for it, the confiscation of physical carriers housing the computer data or files must be avoided whenever it can cause serious damage to the holder or the owner and it is possible to obtain a copy under conditions guaranteeing the authenticity and the integrity of data. 3. When those conducting a search or having access to the information

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	system or to a part of it, in accordance with the provisions in this chapter, have well-founded reasons to believe that the information sought is stored in another computer system or in part of it, they may expand the search, providing such data are lawfully accessible by means of the initial system or available to it. An extended search must be authorized by the magistrate, unless already included in the initial authorization. In case of emergency, the Judicial Police or the prosecutor may carry it out, informing the magistrate immediately and in any case within twenty-four hours maximum, about the action carried out, the way it was conducted and the result obtained. The competent magistrate, also stating the grounds for it, shall revoke or confirm the action within a maximum term of seventy-two hours from the moment interception was ordered. 4. In case of emergency, where a legitimate constitutional interest is discerned rendering indispensable the measure foreseen in the previous Sub-sections of this article, the Judicial Police may carry out a direct examination of data contained in the apprehended device, informing the competent magistrate immediately, and in any case within twenty-four hours maximum, by means of a written report stating the reasons justifying the adoption of the measure, about the action undertaken, the way it has been conducted and the result obtained. The competent magistrate, also stating the grounds for it, shall revoke or confirm the action within a maximum term of seventy-two hours from the moment the measure was ordered. 5. Authorities and officers in charge of the investigation may order any person with knowledge on the operation of the computer system or the measures implemented to protect the computer data contained in it, to provide all necessary information, provided this does not involve a disproportionate burden on the person concerned, on pain of being otherwise guilty of disobedience. This provision shall not be applicable to the investigated or accused

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	person, to those exempted from the obligation to declare for reasons of family relationship and those that, in accordance with Article 416.2, cannot declare being bound under the obligation of professional secrecy.
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: 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.	There is not specific regulation on this subject in Spanish law, but real-time collection of traffic data is regulated jointly with the interception of content. Article 588 bis c Code of Criminal Procedure refers to the need that the judicial authority authorizing the interception of communications, has to establish the scope of the interception, in the following terms: Article 588 bis c. Judicial decision. 1. The examining magistrate shall authorize or refuse the requested measure through a reasoned order, having heard the Public Prosecutor. This decision will be rendered within the twenty-four hours following the submission of the request. 2. Whenever it is necessary to rule on the compliance of some of the requirements set out in the previous articles, the magistrate may require an extension or clarification of the request terms, interrupting thus the term referred to in the preceding subsection,. 3. The judicial decision whereby the measure is authorized shall at least state the following points: a) The punishable deed object of inquiry and its juridical qualification, stating the prima facie on which the measure is based. b) The identity of the individuals investigated or of any other person affected by the measure, if known. c*) The extension of the interference measure, specifying its scope as well as the grounds concerning the adherence to the ruling principles set out in Article 588 bis a.*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	d) The investigating unit of the Judicial Police assuming the intervention. e) La duration of the measure f) The way and the periodicity with which the applicant shall inform the judge about the results of the measure. g) The aim pursued by the measure. h) The legally bound party who shall carry out the measure, if known, with express reference to the duty of collaboration and secrecy, when appropriate, on incurring a crime of disobedience.
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. 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 pointed out before concerning the interception of traffic data, there is not a specific interception for the contents. Both topics are jointly tackled in section I, Chapter V, Title VIII, Book II of the Code of Criminal Procedure, namely in Articles 588 ter a) a i) under the heading interception of telephone and telematic communications. In each case, it is the Judge who, when he sets the scope of the specific measure, defines whether the interception in real time refers only to traffic data or also to content data. Article 588 ter a. Applicable cases. The authorization for the interception of telephone and telematic communications can only be granted when the inquiry focuses on some of the offences referred to in Article 579.1 of this law or offences committed through software tools or any other information or communication technology or communication service. Article 588 ter b. Scope. 1. The terminals or media object of intervention must be those habitually or occasionally used by the investigated person. 2. The court agreed intervention may authorize the access to the content of the communications and traffic electronic data, or associated with the communication process, as well as to those occurring regardless of the establishment or not of a specific communication, involving the investigated individual, either as transmitter or receiver, and can affect terminals or the media of which the person under

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	investigation is the owner or user. The terminals or media of the victim can also be intervened when a serious risk to his life or integrity is foreseeable. For the purposes set forth in this article, electronic data of traffic or associated refer to all those that are generated as a result of the communication through a network of electronic communications, of its making it available to the user, as well as the service provision by a company of information or telematics communication of similar nature. Article 588 ter c. Affecting third parties. The judicial intervention of the communications issued from terminals or telematic media belonging to a third party may be granted provided that: 1st. There is evidence that the investigated individual uses it to transmit or receive information, or 2nd . The holder cooperates with the investigated person in his illicit purposes or benefits from his activity. Such intervention may also be authorized when the device under investigation is used maliciously online by a third party, without the knowledge of its owner. Article 588 ter d. Request for judicial authorization. 1. The request for judicial authorization shall include, in addition to the requirements mentioned in Article 588 bis b, the following: a) the identification number of the subscriber, of the terminal or of the technical label, b) the identification of the connection object of the intervention or c) the necessary data to identify the means of telecommunication in question. 2. In order to determine the measure scope, the request for judicial authorization may aim at one of the following issues: a) The register and recording of the communication content, stating the way or kind of communications affected.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	b) The knowledge of its origin or destination, at the moment in which the communication takes place. c) The geographical position of the origin or destination of the communication. d) The knowledge of other traffic data associated or not, but of added value to the communication. In this case, the request shall specify the concrete data to be obtained. 3. In case of emergency, when inquiries are carried out for the investigation of offences relating to the activities of armed bands or terrorist elements and there are well-founded reasons that make the measure provided for in the preceding sub-sections of this article indispensable, the Minister of Interior or, in his absence, the State Secretary for Security may order it. This measure will be immediately reported to the competent magistrate and, in any case, within the maximum period of twenty-four hours, stating the reasons which justified the taking of the measure, the action performed, the way in which it has been carried out and its result. The competent magistrate, also in a reasoned way, shall revoke or confirm such action in a maximum period of seventy-two hours since the measure was ordered. Article 588 ter e. Duty of collaboration. 1. All the providers of telecommunications services, of access to a telecommunications or services network of the information society, as well as any person that contributes in any way to facilitate the communications through telephone or any other means or system of telematic logical or virtual communication, are obliged to provide the magistrate, the Public Prosecutor and the officers of the Judicial Police appointed to carry out the measure, with the assistance and collaboration required to facilitate the implementation of the telecommunications intervention ruling. Article 588 ter f. Control of the measure. In compliance with the provisions of Article 588 bis g, the Judicial Police will put at the disposal of the magistrate, with the frequency determined

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	by the latter and on different digital carriers, the transcription of the passages deemed of interest and the complete recordings made. The source and destination of each of them shall be indicated and it shall be secured by means of a system of stamping or advanced electronic signature or a sufficiently reliable certification system, the authenticity and integrity of the information transferred from the central computer to the digital carriers on which the communications would have been recorded. Article 588 ter g. Duration. The maximum initial duration of the intervention, to be counted from the date of the judicial authorization, will be of three months, extendable for successive periods of the same duration up to the maximum period of eighteen months. Article 588 ter h. Request for an extension For the justification of the request for extension, the Judicial Police shall provide, where appropriate, the transcription of those passages of the talks from which the relevant information is deducted to decide on the maintenance of the measure. Before rendering the decision, the magistrate may request clarifications or further information, including the full contents of the conversations tapped. Article 588 ter i. Access of the parties to the recordings. 1. Being the secret lifted and the duration of the intervention measure expired, the parties shall receive a copy of the recordings and transcripts made. If the recording contained data relating to aspects of the private life of the people, only the recording and transcripts of those parts that do not relate to them will be handed out. The non-inclusion of the whole transcription handed out shall be expressly stated.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	2. Once examined the recordings and within the period set by the magistrate, in view of the volume of information contained in the carriers, either party may request the inclusion in the copies of those communications deemed pertinent and that had been excluded. The investigating magistrate, having heard or examined these communications, shall decide about their exclusion or inclusion in the case. 3. The investigating magistrate shall notify the people participating in the intercepted communications about the fact of practising the interference and they will be informed of the specific communications in which they may have participated that would be affected, unless it were impossible, it required a disproportionate effort or they could be detrimental to future investigations. If the notified person requests it, he will be given a copy of the recording or transcript of such communications, to the extent that this does not affect the right to privacy of others or is contrary to the purposes of the process under which the measure of interference has been adopted As for the application scope of these precepts and the guarantees and safeguards when these measures are performed, we refer to the comments on Articles 14 and 15 of the Budapest Convention.
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.	The scope of the Spanish jurisdiction in criminal matters is provided in Article 23 of the Organic Law of the Judiciary (LOPJ), which includes the competences of Spanish Courts in the following terms Article 23. 1. In the criminal law it will fall to the Spanish jurisdiction the trial of the cases of offences and misdemeanours committed on Spanish territory or committed on board of Spanish vessels or aeroplanes, without prejudice to the provisions of the international treaties to which Spain is

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	a party. 2. The Spanish jurisdiction will also be in charge of the offences committed outside the national territory, provided that the criminally responsible individuals are Spanish or foreigners having acquired the Spanish nationality after the perpetration of the fact, and with the presence of the following requirements. a) The fact is punishable in the place of execution, except that, by virtue of an international Treaty or the regulations of an international Organization of which Spain is member, this requirement would not be necessary, without prejudice to the provisions of the following subsections. b) The aggrieved person or the Public Prosecutor lodges a complaint before the Spanish Courts. c) The offender has not been acquitted, pardoned or punished abroad or, in the last case, has not served the sentence. If he has only served it partially, this will be taken into account to reduce it proportionally as appropriate. 3. The Spanish jurisdiction will deal with the facts committed by Spaniards or foreigners outside the national territory when they are likely to be defined, according to the Spanish criminal law, as some of the following offences: a) Treason and against the peace or the independence of the State. b) Against the Holder of the Crown, his Spouse, his Successor or the Regent. c) Rebellion and insurrection. d) Forgery of the royal signature or stamp, of the State stamp, of the Ministers' signatures and of public or official stamps. e) Forgery of Spanish currency and its issuing. f) Any other king of forgery that is directly detrimental to the State's reputation or interests, and introduction or issuing of the forgery. g) Attack against Spanish authorities or public officials.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	h) The offences committed in the exercise of their duties by Spanish public officials living abroad and the offences against the Spanish Public Administration. i) The ones related to the exchange control. Finally the 4th sub-section of the same precept includes the principle of universal justice in relation to certain offences (are included only the reference to those contained in Articles 2 to 11 of the Budapest Convention or of the Additional Protocol against Racism or Xenophobia): 4. Likewise, the Spanish jurisdiction will be competent to try the facts committed by Spaniards or foreigners outside the national territory that can be defined, according to the Spanish law, as some of the following offences, when there are the stated conditions: a) Genocide, crimes against humanity or against protected individuals and goods in case of an armed conflict, as long as the proceedings are against a Spaniard or against a foreign citizen living usually in Spain, or against a foreigner that is in Spain and whose extradition would have been refused by the Spanish authorities. j) Offences of setting-up, financing or belonging to a criminal group or organization, or offences committed within them, provided that they are groups or organizations whose action aims at the perpetration, in Spain, of an offence punished with a maximum penalty equal or superior to three years of imprisonment. k) Offences against sexual freedom and indemnity committed on victims under age, as long as: 1st. the proceedings are against a Spaniard; 2nd. the proceedings are against a foreign citizen living habitually in Spain; 3rd. the proceedings are against a legal person, company, organization,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	groups or any other kind of entities or associations of individuals having their registered office in Spain; or, 4th. the offence was committed against a victim that, at the moment of the perpetration of the facts, had the Spanish nationality or whose habitual residence was in Spain. p) Any other kind of offence the prosecution of which is mandatory by a Treaty in force for Spain or by other regulations of an International Organization of which Spain is member, in the cases and conditions laid down in them. Likewise, the Spanish jurisdiction will always be competent to try the offences above committed outside the national territory by foreign citizens that are in Spain and whose extradition had been refused by the Spanish authorities, provided that this is imposed by a Treaty in force for Spain. 5. The offences referred to in the previous sub-section will not be prosecutable in Spain in the following cases: a) When a procedure for their investigation and prosecution has been started in an International Court formed according to the Treaties and Conventions to which Spain is party. b) When a procedure for their investigation and prosecution has been started in the State where the facts were committed or in the nationality State of the person accused of the perpetration, provided that: 1st. The person accused of the perpetration of the fact was not on the Spanish territory; or, 2nd. a procedure had been started for his extradition to the country of the location where the facts were committed or of the nationality of the victims, or to put it at the disposal of an International Court so that he would be tried by them, except that the extradition was not authorized. The provision of this sub-section b) will not be applicable when the State

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	exercising its jurisdiction would not be willing to carry out the investigation or could really not do it, and it would be so deemed by the 2nd Division of the Supreme Court, to which the Judge or Court will submit a reasoned statement. In order to determine whether there are or not disposition to act in a specific case, it will be examined, keeping into account the principles of a process with the due guarantees recognized by the International Law, if there are one or several of the following circumstances, depending on the case: a) The trial has been or is ongoing or the national decision has been adopted with the aim of removing the person in question from his criminal liability. . b) There has been an unjustified delay in the trial that, given the circumstances, would be incompatible with the intention of making the person appear in court. c) The trial has not been or is not being substantiated in an independent or impartial way, or is being carried out in a way that, considering the circumstances, is incompatible with the intention of making the person appear in court. In order to determine the incapacity to investigate or prosecute in a certain case, it will be examined whether the State, due to a total or substantial standstill of its national justice administration or to the fact that it does not have it, cannot make the defendant appear in court, does not have the necessary evidence and statements or, due to other reasons, is not in the situation of carrying out a trial. 6. The offences referred to in the sub-sections 3 and 4 will only be prosecutable in Spain when the aggrieved party or the Public Prosecutor have previously lodged a complaint.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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, 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	Regarding Articles 24 to 28, on International Cooperation, they all are covered by Article 96.1 of the Spanish Constitution which states: "Validly concluded international treaties, once officially published in Spain, shall form part of the internal legal order. Their provisions may only be repealed, amended or suspended in the manner provided in the treaties themselves or in accordance with the general rules of international law." As long as Budapest Convention has been published in the State Official Gazette the 17th September 2010, **the dispositions of this Convention are mandatory and directly applicable in Spain.** Active extradition is regulated in the Title VI ('The extradition procedure') of Book IV of the Criminal Procedure Law (Articles 824 to 833). The passive extradition is governed by the Passive Extradition Act, 4/1985. It should be borne in mind, however, that these provisions are of subsidiary application in respect of international conventions and treaties signed by Spain. Thus, Article 1 of the Passive Extradition Act provides: The conditions, procedures and effects of passive extradition shall be governed by this Law, except as expressly provided for in the Treaties to which Spain is a party. In any event, extradition shall be granted only on the basis of the principle of reciprocity. The Government may require a guarantee of reciprocity to the requesting State. Although the procedure as a whole is basically judicial, there is also a stage of an administrative nature, with the approval of the Council of Ministers, at the beginning of the procedure and, at the end, to approve the surrender.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	See reference above.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	See reference above.
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. 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;	See reference above.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	See reference above.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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:	As long as Spanish legislation regulates this investigative measure, there will be no obstacle in responding to these kinds of requests.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	As long as Spanish legislation regulates this investigative measure, there will be no obstacle in responding to these kinds of requests.
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	As long as Spanish legislation regulates this investigative measure, there will be no obstacle in responding to these kinds of requests.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	As long as Spanish legislation regulates this investigative measure, there will be no obstacle in responding to these kinds of requests.
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.	As long as Spanish legislation regulates this investigative measure, there will be no obstacle in responding to these kinds of requests.
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.	As long as Spanish legislation regulates this investigative measure, there will be no obstacle in responding to these kinds of requests.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	The designated Central Authority is the General Commissariat of the Judicial Police of the Ministry of Interior.
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.	No reservations have been made

Back to the Table of Contents