(the original text, in Portuguese, was published in Diário da República *in 15 September 2009)*

Law no. 109/2009
15 September

Approves the Law on Cybercrime, transposing into national law the framework decision no. 2005/222/JHA of the Council of 24 February on attacks against information systems, and adapting the law to the Convention on Cybercrime of the Council of Europe.

Assembleia da República, under subparagraph c) of Article 161 of the Constitution, decrees the following:

CHAPTER I
Purpose and definitions

Article 1
Subject

This Law establishes the criminal provisions and procedures as well as the provisions on international cooperation in criminal matters relating to the area of cybercrime and the collection of evidence in electronic form, transposing into national law the Council Framework Decision no. 2005/222 /JHA Council of 24 February, on attacks against information systems, and adapting the law to the Convention on Cybercrime of the Council of Europe.

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 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
Criminal provisions

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 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
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
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 are 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 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 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.

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.

Article 10
Assets forfeiture

1 - The court may order the confiscation of the objects, materials, equipment or devices that have served to commit the crimes described under this law and belong to a person who is convicted because of their practice.
2 - In the evaluation, use, disposal and compensation for property seized by the police force which may turn out to be confiscated by the State it will be applied the provisions of Decree-Law No. 11/2007 of 19 January.

CHAPTER III
Procedural provisions

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.

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 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 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 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 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 Procedure.

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.

Article 19
Under covered actions

1 - It is allowed to make use of under covered actions under Law No 101/2001 of 25 August, in the manner specified therein, in the course of investigations concerning the following crimes:
a) described under this law;
b) committed by means of a computer system, if they are punished with, at least, imprisonment of more than 5 years or, even if the abstract penalty is inferior, the act is intentional and respects to crimes against sexual freedom and self determination, or to cases in which the victim is a minor, or in cases of serious fraud, computer and communications fraud, racial, religious or sexual discrimination, economic and financial offenses, and crimes set out under Title IV of the Code of Copyright.
2 - If it becomes necessary the use computer devices, it must followed, when applicable, the same rules as for the interception of communications.

CHAPTER IV
International cooperation

Article 20
International cooperation

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 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 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 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 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 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 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.

CHAPTER V
Final and transitional dispositions

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.

Article 28
General rule

In everything it does not conflict the provisions of this Act, it will be applicable to the crimes here described, to the procedural measures and to international cooperation in criminal matters therein, respectively, the provisions of the Criminal Code, the Criminal Procedure Code and Law No. 144 / 99 of 31 August.

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 30
Protection of personal data

The processing of personal data under this law shall be made in accordance with the provisions of Law No. 67/98 of 26 October and is applicable in case of violation of the provisions in the relevant section VI.

Article 31
Repeal

Law No. 109/91, of 17 August, is repealed.

Article 32
Entry into force

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

Approved on 23 July 2009
Assembleia da República,
Jaime Gama

Promulgated on 29 August 2009
Published
The President of the Republic,
Cavaco Silva

Countersigned on 31 August 2009
The Prime Minister,
José Sócrates Carvalho Pinto de Sousa