Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version 25 March 2010

Cybercrime legislation – country profile

PORTUGAL

This profile has been prepared within the framework of the Council of Europe's capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	**Portugal**
Signature of Convention:	23.11.2001
Ratification/accession: ***Provisions of the Convention***	24.03.2010 ***Corresponding provisions/solutions in Portugal legislation***
Chapter I – Use of terms	
Article 1 – Definitions 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	Cybercrime Law - Law nr 109/2009 (15 th of September) - Article 2 **Article 2 - Definitions** For the purposes of this Law: a) "computer system" means any device or set of connected or related devices, in which one or more of these produces, running a program, the automated

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*"*	processing of data, and the network that supports communication between them and the set of data stored, processed, retrieved or transmitted by that or those devices, with a view to its operation, use, protection and maintenance; b) "computer data" means any representation of facts, information or concepts in a format capable of being processed by means of a computer system, including programs able to make a computer system to perform a function; c) "traffic data" means computer data relating to a communication made through a computer system, generated by this system as part of a chain of communication, indicating the origin of the communication, the destination, route, time, the date, size, duration or type of underlying service; d) "service provider" means any entity, public or private, that provides users of its services the ability to communicate through a computer system and any other entity that stores computer data on behalf and of that service or its users; e) "Interception" means the act intended to capture information in a computer system, using electromagnetic devices, acoustic, mechanical or other; f) "topography", a series of images linked together, regardless of how they are fixed or encoded, representing the three-dimensional configuration of the layers that make up a semiconductor product and in which each image reproduces the drawing, or part of a surface of the semiconductor product, whatever stage of their manufacture; g) "semiconductor product" means the final or intermediate form of any product, comprising a substrate that includes a layer of semiconductor material and comprising one or more layers of conductive, insulating or semiconducting, according to the arrangement to a three-dimensional configuration and intended to fulfil, exclusively or not, an electronic function.
Chapter II – Measures to be taken at the national level	

Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when 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	Cybercrime Law - Law nr 109/2009 (15th of September) - Article 6 **Article 6 - Illegal access** 1 - Any person who, without legal permission or without being authorized to do so by the owner, in any manner accedes to a computer system, shall be punished with imprisonment up to 1 year or with a fine of up to 120 days. 2 - The same penalty will be applied to whoever illegally produces, sells, distributes or otherwise disseminates within one or more computer systems devices, programs, a set of executable instructions, code or other computer data intended to produce the unauthorized actions described under the preceding paragraph. 3 - The penalty will be imprisonment up to 3 years or a fine if access is achieved through violation of safety rules. 4 - The penalty will be imprisonment of 1 to 5 years if: a) by means of this access, the agent becomes aware of commercial or industrial secrets or confidential information protected by law, or b) The benefit or pecuniary advantage obtained is of considerably high value. 5 - The attempt is punishable, except regarding paragraph 2. 6 - In the cases referred to in paragraphs 1, 3 and 5 the prosecution depends on of the complaint.
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.	Cybercrime Law - Law nr 109/2009 (15th of September) - Article 7 **Article 7 - Unlawful interception** 1 - Any person who, without legal permission or without being authorized to do so by the owner, other right holder of the system or part of it, through technical means intercepts transmissions of computer data processed within a computer system, to there directed or from there proceeding, will be punished with imprisonment up to 3 years or a fine. 2 - The attempt is punishable. 3 - The same penalty provided for in paragraph 1 will be applied to those who illegally produce, sell, distribute or otherwise disseminate within one or more computer systems devices, software or other computer data intended to produce the unauthorized actions described under that paragraph.

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.	Cybercrime Law - Law nr 109/2009 (15th of September) - Article 4 **Article 4 - Computer damage** 1 - Any person who without legal permission or without being authorized to do so by the owner, other right holder of the system or part of it, deletes, alters, destroys, in whole or in part, damages, removes or renders unusable or inaccessible programs or other computer data of others or in any way affects their ability to use, shall be punished with imprisonment up to 3 years or a fine. 2 - The attempt is punishable. 3 - The same penalty of paragraph 1 will be applied to those who illegally produce, sell, distribute or otherwise disseminate to one or more computers or other systems devices, software or other computer data intended to produce the unauthorized actions described in that paragraph. 4 - If the damage is of high value, the penalty is imprisonment up to 5 years or a fine of up to 600 days. 5 - If the damage is pretty high value, the penalty is imprisonment of 1 to 10 years. 6 - In the cases provided for in paragraphs 1, 2 and 4 the prosecution depends on the complaint.
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	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 5 **Article 5 - Computer sabotage** 1 - Any person who, without legal permission or without being authorized to do so by the owner, other right holder of the system or part thereof, prevent, stop, or severely disrupt the operation of a computer system through the introduction, transmission, damage, alteration, deletion, preventing access or removal of programs or other computer data or any other form of interference in the computer system is punished with imprisonment of up to 5 years or a fine of up to 600 days. 2 - The same penalty will be applied to those who illegally produce, sell, distribute or otherwise disseminate to one or more computer systems devices, software or other computer data intended to produce the unauthorized actions described in the preceding paragraph. 3 - In the case of the preceding paragraph, the attempt is not punishable. 4 - The penalty will be imprisonment of 1 to 5 years if the damage arising from disturbance is of high value.

	5 - The penalty will be imprisonment of 1 to 10 years if: a) damage arising from disturbance is considerably high value; b) the disturbance reaches seriously a computer system that supports an activity designed to provide critical social functions, including supplying chains, health, safety and economic well-being of persons, or the regular functioning of public services.
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.	Cybercrime Law - Law nr 109/2009 (15th of September) – Articles 3, nr 4, 4, nr 3, 5, nr 2, 6, nº 2 and 7, nr 3 **Article 3 - Computer forgery** 4 - Whoever imports, distributes, sells or holds for commercial purposes any device that allows the access to a computer system, to a payment system, to a communications system or to a conditioned access service, on which was committed any of the actions referred to in paragraph 2 is punished with imprisonment of 1 to 5 years. **Article 4 - Computer damage** 3 - The same penalty of paragraph 1 will be applied to those who illegally produce, sell, distribute or otherwise disseminate to one or more computers or other systems devices, software or other computer data intended to produce the unauthorized actions described in that paragraph. **Article 5 - Computer sabotage** 2 - The same penalty will be applied to those who illegally produce, sell, distribute or otherwise disseminate to one or more computer systems devices, software or other computer data intended to produce the unauthorized actions described in the preceding paragraph. **Article 6 - Illegal access** 2 - The same penalty will be applied to whoever illegally produces, sells, distributes or otherwise disseminates within one or more computer systems devices, programs, a set of executable instructions, code or other computer data intended to produce the unauthorized actions described under the preceding paragraph. **Article 7 - Unlawful interception** 3 - The same penalty provided for in paragraph 1 will be applied to those who

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.	illegally produce, sell, distribute or otherwise disseminate within one or more computer systems devices, software or other computer data intended to produce the unauthorized actions described under that paragraph.
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.	Cybercrime Law - Law nr 109/2009 (15th of September) - Article 3 **Article 3 - Computer forgery** 1 - Whoever, with intent to cause deception in legal relations, enters, modifies, deletes or suppresses computer data or otherwise interferes with computer data to produce information or documents that are not genuine, with the intention that they can be considered or used for legally relevant purposes as if they were, is punished with imprisonment up to 5 years or a fine of 120 to 600 days. 2 - When the actions described in the previous paragraph relate to the data registered or incorporated in a banking card or any other device that allows the access to a payment system or to a communications system or to a conditioned access service, the penalty is 1 to 5 years in prison. 3 - Whoever, acting with intent to cause injury to others or to obtain an unlawful gain for him or her or for others, makes use of a document made of computer data that were the subject of the acts referred to in paragraph 1 or a card or other kind of device in which it were registered or incorporated the data of the acts referred to in the preceding paragraph, shall be punished with the penalties provided for in either number, respectively. 4 - Whoever imports, distributes, sells or holds for commercial purposes any device that allows the access to a computer system, to a payment system, to a communications system or to a conditioned access service, on which was committed any of the actions referred to in paragraph 2 is punished with imprisonment of 1 to 5 years. 5 - If the facts referred to in the preceding paragraphs are committed by an official employee in the performance of their duties, the penalty is imprisonment of 2 to 5 years.

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.	Penal Code - Article 221 **Article 221 - Computer and communications fraud** 1 - Whoever, with intent to obtain for himself or for someone unlawful enrichment, causes loss of another person property, interfering in the result of treatment of computer data or by incorrect structuring of a program computer, incorrect or incomplete use of computer data or by some other unauthorized processing of data or intervention in data, will be punished with imprisonment up to three years or a fine. 2 - The same penalty applies to those whoever, with intent to obtain for themselves or for others an unlawful gain, causes financial loss to another, using programs, electronic devices or other means which, separately or together, are intended to reduce, amend or prevent, in whole or in part, the normal functioning or operation of telecommunications services. 3 - The attempt is punishable. 4 - The prosecution relies on the complaint. 5 - If the injury is: a) high value, the perpetrator is punished with imprisonment up to five years or a fine of up to 600 days; b) a considerably high value, the agent is punished with imprisonment from two to eight years. 6 - It is also applicable to the provisions of Article 206º.
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	Penal Code – Article 176 **Article 176 - Child pornography** 1 - Whoever: a) Uses a minor in a pornographic show or entices that minor for that purpose; b) Uses a minor in photography, film or other pornographic record, in whatever form, or entices that minor for that purpose; c) Produces, distributes, imports, exports, distributes, displays or assigns, in any way or by any means, the materials mentioned in the preceding paragraph; d) Acquires or possesses materials mentioned in b) with the intent to distribute, import, export, advertise, display or transfer;

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.	will be punished with imprisonment of one to five years. 2 - Whoever commits the acts described in the preceding number professionally or with profit purposes, will be punished with imprisonment of one to eight years. 3 – Whoever commits the acts described in c) and d) of number 1 using pornographic material with realistic representation of a minor will be punished with imprisonment up to two years. 4 - Whoever acquires or possesses materials provided in b) of number 1 shall be punished with imprisonment up to one years or a fine. 5 - The attempt is punishable.
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	Cybercrime Law - Law nr 109/2009 (15th of September) - Article 8 and Decree-Law nr 252/94 (20th of October) (Directive nr. 91/250/CEE) – Article 14. Also Law nr 45/85 (17 September) – Articles 195, 196, 199, 218 and 224 (*Código de Direito de Autor*), amended by Law nr 16/2008 (1 April) **Cybercrime Law - Article 8 - Illegal reproduction of protected program** 1 - Whoever illegally reproduces discloses or communicates to the public a computer program protected by law will be punished with imprisonment up to 3 years or a fine. 2 - The same penalty will be applied to whoever illegally reproduces the topography of a semiconductor product, or commercially exploits or imports for these purposes a design or a semiconductor product manufactured from the same topography. 3 - The attempt is punishable **Decree-Law nr 252/94 (20th of October) - Article 14**

infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**Article 14 - Criminal Protection** 1 - A computer program is protected from criminal unauthorized reproduction. 2 - It is applicable to computer software to the provisions of paragraph 1 of Article 9 of Law No. 109/91 of 17 August. (*The Act was repealed and replaced by Law No. 109/2009, and Article 9, paragraph 1 be replaced by the new Article 8, paragraph 1)* **Law No. 45/85, September 17, as amended by Law No. 16/2008 (*Código de Direito de Autor*)** **Article 195 - Usurpation** 1 – It shall commit the crime of usurpation whoever, without authorization from the author or artist, phonogram producer and image storage or the broadcaster, uses a work or performance by any of the methods provided in this Code. 2 – It also commits the crime of usurpation: a) Whoever unlawfully discloses or publishes a work not disclosed nor published by its author or not destined for distribution or publication, even if he present it as it belongs to the author whether or not he pretends any economic advantage; b) Whoever collects or compiles published or unpublished works without permission of the author; c) Whoever, being authorized to use a work, phonogram or broadcast program, uses it beyond the limits of authorization, except as expressly provided in this Code. 3 – It shall be punished with the penalties provided in Article 197 the author who has submitted, in whole or in part, their rights or having authorized the use of his work by any manner prescribed in this Code, uses directly or indirectly the rights assigned to others. **Article 196 – Counterfeiting** 1 – It shall commit the crime of counterfeiting whoever uses, as its creation or provision, work, phonogram, broadcasting that is mere total or partial reproduction of the work or performance of others, disclosed or undisclosed, or so similar that does not have individuality. 2 - If the reproduction mentioned above represent only a portion or fraction of the work or performance, only that part or fragment is considered as counterfeiting. 3 - To be counterfeit it is not essential that the reproduction is made by the same

	process as the original, with the same size or with the same format. 4 – It does not constitute infringement: a) the resemblance between duly authorized translations of the same work, or between photographs, drawings, engravings or other forms of representation of the same subject, if, despite the similarities due to the identity of the object, each of the works has its own individuality; b) the reproduction by photography or engraving made solely for the purpose of documentation of artistic criticism. **Article 199 - Use of counterfeit or usurped work** 1 - Anyone who sells, offers for sale, imports, exports or otherwise distributes to the public counterfeited or usurped works, or unauthorized copies of phonograms or videograms, whether the copies have been produced in the country or abroad, shall be punished with the penalties under Article 197. 2 - Negligence is punishable by a fine of up to 50 days. **Article 218 - Penal protection** 1 - Whoever, not being authorized to neutralize any effective measure of a technological nature, so knowing or having reasonable grounds to know, is punishable with imprisonment up to 1 year or a fine of up to 100 days. 2 - The attempt is punishable by a fine of up to 25 days. **Article 224 - Penal protection** 1 - Whoever, not being authorized, intentionally, knowingly or having reasonable grounds to know, practice one of the following acts: a) The removal or change of any information for the electronic management of rights; b) Distribution, import for distribution, broadcasting, communication or making available to the public works, performances or productions protected, which has been removed or altered without authorization or information for the electronic management of rights, knowing that at any of the situations listed is inducing, enabling, facilitating or concealing an infringement of intellectual property rights; is punishable with imprisonment up to 1 year or a fine of up to 100 days. 2 - The attempt is punishable by a fine of up to 25 days.
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.	General provisions on Articles 22, 23 from Penal Code, concerning abetting. The same, on Article 27 to aiding. **PORTUGUESE PENAL CODE (Decree-Law nr 400/82, from 23 September 1982, amended by Law nr 59/2007, from 4 September 2007.** **Article 22 – Attempt** 1 - There is attempt when the agent acts pretending to practice acts of execution of a crime that is not consummate. 2 - There are acts of execution: a) those that fulfill one element of a type of crime; b) those that are able to produce the typical result, or c) those that, according to common experience, and unless unforeseen circumstances are such as to expect them to follow acts of the species listed in the preceding paragraphs. **Article 23 - Punishment of attempts** 1 - Unless otherwise stated, the attempt is only punishable if the crime is punished with more than three years in prison. 2 - The attempt is punishable by a penalty for the consummated crime, especially reduced. 3 - The attempt is not punishable when it is obvious that the means employed are not able to commit the crime by the agent or when it does not exist the essential object of the consummation of the crime. **Article 27 - Abetting** 1 – It is punishable as an accomplice who, intentionally and by any way gives material or moral help to practice by other of an intentional fact. 2 - It is applicable to the accomplice the same penalty described to the author, especially reduced.
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;	Cybercrime Law - Law nr 109/2009 (15th of September) - Article 9 **Article 9 - Criminal liability of legal persons and other legal entities** Legal persons and other legal entities are legally responsible for the crimes described under this law in the same terms and limitations of the system of liability described in the Penal Code.

b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
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.	Not specifically transposed by any specific legislation, but already included in other rules.
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;	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 11 **Article 11 - Scope of procedural provisions** 1 - Except as provided in Articles 18 and 19, the procedural provisions of this chapter shall apply to proceedings relating to crimes: a) described under this Law; b) committed by means of a computer system, or c) when it is necessary to collect evidence in electronic form. 2 - The procedural provisions of this Chapter shall not affect the rules of Law No. 32/2008 of 17 July.

b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
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	Not specifically transposed by any specific legislation, but already included in other rules.

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.	
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.	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 12. **Article 12 - Expedited preservation of data** 1 – If, during the proceedings, when gathering evidence in order to ascertain the truth, it is required to obtain specified computer data stored on a computer system, including traffic data, which might be lost, changed or no longer available, the competent judicial authority orders the person who has the control or availability of such data, including the service provider, to preserve the data in question. 2 - The preservation can also be ordered by the criminal police force, authorized by the judicial authority or even not in emergency or danger in delay but, in this case, notice must be given immediately to the judicial authority, by the report described under Article 253 of the Code of Criminal Procedure. 3 - A preservation order describes, under penalty of nullity: a) the nature of the data; b) the origin and destination, if known, and c) the period of time covered by the preservation order, up to three months. 4 - In compliance with the preservation order addressed to it, whoever has availability or control over such data, including the service provider, preserves immediately the data concerned, protecting and maintaining their integrity for the appointed period of time, in view to allow the competent judicial authority to effectively obtain that information, and remains obliged to ensure the confidentiality of the implementation of these procedures. 5 - The competent judicial authority may order the renewal of the measure for periods of time according to the limit specified in c) of paragraph 3, providing all the requirements, up to a maximum of one year.
Article 17 – Expedited preservation and partial disclosure of traffic data	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 13

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Article 13 - Expedited disclosure of traffic data** In order to ensure the preservation of traffic data from a particular communication, regardless of the number of service providers participating in it, the service provider to whom the preservation has been ordered under the preceding article, discloses to the judicial authority or criminal police force, once known, other service providers through which this communication was carried out in order to identify all service providers used by that communication.
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.	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 14 **Article 14 - Injunction for providing data or granting access to data** 1 - If during the proceedings it becomes necessary for the gathering of evidence in order to ascertain the truth, obtain certain and specific data stored in a given system, the judicial authority orders to the person who has the control or availability of those data to communicate these data or to allow the access to them, under penalty of punishment for disobedience. 2 - The order referred to in the preceding paragraph identifies the data in question. 3 - In compliance with the order described in paragraphs 1 and 2, whoever has the control or availability of such data transmits these data to the competent judicial authority or allows, under penalty of punishment for disobedience, the access to the computer system where they are stored. 4 - The provisions of this Article will apply to service providers, who may be ordered to report data on their customers or subscribers, which would include any information other than the traffic data or the content data, held by the service provider, in order to determine: a) the type of communication service used, the technical measures taken in this regard and the period of service; b) the identity, postal or geographic address and telephone number of the subscriber, and any other access number, the data for billing and payment available under a contract or service agreement, or c) any other information about the location of communication equipment,

	available under a contract or service agreement. 5 - The injunction contained in this article may not be directed to a suspect or a defendant in that case. 6 - The injunction described under this article is not applicable to obtain data from a computer system used within a legal profession, medical, banking, and journalists activities. 7 - The system of professional secrecy or official and State secrets under Article 182 of the Code of Criminal Procedure shall apply *mutatis mutandis*.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the	Cybercrime Law - Law nr 109/2009 (15th of September) – Articles 15, 16 e 17 **Article 15 - Search of computer data** 1 – When, during the proceedings, it becomes necessary for the gathering of evidence, in order to ascertain the truth, obtain certain and specific data stored in a given system, the judicial authority authorizes by order, or orders, a search in that computer system, and, where possible, leads the event. 2 - The order of the preceding paragraph has a maximum validity of 30 days, under penalty of nullity. 3 - The criminal police force may execute the search without prior judicial authority, when: a) it is voluntarily consented by the person who has the availability or control of such data, provided that the consent is given in any documented way; b) In cases of terrorism, violent or highly organized crime, when there is founded evidence of the imminence of a crime which poses a serious risk to life or health of any person. 4 - When the criminal police force searches a system under the preceding paragraph: a) in the case of b) the investigation is immediately informed to the competent judicial authority so as it can validate it, with the penalty of nullity; b) in any case, the report under Article 253 of the Code of Criminal Procedure must be fulfilled and forwarded to the competent judicial authority. 5 – When, during a of search, there are reasons to believe that the information sought is stored in another computer system or in a different part of the previous system, but these data are legally accessible from the initial system, the search can be extended by authorization of the competent authority in accordance with

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.	paragraphs 1 and 2. 6 – It will be applied to the searches referred to in this Article, *mutatis mutandis*, the rules for searches of the Code of Criminal Procedure and the Statute of the Journalist. **Article 16 - Seizure of computer data** 1 - When, during a computer search or other legitimate access to a computer system, it is found computer data or computer documents that are necessary to gather, as evidence, in order to ascertain the truth, the competent judicial authority authorizes or orders their seizure. 2 - The criminal police force can seize computer data without prior judicial authority in the course of a search lawfully enforced under the previous article, as well as in emergency or when there is danger in delay. 3 – In case of seizure of computer data or computer documents which content is likely to disclose personal or intimate information, that would jeopardize the privacy of its owner or a third party, under penalty of nullity, the data or documents shall be submitted to the judge, who will consider its seizure regarding the concrete interests of the case. 4 - The seizures made by the criminal police force are always subject to validation by the judicial authority within 72 hours. 5 - Seizures related to computer systems used for the practice of legal professions, medical, banking and journalistic activities are subject, *mutatis mutandis*, the rules and procedures of the Code of Criminal Procedure and the Statute of the Journalist. 6 - The system of secrecy or official and state Secrets under Article 182 of the Code of Criminal Procedure shall apply *mutatis mutandis*. 7 - The seizure of computer data, whichever is most appropriate and proportionate, taking into account the interests of the case, may in particular take the following forms: a) seizure of the media where the system is installed or seizure of the media where the computer data are stores, and the necessary devices for their reading; b) production of a copy of the data on an autonomous media; c) preservation, by technological means, of the integrity of the data, without performing a copy or removing them, or d) removing in a non-reversing way or blocking the access to the data. 8 - In the case of seizure under b) above, the copy is made in duplicate, being one of the copies sealed and entrusted to the Clerk of Services where the

	investigation runs its terms and, if technically possible, the data entered are certified by digital signature. **Article 17 - Seizure of email communications and records of communications of similar nature** If during a search or other legitimate access to a computer system, e-mails or records of communications of a similar nature are found, stored in this system or in another system where it is legitimately allowed the access from the first, the judge may authorize or order, the seize of those records who appear to have a great interest to establish the truth, applying the corresponding rules of the seizure of mail of the Code of Criminal.
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.	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 18 **Article 18 - Interception of communications** 1 - It is allowed to intercept communications in proceedings relating to crimes: a) described under this Act, or b) committed by the means of a computer system or, when it is necessary to gather evidence in electronic form if such crimes are described in Article 187 of the Code of Criminal Procedure. 2 - The interception and recording of transmissions of computer data can only be allowed during the investigation, by founded decision of the judge or by request of the Prosecution Service, if there are reasons to believe that this is essential to establish the truth or that gathering the evidence would otherwise be impossible or very difficult to obtain by other means. 3 - The interception may be intended for data on the content of communications or only to collect and recording traffic data; the judicial order referred above must specify the scope of the interception, according to the specific needs of the investigation. 4 – Respecting all the aspects not described under this article, the interception and recording of transmissions of computer data are subject to the general regulation on interception and recording conversations or telephone conversations contained in Articles 187, 188 and 190 of the Code of Criminal Procedure.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 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.	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 18 **Article 18 - Interception of communications** 1 - It is allowed to intercept communications in proceedings relating to crimes: a) described under this Act, or b) committed by the means of a computer system or, when it is necessary to gather evidence in electronic form if such crimes are described in Article 187 of the Code of Criminal Procedure. 2 - The interception and recording of transmissions of computer data can only be allowed during the investigation, by founded decision of the judge or by request of the Prosecution Service, if there are reasons to believe that this is essential to establish the truth or that gathering the evidence would otherwise be impossible or very difficult to obtain by other means. 3 - The interception may be intended for data on the content of communications or only to collect and recording traffic data; the judicial order referred above must specify the scope of the interception, according to the specific needs of the investigation. 4 – Respecting all the aspects not described under this article, the interception and recording of transmissions of computer data are subject to the general regulation on interception and recording conversations or telephone conversations contained in Articles 187, 188 and 190 of the Code of Criminal Procedure.

Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 27. Besides, general rules from Penal Code – Articles 4, 5, 6 and 7. **Cybercrime Law** **Article 27 - Territorial jurisdiction of Portuguese criminal law and of Portuguese courts** 1 - For the purposes of this Act, in addition to the provisions of the Penal Code regarding jurisdiction of Portuguese criminal law, unless any contrary disposition from a treaty or international agreement, the Portuguese criminal law is still applicable to the facts: a) committed by Portuguese nationals, if it is not applicable to the case the criminal law of any other State; b) committed to the benefit of legal persons established in Portuguese territory; c) physically committed within Portuguese territory, though they aimed to reach computer systems located outside that territory, or d) that aimed computer systems located within Portuguese territory, regardless of where those facts were physically committed. 2 - If, due to the applicability of Portuguese criminal law, it is established simultaneous jurisdiction by the courts of Portugal and the courts of any other Member State of the European Union, being legally admissible in both of them to prosecute the same facts, the competent judicial authority requests to the bodies and mechanisms established within the European Union to facilitate cooperation between judicial authorities of the Member States to coordinate their actions in order to decide which of the two States introduces or continues the prosecution regarding the agents of the offense in order to concentrate it in one of them. 3 - The decision of acceptance or transmission of the procedure is taken by the competent judicial authority, taking into account successively the following: a) the location where the crime occurred; b) the nationality of the perpetrator, and c) the location where the perpetrator was found. 4 – It will be applied to the crimes under this Act the general rules of jurisdiction

	of the Code of Criminal Procedure. 5 - In case of doubt regarding jurisdiction, including because the physical location where the agent acted and the place where the target computer system is physically installed, jurisdiction is established according the tribunal that has been the first to know about the facts. **PORTUGUESE PENAL CODE (Decree-Law nr 400/82, from 23 September 1982, amended by Law nr 59/2007, from 4 September 2007.** **Article 4 - Application in space - general principle** Unless international treaty or convention in the contrary, the Portuguese criminal law shall apply to acts committed: a) In Portuguese territory, whatever the nationality of the agent or b) on board Portuguese ships or aircrafts. **Article 5 - Acts committed outside Portuguese territory** 1 - Unless international treaty or convention in the contrary, the Portuguese criminal law is also applicable to acts committed outside national territory: a) When they constitute crimes under Articles 221 º, 262º to 271º, 308º to 321º and Article 325º to 345; b) Against a Portuguese citizen, a Portuguese citizen who usually lives in Portugal at the time of their practice and is found here; c) When they constitute crimes under Articles 159º to 161º, 171º, 172º, 175º, 176º and 278º to 280º, provided that the agent is found in Portugal and can not be extradited or surrendered as a result of implementing the European arrest warrant or another instrument of international cooperation that binds the Portuguese State; d) When they constitute crimes under Articles 144º, 163º and 164º, being the victim a child, provided that the agent is found in Portugal and can not be extradited or surrendered as a result of implementing the European Arrest Warrant or other instrument of international cooperation that binds the Portuguese State; e) By a Portuguese citizen, or by foreigners against a Portuguese citizen, where: i) agents are found in Portugal; ii) they are also punishable under the law of the place where they were charged, except where that place does not exercise punitive power, and

	iii) if they constitutes an extraditable crime and this can not be granted or decided or if the agent cannot be delivered in executing the European arrest warrant or other instrument of international cooperation that binds the Portuguese State; f) For foreigners who are found in Portugal and whose extradition was requested there, when they constitute crimes which allow the extradition and this can not be granted or decided not to deliver the agent in executing the European arrest warrant or other instrument of cooperation international binding the Portuguese State; g) A corporate body or against a legal person having its headquarters in Portuguese territory. 2 - The Portuguese criminal law is also applicable to acts committed outside national territory if the Portuguese State is obliged to trial them by any treaty or international agreement. **Article 6 - Restrictions on the application of Portuguese law** 1 - The application of Portuguese law to acts committed outside national territory only takes place if the agent was not submitted to a trial in the country where the infringement was committed or if he subtracted from the total or partial fulfillment of the sentence. 2 - Although it is applicable the Portuguese law, under the terms of the preceding paragraph, the trial will follow the law of the country where the crime has been committed whenever it is actually more favorable to the agent. The penalty is cast in what will be at the Portuguese system or, if there is no direct correspondence, in what the Portuguese law provides for this. 3 - The regime of the preceding paragraph shall not apply to crimes defined in a) and b) of paragraph 1 of the preceding article. **Article 7 - Place of practice of the fact** 1 – It is considered that the fact is practiced both in the place where, in whole or in part, the agent has acted, or in the case of omission, should have acted as on that where the typical result or outcome not included in the type of crime it produced. 2 – In the case of attempt, it is considered that the fact is also practiced in the place where, according to the representation of the agent, the result should have been produced.

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	Not specifically transposed by any specific legislation, but already included in other rules.

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 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	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 20 **Article 20 - International cooperation**

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. 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.	The national authorities shall cooperate with the competent foreign authorities for the purpose of criminal investigations or proceedings relating computer systems or data, as well as the collection of evidence of a crime in electronic form, according to the rules on transfer of personal data contained in Law No 67/98 of 26 October.
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	Not specifically covered by any specific legislation in force, but allowed by general rules.

investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a	Not covered by any specific legislation in force.

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 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. 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.	Not specifically transposed by any specific legislation, but already included in other rules.
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:	Cybercrime Law - Law nr 109/2009 (15th of September) – Articles 22 and 23 **Article 22 - Preservation and expedited disclosure of computer data within international cooperation** 1 – Portugal may be requested to expedite preservation of data stored in a computer system located in the country, referring to crimes described under Article 11, in view to submit a request for assistance for search, seizure and disclosure of those data. 2 - The request specifies: a) the authority requesting the preservation;

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: 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	b) that the offense is being investigated or prosecuted, as well as a brief statement of the facts relating thereto; c) the computer data to be retained and its relation to the offense; d) all the available information to identify the person responsible for the data or the location of the computer system; e) the necessity of the measure of preservation, and f) The intention to submit a request for assistance for search, seizure and disclosure of the data. 3 – Executing the demand of a foreign authority under the preceding paragraphs, the competent judicial authority orders the person who has the control or availability of such data, including a service provider, to preserve them. 4 - Preservation can also be ordered by *Polícia Judiciária*, after authorization obtained from the competent judicial authority or when there is emergency or danger in delay; in this case it is applicable, paragraph 4 of the preceding article. 5 - A preservation order specifies, on penalty of nullity: a) the nature of the data; b) if known, the source and their destination, and c) the period of time during which that data must be preserved for up to three months. 6 - In compliance with the addressed preservation order, who has the control or availability of such data, including a service provider, preserves immediately the data by the specified period of time, protecting and maintaining its integrity. 7 - The competent judicial authority, or *Policia Judiciária* with permission of the judicial authority, may order the renewal of the measure for periods subject to the limit specified in item c) of paragraph 5, provided they meet the respective requirements of admissibility, to the maximum a year. 8 - When the request referred to in paragraph 1 is received, the competent judicial authority decides the preservation of data until the adoption of a final decision on the request. 9 - Data preserved under this Article may only be provided: a) to the competent judicial authority, in the execution of the application for cooperation referred to in paragraph 1, in the same way that it could have been done in a similar national case, under Articles 13 to 17; b) to the national authority which issued the order to preserve, in the same way that it could have been done, in a similar national case under Article 13. 10 - The national authority that, under the preceding paragraph, receives traffic data identifying intermediate service providers by which the communication was

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.	made, quickly communicates this fact to the requesting authority in order to enable this authority to submit to the competent authority another request for expedited preservation of data. 11 – The provisions of paragraphs 1 and 2 shall apply, *mutatis mutandis*, to requests sent to other authorities by the Portuguese authorities. **Article 23 - Grounds for refusal** 1 - A request for expedited preservation or disclosure of computer data is refused if: a) the computer data in question refer to a political offense or a related offense according to Portuguese law; b) it attempts against the sovereignty, security, *ordre publique* or other constitutionally defined interests of the Portuguese Republic; c) the requesting State does not provide guarantees for the protection of personal data. 2 - A request for expedited preservation of computer data can still be refused if there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such data shall be denied for lack of verification of dual criminality.
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	Cybercrime Law - Law nr 109/2009 (15th of September) – Articles 22 and 23 **Article 22 - Preservation and expedited disclosure of computer data within international cooperation** 1 – Portugal may be requested to expedite preservation of data stored in a computer system located in the country, referring to crimes described under Article 11, in view to submit a request for assistance for search, seizure and disclosure of those data. 2 - The request specifies: a) the authority requesting the preservation; b) that the offense is being investigated or prosecuted, as well as a brief statement of the facts relating thereto; c) the computer data to be retained and its relation to the offense; d) all the available information to identify the person responsible for the data or the location of the computer system;

	e) the necessity of the measure of preservation, and f) The intention to submit a request for assistance for search, seizure and disclosure of the data. 3 – Executing the demand of a foreign authority under the preceding paragraphs, the competent judicial authority orders the person who has the control or availability of such data, including a service provider, to preserve them. 4 - Preservation can also be ordered by *Polícia Judiciária*, after authorization obtained from the competent judicial authority or when there is emergency or danger in delay; in this case it is applicable, paragraph 4 of the preceding article. 5 - A preservation order specifies, on penalty of nullity: a) the nature of the data; b) if known, the source and their destination, and c) the period of time during which that data must be preserved for up to three months. 6 - In compliance with the addressed preservation order, who has the control or availability of such data, including a service provider, preserves immediately the data by the specified period of time, protecting and maintaining its integrity. 7 - The competent judicial authority, or *Policia Judiciária* with permission of the judicial authority, may order the renewal of the measure for periods subject to the limit specified in item c) of paragraph 5, provided they meet the respective requirements of admissibility, to the maximum a year. 8 - When the request referred to in paragraph 1 is received, the competent judicial authority decides the preservation of data until the adoption of a final decision on the request. 9 - Data preserved under this Article may only be provided: a) to the competent judicial authority, in the execution of the application for cooperation referred to in paragraph 1, in the same way that it could have been done in a similar national case, under Articles 13 to 17; b) to the national authority which issued the order to preserve, in the same way that it could have been done, in a similar national case under Article 13. 10 - The national authority that, under the preceding paragraph, receives traffic data identifying intermediate service providers by which the communication was made, quickly communicates this fact to the requesting authority in order to enable this authority to submit to the competent authority another request for expedited preservation of data. 11 – The provisions of paragraphs 1 and 2 shall apply, *mutatis mutandis*, to requests sent to other authorities by the Portuguese authorities.

	Article 23 - Grounds for refusal 1 - A request for expedited preservation or disclosure of computer data is refused if: a) the computer data in question refer to a political offense or a related offense according to Portuguese law; b) it attempts against the sovereignty, security, *ordre publique* or other constitutionally defined interests of the Portuguese Republic; c) the requesting State does not provide guarantees for the protection of personal data. 2 - A request for expedited preservation of computer data can still be refused if there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such data shall be denied for lack of verification of dual criminality.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 24 **Article 24 - Access to computer data within international cooperation** 1 – In the execution of the request of the foreign authority, the competent judicial authority may proceed with the search, seizure and disclosure of data stored in the computer system located in Portugal, related to crimes defined in Article 11, when the search and seizure would be admissible in a similar national case. 2 - The judicial authority shall proceed as quickly as possible when there is reason to believe that the computer data in question are particularly vulnerable to loss or modification, or where cooperation is provided for an expedited instrument of cooperation described in any international legal instrument. 3 - The provisions of paragraph 1 shall apply, *mutatis mutandis*, to requests made by Portuguese judicial authorities.
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	Cybercrime Law - Law nr 109/2009 (15th of September) – Articles 25 **Article 25 - Cross-border access to computer data stored when publicly available or with consent** The competent foreign authorities without prior request from the Portuguese authorities, in accordance with the rules on transfer of personal data provided by Law No. 67/98 of 26 October, may: a) access data stored in a computer system located in Portugal, where publicly

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.	available; b) receive or access through a computer system located in its territory, the data stored in Portugal, through legal and voluntary consent of the person legally authorized to disclose them.
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.	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 26 **Article 26 - Interception of communications within international cooperation** 1 - Pursuant to a request by the competent foreign authority it may be authorized by the judge the interception of computer data transmissions from a computer system located in Portugal, since it is stipulated by a treaty or an international agreement and whether it is a case where such interception is allowed under Article 18, in a similar national case. 2 – *Policia Judiciária* is the responsible entity for receiving requests to intercept communications, which report to the Public Prosecution Service, so as they can be presented to the judge in charge of the *comarca* of Lisbon for authorization. 3 - The referred order of authorization also allows the immediate transmission of the communication to the requesting State, if such a procedure is foreseen in a treaty or an international agreement under which the request is made. 4 - The provisions of paragraph 1 shall apply, *mutatis mutandis*, to requests made by Portuguese judicial authorities.
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.	Cybercrime Law - Law nr 109/2009 (15th of September) – Article 26 **Article 26 - Interception of communications within international cooperation** 1 - Pursuant to a request by the competent foreign authority it may be authorized by the judge the interception of computer data transmissions from a computer system located in Portugal, since it is stipulated by a treaty or an international agreement and whether it is a case where such interception is allowed under Article 18, in a similar national case. 2 – *Policia Judiciária* is the responsible entity for receiving requests to intercept communications, which report to the Public Prosecution Service, so as they can be presented to the judge in charge of the *comarca* of Lisbon for authorization. 3 - The referred order of authorization also allows the immediate transmission of the communication to the requesting State, if such a procedure is foreseen in a treaty or an international agreement under which the request is made.

	4 - The provisions of paragraph 1 shall apply, *mutatis mutandis*, to requests made by Portuguese judicial authorities.
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.	Cybercrime Law - Law nr 109/2009 (15th of September) – Articles 21 and 29 **Article 21 - Permanent contact point for international cooperation** 1 - For purposes of international cooperation, in order to provide immediate assistance for the purposes of the preceding Article, *Polícia Judiciária* must maintain a structure that guarantees a point of contact available at all times, twenty-four hours a day, seven days a week. 2 – This contact point can be contacted by other contact points in accordance with agreements, treaties or conventions to which Portugal is bound, or in pursuance of protocols of cooperation with international judicial or law enforcement agencies. 3 - The immediate assistance provided by the permanent contact point includes: a) technical advice to other points of contact; b) expeditious preservation of data in cases of urgency or danger in delay, in accordance with the following article; c) collection of evidence for which has the legal jurisdiction in cases of urgency or danger in delay; d) detection of suspects and providing of legal information in cases of urgency or danger in delay; e) the immediate transmission to the Public Prosecution Service of requests concerning the measures referred to in b) and d) in the case there are excluded of the jurisdiction of *Polícia Judiciária*, with a view to its expedited implementation. 4 - When acting under b) to d) above, *Polícia Judiciária* immediately notifies the Public Prosecution Service by the means of the report described under Article 253 of the Code of Criminal Procedure. **Article 29 - Competence of *Polícia Judiciária* for international cooperation** The competence conferred by this Act to *Polícia Judiciária* for the purpose of international cooperation is carried out by the unit who is committed to the investigation of crimes under this Law.
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	**Declaration transmitted by a letter from the Permanent Representative of Portugal, dated 30 April 2010, registered at the Secretariat General on 4 May 2010 - Or. Engl.** In accordance with Article 24, paragraph 7a, of the Convention, Portugal declares

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.	that in those cases in which the Convention on Extradition or other bilateral or multilateral instruments on extradition are not applicable, the authority responsible for making or receiving requests for extradition or provisional arrest is the *Procuradoria-Geral da República* (Rua da Escola Politécnica, 140 - 1269-269 Lisboa, Portugal). **Period covered: 1/7/2010 -** The preceding statement concerns Article(s) : 24 **Declaration transmitted by a letter from the Permanent Representative of Portugal, dated 30 April 2010, registered at the Secretariat General on 4 May 2010 - Or. Engl.** In accordance with Article 27, paragraph 2c, of the Convention, Portugal declares that, in the absence of applicable international agreements, the authority responsible for sending and answering requests for mutual legal assistance is the *Procuradoria-Geral da República* (Rua da Escola Politécnica, 140 - 1269-269 Lisboa, Portugal). **Period covered: 1/7/2010 -** The preceding statement concerns Article(s) : 27 **Declaration contained in the instrument of ratification deposited on 24 March 2010 - Or. Engl.** In accordance with Article 24, paragraph 5, of the Convention, the Portuguese Republic declares that it shall not grant extradition of persons who: a) are to be trialled by an exceptional court or who are to serve a sentence passed by such a court; b) it has been proved will be subject to a trial which affords no legal guarantees of criminal proceedings complying with the conditions internationally recognised as essential to the protection of human rights, or will serve their sentences in inhuman conditions; c) are being demanded in connection with an offence punishable with a lifetime sentence or a lifetime detention order. The Portuguese Republic shall grant extradition only for crimes punishable with penalty of deprivation of liberty superior to one year. The Portuguese Republic shall not grant extradition of Portuguese nationals.

	Portugal shall not grant extradition for offences punishable with the death penalty under the law of the requesting State. Portugal shall authorise transit through its national territory only in respect of persons whose circumstances are such that their extradition may be granted. **Period covered: 1/7/2010 -** The preceding statement concerns Article(s) : 24 **Declaration transmitted by a letter from the Permanent Representative of Portugal, dated 30 April 2010, registered at the Secretariat General on 4 May 2010 - Or. Engl.** In accordance with Article 35, paragraph 1, of the Convention, Portugal designates as point of contact for the network 24/7 the *Policia Judiciária* (Rua Gomes Freire, 174 - 1169-007 Lisboa, Portugal; telephone (+351) 218 641 000, fax (+351) 213 304 260). **Period covered: 1/7/2010 -** The preceding statement concerns Article(s) : 35