Assembleia da República (Assembly of the Republic)

Law no. 109/2009, of 15 September

Approves the Cybercrime Law, transposing to the national legal order Council Framework Decision 2005/222/JHA, of 24 February, on attacks against information systems, and adapts to national law the Convention on Cybercrime of the Council of Europe.

Pursuant to article 161 c) of the Constitution, the Assembly of the Republic hereby decrees as follows:

CHAPTER I
Subject-matter and definitions

Article 1
Subject-matter

This law lays down the substantive and procedural criminal provisions, as well as provisions on international cooperation on criminal matters, concerning cybercrime and collection of electronic evidence, transposing to the national legal order Council Framework Decision 2005/222/JHA, of 24 February, on attacks against information systems, and adapting to national law the Convention on Cybercrime of the Council of Europe.

Article 2
Definitions

For the purposes hereof, the following definitions shall apply:

a) "Computer system" shall mean any device or group of inter-connected or related devices, one or more of which, pursuant to a programme, performs automatic processing of computer data, as well as the network supporting the communication between them and computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

b) "Computer data" shall mean any representation of facts, information or concepts in a form suitable for processing in a computer system, including programmes suitable for causing a computer system to perform a function;

c) "Traffic data" shall mean 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;

d) "Service provider" shall mean any public or private entity that provides to users of its service the ability to communicate by means of a computer system, as well as any other entity that processes or stores computer data on behalf of such communication service or users of such service;

e) "Interception" shall mean the act intended to capture information in a computer system by means of an electro-magnetic, acoustic, mechanical or other device;

f) "Topography" shall mean a series of related images, however fixed or encoded, representing the three-dimensional pattern of the layers of which a semiconductor product is composed, in which series, each image has the pattern or part of the pattern of a surface of the semiconductor product at any stage of its manufacture;

g) "Semiconductor product" shall mean the final or an intermediate form of any product, consisting of a body of material which includes a layer of semiconducting material and having one or more other layers composed of conducting, insulating or semiconducting material, the layers being arranged in accordance with a three-dimensional pattern and intended to perform, exclusively or together with other functions, an electronic function.

CHAPTER II
Substantive criminal provisions

Article 3
Computer-related forgery

1 - Whoever, with the purpose of deceiving legal relationships, inputs, alters, erases or suppresses computer data, or commits any other form of interference with the automatic processing of data resulting in inauthentic data or documents, with the intent that it be considered or acted upon for legal purposes as if it were authentic, shall be punishable by a term of imprisonment up to 5 years or by fine between 120 and 600 days.

2 - Where actions described in the preceding paragraph concern data registered or incorporated in a payment bank card or in any other device enabling access to a payment system or means, communications system or conditional access service, offenders shall be punishable by a term of imprisonment between 1 and 5 years.

3 - Whoever, with the purpose of causing damage to another person or of procuring an illegitimate benefit for oneself or for another person, uses documents produced from computer data subject to acts referred in paragraph 1 or any device wherein data subject to acts referred in paragraph 2 are registered or incorporated, shall be punishable by penalties provided respectively in one paragraph or another, as appropriate.

4 - Whoever imports, distributes, sells or holds for commercial purposes any device enabling access to a payment system or means, communications system or conditional access service, which has been subject to any of the acts referred in paragraph 2, shall be punishable by a term of imprisonment between 1 and 5 years.

5 - Where facts referred to in the preceding paragraphs have been committed by staff in the performance of their duties, offenders shall be punishable by a term of imprisonment between 2 and 5 years.

Article 4
Damage caused to programmes or other computer data

1 - Whoever, without legal permission or authorization from the owner or holder of the right over the full system, or part thereof, deletes, alters, fully or partially deteriorates, damages, suppresses or renders unusable or inaccessible other people's programmes or other computer data or by any other means seriously hinders their functioning, shall be punishable by a term of imprisonment up to 3 years or by fine.

2 - The attempt to commit the established offences shall be punishable.

3 - The penalty provided for in paragraph 1 shall also apply to whoever illegally produces, sells, distributes or otherwise disseminates or introduces in computer systems devices, programmes, or other computer data designed to produce any of the non-authorized actions described in that paragraph.

4 - Where high-value damage is caused, offenders shall be punishable by term of imprisonment up to 5 years or by fine up to 600 days.

5 - Where considerable high-value damage is caused, offenders shall be punishable by term of imprisonment between 1 and 10 years.

6 - In the situations provided for in paragraphs 1, 2 and 4, criminal proceedings shall be initiated on complaint.

Article 5
Computer-related fraud

1 - Whoever, without legal permission or authorization from the owner or holder of the right over the full system, or part thereof, hinders, prevents, interrupts or seriously disrupts the functioning of a computer system by inputting, transmitting, deteriorating, damaging, altering, deleting, preventing access or suppressing programmes or other computer data or by any other means interferes in a computer system, shall be punishable by a term of imprisonment up to 5 years or by fine up to 600 days.

2 - The penalty provided for in paragraph 1 shall also apply to whoever illegally produces, sells, distributes or otherwise disseminates or introduces in computer systems devices, programmes, or other computer data designed to produce any of the non-authorized actions described in the preceding paragraph.

3 – The attempt to commit offences established in the preceding paragraph shall not be punishable.

4 - Where high-value damage is caused by the disruption, offenders shall be punishable by a term of imprisonment between 1 to 5 years.

5 - Offenders shall be punishable by a term of imprisonment between 1 to 10 years where:

a) Considerable high-value damage is caused by the disruption;

b) The disruption produced affects seriously or on a long-term basis a computer system supporting an activity with critical social functions, namely supply chains, health, safety and economic well-being of people, or the proper operation of public services.

Article 6
Illegal access

1 - Whoever, without legal permission or authorization from the owner or holder of the right over the full system, or part thereof, accesses a computer system, shall be punishable by a term of imprisonment up to 1 year or by fine up to 120 days.

2 - The penalty provided for in paragraph 1 shall also apply to whoever illegally produces, sells, distributes or otherwise disseminates or introduces in computer systems devices, programmes, or a set of executable instructions, a code or other computer data designed to produce any of the non-authorized actions described in the preceding paragraph.

3 - Offenders shall be punishable by a term of imprisonment up to 3 years or by fine where access is achieved through violation of security rules.

4 - Offenders shall be punishable by a term of imprisonment between 1 to 5 years where:

a) The access enables the agent to be aware of legally-protected commercial or industrial secret information or confidential data; or

b) Considerable high-value benefits or monetary advantages are achieved.

5 - The attempt to commit the established offences shall be punishable, except for cases provided for in paragraph 2.

6 - In the situations provided for in paragraphs 1, 3 and 5, criminal proceedings shall be initiated on complaint.

Article 7
Illegal interception

1 - Whoever, without legal permission or authorization from the owner or holder of the right over the full system, or part thereof, intercepts by technical means transmissions of computer data to, from or within a computer system, shall be punishable by a term of imprisonment up to 3 year or by fine.

2 - The attempt to commit the established offences shall be punishable.

3 - The penalty provided for in paragraph 1 shall also apply to whoever illegally produces, sells, distributes or otherwise disseminates or introduces in computer systems devices, programmes, or other computer data designed to produce any of the non-authorized actions described in that paragraph.

Article 8
Illegal reproduction of protected programmes

1 - Whoever illegally publicly reproduces, discloses or communicates a legally-protected computer programme, shall be punishable by a term of imprisonment up to 3 years or by fine.

2 - The penalty provided for in paragraph 1 shall also apply to whoever reproduces the topography of a semiconductor product or commercially operates or imports, for such purposes, topographies or semiconductor products manufactured on the basis of those topographies.

3 - The attempt to commit the established offences shall be punishable.

Article 9
Corporate liability

Legal persons and related entities shall be held liable for criminal offences established in accordance with this law, under the terms and limits of the liability regime provided for in the Criminal Code.

Article 10
Forfeit of goods

1 - The court may order the forfeit to the State of objects, materials, equipment or devices used to commit criminal offences provided for herein which are owned by the convicted person.

2 - Decree-Law number 11/2007, of 19 January, shall apply to the evaluation, use, sale and reimbursement of goods seized by police authorities which are likely to be forfeited to the State.

CHAPTER III
Procedural provisions

Article 11
Scope of application of procedural provisions

1 - Except as specifically provided for otherwise in articles 18 and 19, the procedural provisions provided for in this chapter apply to proceedings on criminal offences:

a) Provided for herein;

b) Committed by means of a computer system; or

c) Relatively to which the collection of electronic evidence is required.

2 - Procedural provisions provided for in this chapter shall be without prejudice to the regime laid down in Law number 32/2008, of 17 July.

Article 12
Expedited preservation of data

1 - Where, in the course of proceedings, the collection of evidence, necessary to uncover the truth, requires that specified computer data, including traffic data, that has been stored by means of a computer system, are obtained, in particular where there are grounds to believe that the computer data are particularly vulnerable to loss, modification or unavailability, the competent judicial authority shall order whoever holds or controls such data, namely the service provider, to preserve the data under consideration.

2 - Preservation may also be ordered by criminal police bodies, authorized by the competent judicial authority, or where there is urgency or danger in delay; in this last situation, the former must promptly warn the judicial authority, submitting the report provided for in article 253 of the Procedural Criminal Code.

3 - Under pain of being deemed null and void, the preservation order must indicate:

a) The nature of data;

b) Their origin and destination, if known; and

c) The period of time over which data must be preserved, up to three months.

4 - In compliance with the preservation order, whoever holds or controls such data, namely the service provider, shall promptly preserve the data under consideration, protecting and maintaining its integrity for the established period of time, to enable the competent judicial authority to obtain it, being subject to ensure that the undertaking of such procedures is kept confidential.

5 - The competent judicial authority may order the renewal of the measure for periods subject to the limit provided for in paragraph 3 c), insofar as the respective conditions of admissibility are met, up to a maximum limit of one year.

Article 13
Expedited preservation of traffic data

In order to ensure the preservation of traffic data related to a specific communication, regardless of whether one or more service providers were involved in the transmission of that communication, the service provider which was ordered to perform such preservation pursuant to the preceding article shall indicate to the judicial authority or to criminal police bodies, as soon as this information is available to it, other service providers through which the communication was made, in order to identify the service providers and the path through which the communication was transmitted.

Article 14
Injuction to submit or provide access to data

1 - Where, in the course of proceedings, the collection of evidence, necessary to uncover the truth, requires that specified computer data, stored in a specific computer system, are obtained, the competent judicial authority shall order whoever holds or controls such data to

register such data in the proceedings file or to provide access thereto, on pain of punishment for disobedience.

2 - The order referred to in the preceding paragraph shall identify data under consideration.

3 - In compliance with the order described in paragraphs 1 and 2, whoever holds or controls data under consideration shall communicate them to the competent judicial authority or provide access to the computer system where such data are stored, on pain of punishment for disobedience.

4 – Provisions in this article apply to service providers, which may be ordered to register in the proceedings file data on customers or subscribers, including any information other than traffic or content data, contained in the form of computer data or any other form that is held by the service provider, 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; or

c) Any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

5 - The injuction provided for herein shall not be addressed to a suspect or defendant in those proceedings.

6 - The injuction provided for herein shall also not be used as regards computer systems used in legal, medical and bank practises, as well as by journalists.

7 - The regime governing professional, staff and State secret information, provided for in article 182 of the Criminal Procedure Code, shall apply hereto, duly adapted.

Article 15
Search of computer data

1 - Where, in the course of proceedings, the collection of evidence, necessary to uncover the truth, requires that specified computer data, stored in a specific computer system, are obtained, the competent judicial authority shall authorize or order the search to that computer system, overseeing such investigations whenever possible.

2 - The order provided for in the preceding paragraph shall be valid for a maximum period of 30 days, on pain of being deemed null and void.

3 - Criminal police bodies shall undertake the search, without a prior authorization from the judicial authority:

a) Where whoever holds or controls data under consideration voluntarily consents to the search, insofar as the consent is documented in any way;

b) In cases of terrorism, violent or highly-organized crimes, or where there is evidence to substantiate the imminent commission of a criminal offence threatening the life or integrity of any person.

4 - Where criminal police bodies undertake the search pursuant to the preceding paragraph:

a) In the situation provided for in point b), the investigation shall be promptly communicated to the competent judicial authority, and assessed by the latter as far as the validation of the measure is concerned, on pain of being deemed null and void;

b) In any other situation, the report provided for in article 253 of the Criminal Procedure Code shall be drawn up and submitted to the competent judicial authority.

5 - Where, in the course of the search, there are grounds to believe that the data sought is stored in another computer system or part of it, and such data is lawfully accessible from the initial system, the search may be extended to the other system, by means of an authorization or order from the competent authority, pursuant to paragraphs 1 and 2.

6 – To the search referred to herein shall apply, duly adapted, the rules on execution of searches provided for in the Criminal Procedure Code and in the Journalists Statute.

Article 16
Seizure of computer data

1 - Where, in the course of a computer system search, or of another legitimate means of access to a computer system, computer data or documents necessary to the collection of evidence, in order to uncover the truth, are found, the competent judicial authority shall authorize or order the seizure thereof.

2 - Criminal police bodies are entitled to perform seizures, without any prior authorization from the judicial authority, in the course a computer system search lawfully ordered and executed pursuant to the preceding article, or where there is urgency or danger in delay.

3 - In case of seizure of computer data or documents the contents of which may disclose personal or intimate data, thus hindering the privacy of the respective holder or of a third party, on pain of being deemed null and void such data or documents shall be submitted to the judge, who shall weight their attachment to the file, taking into account the interests of the case.

4 - Seizures carried out by criminal police bodies shall always be validated by the judicial authority, within at the most 72 hours.

5 - Seizures related to computer systems used for legal, medical and bank practises shall comply with the rules and formalities provided for in the Criminal Procedure Code, duly adapted, and those related to computer systems used by journalists shall comply with the rules and formalities provided for in the Journalists Statute, duly adapted.

6 - The regime governing professional, staff and State secret information, provided for in article 182 of the Criminal Procedure Code, shall apply, duly adapted.

7 - Seizure of computer data, depending on what is deemed to be most appropriate or proportional, taking into account the interests of the case, may take the following forms:

a) Seizing the computer system support equipment or the computer-data storage medium, as well as devices required to read data;

b) Making a copy of those computer data, in an autonomous means of support, which shall be attached to the file;

c) Maintaining by technological means the integrity of data, without copying or removing them; or

d) Removing the computer data or blocking access thereto.

8 - In the situation of seizure provided for in point b) of the preceding paragraph, copies shall be made in duplicate, one of them being sealed and entrusted to the court clerk of services where the case has been brought and, where technically possible, seized data shall be certified by means of a digital signature.

Article 17
Seizure of emails or similar communication records

Where, in the course of a computer system search, or of another legitimate means of access to a computer system, emails or similar communication records are found, stored in that computer system or in another system which can be lawfully accessed from the former, the competent judicial authority shall authorize or order the seizure of data deemed to be of major interest to uncover the truth or to collect evidence, applying as appropriate the regime of seizure of correspondence provided for in the Criminal Procedure Code.

Article 18
Interception of communications

1 – The interception of communications shall be permitted in proceedings on criminal offences:

a) Provided for herein; or

b) Committed by means of a computer system or which require the collection of electronic evidence, where such criminal offences are provided for in article 187 of the Criminal Procedure Code.

2 - Interception and record of transmission of computer data shall only be authorized during the investigation stage, where there are reasons to believe that this measure is essential to the uncovering of the truth or that, otherwise, it would be impossible or very difficult to obtain evidence, on the basis of a substantiated order from the examining judge, further to a request from the Public Prosecution.

3 - The interception may concern the record of data on the content of communications or aim only at the collection and record of traffic data, and the order referred to in the preceding

paragraph shall specify the respective scope, according to the specific needs of the investigation.

4 - With regard to all matters which are not contrary to this article, the regime of interception and recording of telephone conversations or communications laid down in articles 187, 188 and 190 of the Criminal Procedure Code shall apply to the interception and record of transmissions of computer data.

Article 19
Undercover operations

1 – Undercover operations governed by Law number 101/2001, of 25 August, shall be permitted in the manner specified therein, in the course of the investigation of criminal offences:

a) Provided for herein; or

b) Committed by means of a computer system, to which correspond, in abstract, a term of imprisonment with a maximum band of over 5 years or, even where lower penalty has been provided for, and as regards intentional offences, those against freedom and sexual self-determination, in case victims are minors or incapacitated adults, qualified swindling, computer-related and communication forgery, racial, religious or sexual discrimination, economic and financial infringements, as well as criminal offences laid down in title IV of the Code of Copyright and Related Rights.

2 - Rules on interception of communications shall apply, as appropriate, where the resort to computer means and devices is required.

CHAPTER IV
International cooperation

Article 20
Scope of international cooperation

Competent national authorities shall cooperate with competent foreign authorities for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence of a criminal offence, according to rules on transfer of personal data provided for in Law number 67/98, of 26 October.

Article 21
International cooperation permanent point of contact

1 - For international cooperation purposes, in order to ensure the provision of immediate assistance for the purposes referred to in the preceding article, the Polícia Judiciária (Judicial Police) shall guarantee the maintenance of a structure ensuring a point of contact available on a twenty-four hour, seven-day-a-week basis.

2 - This point of contact may be contacted by other points of contact, pursuant to agreements, treaties or conventions to which Portugal is bound, or in compliance with international cooperation protocols signed with judicial or police bodies.

3 - The immediate assistance provided by this permanent point of contact includes:

a) The provision of technical advice to other points of contact;

b) The expedite preservation of data in situations of urgency or danger in delay, in compliance with the following article;

c) The collection of evidence for which it is incumbent in situations of urgency or danger in delay;

d) The locating of suspects and provision of legal information, in situations of urgency or danger in delay;

e) The immediate transfer to the Public Prosecution of requests on measures referred to in points b) and d), in cases other than those referred to therein, so that they may be quickly executed;

4 - When acting under points b) and d) of the preceding paragraph, the Polícia Judiciária shall immediately notify the Public Prosecution Office, submitting thereto the report provided for in article 253 of the Criminal Procedure Code.

Article 22
Expedited preservation and disclosure of computer data in international cooperation

1 - Portugal may be requested to obtain the expeditious preservation of data stored by means of a computer system, located within Portuguese territory, for criminal offences provided for in article 11, and in respect of which the requesting Party intends to submit a request for mutual assistance for the search, seizure or disclosure of the data.

2 - A request for preservation shall specify:

a) The authority seeking the preservation;

b) The offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c) The computer data to be preserved and its relationship to the offence;

d) Any available information identifying the custodian of the computer data or the location of the computer system;

e) The necessity of the preservation; and

f) The intention to submit a request for mutual assistance for the search, seizure or disclosure of data.

3 - In order to execute the request from the competent foreign authority pursuant to the preceding paragraphs, the competent judicial authority shall order whoever holds or controls such data, namely the service provider, to preserve them.

4 - The preservation may also be ordered by the Polícia Judiciária, by means of an authorization from the competent judicial authority or where there is urgency or danger in delay, and in this case the provision in paragraph 4 of the preceding article shall apply.

5 - Under pain of being deemed null and void, the preservation order must indicate:

a) The nature of data;

b) Their origin and destination, if known; and

c) The period of time over which data must be preserved, up to three months.

6 - In compliance with the preservation order, whoever holds or controls such data, namely the service provider, shall promptly preserve the data under consideration for the specified period of time, protecting and maintaining their integrity.

7 - The competent judicial authority, or the Polícia Judiciária by mean of an authorization from the former, may order the renewal of the measure for periods subject to the limit provided for in paragraph 5 c), insofar as the respective conditions of admissibility are met, up to a maximum limit of one year.

8 - Upon receiving the request for assistance referred to in paragraph 1, the judicial authority with powers to decide on the matter shall determine the preservation of data until a final decision is taken on the request.

9 - Data preserved under this article shall only be provided:

a) To the competent judicial authority, to execute the request for assistance referred to in paragraph 1, as if a similar national situation were at stake, pursuant to articles 13 to 17;

b) To the national authority that issued the preservation order, as if a similar national situation were at stake, pursuant to article 13.

10 - The national authority which receives, pursuant to the preceding paragraph, a communication on traffic data to identify the service provider and the path through which the communication was transmitted, shall communicate them promptly to the requesting authority, to enable that authority to submit a new request for expedite preservation of computer data.

11 - Paragraphs 1 and 2 hereof apply, duly adapted, to requests made by Portuguese authorities.

Article 23
Grounds for refusal

1 - The request for expedite preservation or disclosure of computer data may be refused on the following grounds:

a) Computer data under consideration concern an offence which to Portuguese Law is deemed to be a political offence or an offence connected with a political offence;

b) The execution of the request is likely to prejudice the sovereignty, security, ordre public or other essential interests of the Portuguese Republic, defined as such in the Constitution;

c) The requesting State does not provide appropriate guarantees of protection of personal data.

2 - The request for expedite preservation of computer data may also be refused in cases where there are reasons to believe that the execution of the subsequent request for judicial assistance for purposes of search, seizure and disclosure of such data will be refused for lack of fulfilment of the dual criminality requirement.

Article 24
Access to computer data in international cooperation

1 - In execution of the request of the competent foreign authority, the competent judicial authority may undertake the search, seizure and disclosure of computer data stored in a computer system located within Portuguese territory, relatively to criminal offences provided for in article 11, in situations where the search and seizure are lawfully admitted in a similar national situation.

2 - The competent judicial authority shall act as quickly as possible where there are reasons to believe that computer data under consideration are particularly vulnerable to loss or modification, or where a swift cooperation is provided for in an applicable international instrument.

3 - Paragraph 1 hereof applies, duly adapted, to requests made by Portuguese judicial authorities.

Article 25
Trans-border access to stored computer data where publicly available or with consent

Competent foreign authorities, without the prior authorisation of Portuguese authorities, according to rules on transfer of personal data provided for in Law number 67/98, of 26 October, are entitled to:

a) Access computer data stored in a computer system located in Portugal, where publicly available;

b) Receive or access, through a computer system in their territory, stored computer data located in Portugal, by means of a lawful and voluntary consent of the person who has the lawful authority to disclose the data.

Article 26
Interception of communications in international cooperation

1 - In execution of the request of the competent foreign authority, the judge may authorize the interception of communications transmitted by means of a computer system located within the Portuguese territory, to the extent permitted under agreements, treaties or international conventions, and the situation is as such as to admit the interception, pursuant to article 18, if a similar national situation were at stake.

2 - The Polícia Judiciária shall be competent to receive requests for interception, and shall submit such requests to the Public Prosecution Office, which on its turn shall submit them for authorization to the examining judge at the District Court of Lisbon.

3 - The authorization order referred to in the preceding article shall also allow the prompt transmission of the communication to the requesting State, to the extent permitted under agreements, treaties or international conventions on the basis of which the request was made.

4 - Paragraph 1 hereof applies, duly adapted, to requests made by Portuguese judicial authorities.

CHAPTER V
Final and transitional provisions

Article 27
Territorial application of Portuguese criminal law and jurisdiction of Portuguese courts

1 - In addition to provisions in the Criminal Code on territorial application of Portuguese criminal law, and unless otherwise provided for in international treaties or conventions, for the purposes hereof, Portuguese criminal law shall also apply to facts:

a) Committed by Portuguese nationals, to whom criminal rules of any other State do not apply;

b) Committed to the advantage of legal persons with headquarters in Portuguese territory;

c) Physically committed in Portuguese territory, even if focusing on computer systems located abroad; or

d) Focusing on computer systems located on Portuguese territory, regardless of where the facts were physically committed.

2 - Where on the basis of the applicability of the Portuguese criminal law, both Portuguese courts and courts of another Member State of the European Union claim jurisdiction over a criminal offence established in accordance with this Law, and both courts may start or continue prosecution on the basis of the same facts, the competent judicial authority shall resort to bodies and mechanisms established within the European Union to facilitate cooperation between judicial authorities of Member States and coordination of respective actions, with a view to deciding which of the two States will start or continue prosecution against infringers, in order to centralise prosecution within only one of them.

3 - The decision to accept or to transfer jurisdiction shall be taken by the competent judicial authority, taking into consideration, in turn, the following elements:

a) The place where the infringement was committed;

b) The nationality of the infringer;

c) The place where the infringer was found.

4 - To criminal offences provided for herein shall apply general rules on court jurisdiction provided for in the Criminal Procedure Code.

5 - Where there is any doubt concerning court jurisdiction, namely where the place where the infringer acted does not correspond to the site of installation of the computer system concerned, jurisdiction shall lie with the court where facts were first reported.

Article 28
Applicable general regime

With regard to all matters which are not contrary hereto, to criminal offences, procedural measures and international cooperation in criminal matters provided for herein shall apply, respectively, the provisions of the Criminal Code, Criminal Procedure Code and Law number 144/99, of 31 August.

Article 29
Competence of the Polícia Judiciária for international cooperation

Powers granted to the Polícia Judiciária for the purpose of international cooperation shall be undertaken by the organisational unit responsible for the investigation of criminal offences provided for herein.

Article 30
Protection of personal data

The processing of personal data pursuant hereto shall comply with Law number 67/98, of 26 October, and in case of infringement, provisions in chapter VI thereof shall apply.

Article 31
Repealing provision

Law number 109/91, of 17 August, is hereby repealed.

Article 32
Entry into force

This law shall enter into force 30 days following its publication.

Approved in 23 July 2009.

The President of the Assembly of the Republic, Jaime Gama.

Promulgated on 29 August 2009.

Let it be published.

The President of the Republic, ANÍBAL CAVACO SILVA.

Counter-signed on 31 August 2009.

The Prime Minister, José Sócrates Carvalho Pinto de Sousa.