EUROPEAN JUDICIAL NETWORK

Fiches Belges on electronic evidence

Portugal

1. Definition of electronic evidence

Our legislation doesn't define "electronic evidence" in general. We retrieve the definition from the practice and doctrine.

It can be defined «*as any type of information, with probative value, stored on any digital storage device or transmitted (on computer systems and networks or electronic communications networks, private or publicly accessible), in binary or digital form*».

The electronic evidence, like any other evidence, must retain its value, to be valued by the judge, and creates its own conviction of veracity of the fact. In turn, the difference between this and the other proofs, is the characteristic of the digital format. So, this may be stored or transmitted also in the digital medium, either on a computer, or any other device capable of safely holding the proof.

The digital format, also responds to the need that society current is presenting in the fight against computer crime. It then becomes possible the location, identification, and delimitation of offenders, with respect to crimes that due to its technological nature, it would be impossible or very complicated to extract a sustained evidence, capable of creating conviction.[1]

2. Which measures are possible in your Member State under International Judicial Cooperation?

1 https://repositorio.ual.pt/bitstream/11144/1849/1/A%20prova%20Digital%20%28Disserta%C3%A7%C3%A3o%29%20%281%29.pdf

Any of the measures provided for in the Chapter III – "International co-operation" of the Budapest Convention are possible:

- Spontaneous information (article 26);
- Expedited preservation of stored computer data (article 29);
- Expedited disclosure of preserved traffic data (article 30);
- Access to stored computer data (article 31);
- Trans-border access to stored computer (article 32);
- Real-time collection of traffic data (article 33)
- Interception of content data (article 34).

As well as the measures provided in general MLA or EIO.

3. Procedure for obtaining electronic evidence

a. National procedures

The discipline for the collection of electronic evidence is outlined:

- In the Criminal Procedure Code;
- In the Law number 32/2008, 17.7 (special regime for the telecommunication providers);
- In the Law number 109/2009, 15.9 (which is our cybercrime law).

The selection of the procedure depends on the type of data we need to collect, the seriousness of the offence under the investigation and the urgency of the situation.

In urgent cases

The determining legal provision is article 12.º of the Cybercrime Law.

If in the course of the case it is necessary to obtain specific computer data stored in a computer system, including traffic data, in relation to which there is fear that they may be lost, altered or no longer available, the competent judicial authority, which is the public prosecutor during the investigation, orders whoever has availability or control of such data, namely the service provider, to preserve the data in question.

The preservation order must contain the following elements (if not, it's considered null and void):

a) The nature of the data;

b) Its origin and destination, if known; and

c) The period of time for which they must be preserved, up to a maximum of three months.

Preservation may also be ordered by the judiciary police with the authorization of the public prosecutor or when there is an urgency or danger in the delay.

If the preservation is asked by the judiciary police, it is necessary to elaborate a report to the public prosecutor in charge, describing the operations, the results and the evidence collected.

In compliance with a preservation order addressed, whoever has availability or control over these data, namely the service provider, immediately preserves the data in question, protecting and preserving its integrity for the fixed time, in order to allow competent judicial authority to obtain it, and is obliged to ensure the confidentiality of the application of the procedural measure.

Injunction to produce or grant access to data

The legal provision is article 14.º of the Cybercrime Law and the specific data retention regime is found in Law n.º 32/2008.

If, in the course of the case, it becomes necessary to produce evidence, with the aim to discover the truth, obtaining specific and determined computer data, stored in a computer system, the competent judicial authority, which is the public prosecutor during investigation, orders whoever

has availability or control of that data to communicate them to the case or allow access to them, under penalty of disobedience.

This provisions are applicable to service providers, who may be ordered to communicate data related to their customers or subscribers to the case, including any information other than traffic or content data, contained in the form computer data or in any other form, held by the service provider, and which allows determining:

a) The type of communication service used, the technical measures taken in this regard and the period of service;

b) The subscriber's identity, postal or geographical address and telephone number, and any other access number, billing and payment details, available on the basis of a service contract or agreement; or

c) Any other information on the location of the communication equipment, available on the basis of a service contract or agreement.

Note that this provision grants protection of right of non-self-incrimination, which means that it's legally prohibited to issue an order to a suspect person or to the defendant to produce data.

Computer data search

The provision is in the article 15.º of the Cybercrime Law.

When it becomes necessary to obtain specific and determined computer data, stored in a computer system, the competent judicial authority, authorizes or orders a research in that computer system, and should, whenever possible, preside over diligence.

It can be ordered by the public prosecutor if the computer system belongs to an enterprise or state service.

The order provided has a maximum validity period of 30 days, which means that it has to be complied within that period (unless an order to extend the period is produced), or it is rendered null and void.

The judiciary police may proceed with the investigation, without prior authorization from the judicial authority, when:

a) It is voluntarily consented by whoever has the availability or control of such data, since the consent given is, in any way, documented;

b) In the case of terrorism, violent or highly organized crime, when there is well-founded evidence of the imminent practice of a crime that puts the life or integrity of any person at grave risk.

When the judiciary police carries out the search under the terms of the previous paragraph, the performance of the due diligence is, under penalty of nullity, immediately communicated to the competent judicial authority (usually the public prosecutor) and assessed by it in order to validate it.

When, in the course of the research, there are reasons to believe that the data sought are in another computer system, or in a different part of the system searched, but that such data are legitimately accessible from the initial system, the search may be extended by authorization or order from the competent authority, which is the public prosecutor during investigation.

Seizure of computer data

The legal provision is article 16.º of the Cybercrime Law.

When, in the course of a computer search or other legitimate access to a computer system, computer data or documents necessary to produce evidence are found, with a view to discovering the truth, the competent judicial authority authorizes or orders the apprehension of them.

The judiciary police may carry out apprehensions, without prior authorization from the judicial authority, in the course of a computer search legitimately ordered and carried, as well as when there is urgency or danger in the delay.

Seizures made by a criminal police body are always subject to validation by the judicial authority, within a maximum period of 72 hours.

If data or computer documents are seized whose content is likely to reveal personal or intimate data, which may jeopardize the privacy of the respective owner or third party, under penalty of nullity these data or documents are presented to the judge, who will consider their inclusion in the case taking into account the interests of the specific case.

Seizures related to computer systems of lawyers, medical and banking activities are subject to an order from the judge.

The seizure of computer data, as appropriate and proportionate, taking into account the interests of the specific case, may, in particular, take the following forms:

a) Seizure of the support where the system is installed or seizure of the support where the computer data are stored, as well as the devices necessary for the respective reading;

b) Making a copy of the data, in autonomous support, which will be attached to the case;

c) Preservation, by technological means, of data integrity, without making a copy or removing them; or

d) Non-reversible elimination or blocking access to data.

Seizure of electronic mail and communications

This specific provision is in article 17.º of the Cybercrime Law.

When, in the course of a computer search or other legitimate access to a computer system, e-mails or communications records of a similar nature are found, stored in that computer system or in another that is legitimate access, the judge may authorize or order the apprehension of those who appear to be of great interest for the discovery of the truth or for the proof.

Interception of telecommunications

The specific provision is in article 18.º of the Cybercrime Law, conjugated with the regime of articles 187.º and 188.º of the Criminal Procedure Code.

The use of interception of communications in criminal proceedings is admissible on cybercrime and in the investigation of the crimes committed by means of a computer system or in relation to which it is necessary to collect evidence in electronic support, when such crimes are:

a) Criminal offences to which a custodial sentence with a maximum limit over three years applies;

b) Drug-related offences;

c) Possession of a prohibited weapon and illicit trafficking in weapons;

d) Smuggling offences;

e) Insult, threat, coercion, disclosure of private life and disturbance of the peace and quiet, whenever committed by means of a telephone device;

f) Threat with the commission of a criminal offence or abuse and simulation of danger signals; or

g) Escape from justice, whenever the defendant has been sentenced for a criminal offence foreseen in the preceding sub-paragraphs.

The interception and registration of computer data transmissions can only be authorized during the investigation, if there are reasons to believe that diligence is indispensable for the discovery of the truth or that proof would otherwise be impossible or very difficult to obtain, by reasoned order from the investigating judge and upon request from the Public Prosecutor.

The interception can be used to record data related to the content of communications or to only collect and record traffic data, the order referred to in the preceding paragraph specifying the respective scope, according to the specific needs of the investigation.

Under covered operations

The specific provision is article 19.º of the Cybercrime Law and the regime of Law n.º 101/2001.

Under covered operations are admissible in the course of an investigation concerning the following crimes:

a) Cybercrime;

b) Those committed by means of a computer system, when, in the abstract, the maximum sentence of imprisonment is greater than 5 years or, even if the penalty is lower, and being intentional, crimes against freedom and sexual self-determination in cases where the offended are minors or incapacitated, qualified fraud, computer and communications fraud, racial, religious or sexual discrimination, economic and financial offenses, and authorial rights violation crimes.

b. international procedures (including Available channels/ways to obtain electronic evidence from your Member State; urgent procedures; specialised networks to obtain electronic evidence e.g. 24/7 Budapest Convention/police channels)

Portuguese 24/7 channel

For the purpose of international cooperation, with a view to providing immediate assistance, the Judiciary Police ensures the maintenance of a structure that guarantees a point of contact available permanently, twenty-four hours a day, seven days per week.

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

The immediate assistance provided by this permanent contact point includes:

a) Provision of technical advice to other contact points;

b) The expeditious preservation of data in cases of urgency or danger in delay;

c) The collection of evidence for which it is competent in cases of urgency or danger in the delay;

d) The location of suspects and the provision of information of a legal nature, in cases of urgency or danger in delay.

Judiciary Police (Lisbon) contacts:

National Cybercrime Unit – UNC3T

Address: Rua Gomes Freire,174, 1169-007 Lisboa

EUROPEAN JUDICIAL NETWORK

Contacts:

9h00 – 17h30:

+351 211967484

+351 925486485

+351 211967847

In other hours (24/7):

+351 211967000 – ask for connection to Computer Crime Unit

E-mail: contacto24.7@pj.pt

Contact person:

Mr. Bravo, Rogerio +351968030160 r.bravo@pj.pt

Police Channels:

- Europol
- Interpol
- Sienna
- Liaison and foreign liaison officers

EIO or MLA:

- COE and EU Treaties;
- UN Treaties;
- Bilateral Treaties

3. International legal framework applicable for this measure in your Member State

- Directive 2014/41/EU: the European Investigative Order (EIO) was implemented in the Portuguese Law as of 22 August 2017, by the Law number 88/2017, 21 August;
- EU Convention on Mutual Assistance in criminal matters between the Member States of the European Union (29 May 2000);
- European Convention on Mutual Assistance in criminal matters (20 April 1959) and its Additional Protocols;
- Multilateral or bilateral treaties;
- 2001 Budapest Cybercrime Convention.

4. competent authority to receive and execute your request

European Investigation Order:

The competent authorities to receive and execute an EIO, in accordance with the article 19 of Law 88/2017, of 21 August, are the same national authorities locally competent to order an investigative measure, in accordance with the provisions of the Portuguese criminal procedural law, that is the public prosecutor, the examining judge in the limits of its competences or the judge (during the trial phase). The Atlas of the European Judicial Network should be consulted.

MLA requests:

In rogatory letters, in case there is no direct communication between judicial authorities, the request must be sent to the Central Authority, which is the Procuradoria-Geral da República (Prosecutor General's Office), who in turn will forward to the competent authority to execute the request:

Person of contact inside Central Authority:

Joana Gomes Ferreira
Rua do Vale do Pereiro, nº2 - 1269-113 Lisboa
+351 21 382 03 57 - +351 21 382 03 00

EUROPEAN
JUDICIAL NETWORK

21 386 90 49 (fax)
joana.ferreira@pgr.pt

5. accepted languages

Portuguese and Spanish (only for EIO's received from Spain).

7. Definition of data category and examples: subscriber, traffic/transaction and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations

Subscriber and access data: elements that serve to identify a subscriber or customer, such as the user (name), date of birth, postal address, gender, type and kind of service (eg. Network provider, VPS or dedicated server, physical location of the server), administrative features (sometimes: bank account), telephone number, email address or IP address at the time of registration, registration date, etc.

Traffic and localization data: Our domestic law defines traffic data in the article 2, c) of the Law number 109/2009 as the computer data related to a communication chain, indicating the origin of the communication, the destination, the route, the time, the date, the size, the duration or the type of underlying service.

Content data: any stored data in a digital format (text, voice, videos, images and sound), different from the real time interception.

Access to subscriber and access data

If, in the course of the case, it becomes necessary to produce evidence, with the aim to discover the truth, obtaining specific and determined computer data, stored in a computer system, the competent judicial authority, which is the public prosecutor during investigation, orders whoever has availability or control of that data to communicate them to the case or allow access to them, under penalty of disobedience.

This provisions are applicable to service providers, who may be ordered to communicate data related to their customers or subscribers to the case, including any information other than traffic or content data, contained in the form computer data or in any other form, held by the service provider, and which allows determining:

a) The type of communication service used, the technical measures taken in this regard and the period of service;

b) The subscriber's identity, postal or geographical address and telephone number, and any other access number, billing and payment details, available on the basis of a service contract or agreement; or

c) Any other information on the location of the communication equipment, available on the basis of a service contract or agreement.

No threshold is necessary.

Access to traffic and localization data

The procedure is similar to the one described for the access to subscriber data, but in this case, the public prosecutor should ask first the authorization to the examining judge.

The access to traffic data is admissible on cybercrime and in the investigation of the crimes committed by means of a computer system or in relation to which it is necessary to collect evidence in electronic support, when such crimes are:

a) Criminal offences to which a custodial sentence with a maximum limit over three years applies;

b) Drug-related offences;

c) Possession of a prohibited weapon and illicit trafficking in weapons;

d) Smuggling offences;

e) Insult, threat, coercion, disclosure of private life and disturbance of the peace and quiet, whenever committed by means of a telephone device;

f) Threat with the commission of a criminal offence or abuse and simulation of danger signals; or

g) Escape from justice, whenever the defendant has been sentenced for a criminal offence foreseen in the preceding sub-paragraphs.

Access to content data:

The examining judge may authorize the apprehension of those content who appear to be of great interest for the discovery of the truth or for the proof.

The investigative measure shall meet the principles of speciality, adequacy, exceptional nature, necessity and proportionality of the measure.

The access to content data is admissible on cybercrime and in the investigation of the crimes committed by means of a computer system or in relation to which it is necessary to collect evidence in electronic support, when such crimes are:

a) Criminal offences to which a custodial sentence with a maximum limit over three years applies;

b) Drug-related offences;

c) Possession of a prohibited weapon and illicit trafficking in weapons;

d) Smuggling offences;

e) Insult, threat, coercion, disclosure of private life and disturbance of the peace and quiet, whenever committed by means of a telephone device;

f) Threat with the commission of a criminal offence or abuse and simulation of danger signals; or

g) Escape from justice, whenever the defendant has been sentenced for a criminal offence foreseen in the preceding sub-paragraphs.

8. Voluntary-disclosure:
    a. As issuing state: Admissibility of the electronic evidence obtained by voluntary disclosure.

There is not a specific legal provision, but the principle inscribed in the article 14.º of the Cybercrime Law and the provisions regarding the preservation order, don't prohibit evidence gathering through voluntary disclosure.

b. As executing state: Procedures/legislation in your Member State with regards to the possibility for the OSPs in your Member State to provide data directly to other Member States

There is no specific legal provision determining an obligation to the Portuguese based ISP's and OSP's to address direct requests made by a foreign Law Enforcement or Judicial authority, but voluntary cooperation requests are also not prohibited, and voluntary disclosure depends on their specific policies.

Another possibility to circumvent or bypass judicial cooperation mechanisms for the gathering of subscriber and access data (the only situation where no judicial authorization is needed), is to address the requests for such data via the 24/7 Network.

9. Data retention periods (including procedures for extensions)

Service Providers store data according to two different legal regimes:

- the general regime, provided for in the Cybercrime Law, in Law no. 41/2004 and in Article 189.º, no. 2 of Criminal Procedure Code and
- the special regime, provided for in Law 32/2008.

General Regime:

The regulatory framework allows operators to retain such data for six months.

Special Regime:

Law 32/2008 provides the obligation for the service providers to maintain traffic data (between others) for a period of one year. However, it expressly stipulates (Article 1, paragraph 1) that such conservation of data is carried out "*for the purpose of investigating, detecting and prosecuting serious crimes*". This standard establishes, in a definitive manner, corroborated by paragraph 1 of Article 3 of the same Law, that "*the conservation and transmission of data are for the sole purpose of investigating, detecting and prosecuting serious crimes*".

On the other hand, the same diploma establishes, in Article 2, paragraph 1, point g), that serious crimes are: "*crimes of terrorism, violent crime, highly organized crime, kidnapping, kidnapping and taking hostages, crimes against cultural identity and personal integrity, against state security, counterfeiting currency or currency-related securities and crimes covered by an air navigation safety convention or maritime*".

So, in short, in addition to several other requirements, only these data can be requested, retained by the under Law 32/2008, if one of the types of crime referred to above is under investigation. Such a request must be made by court order from the judge, pursuant to Article 3, paragraph 2 and Article 9 of Law No. 32/2008.

Type of data	Period of data retention
Subscriber data	Always available
Access data and Internet Protocol (IP address)	Six months
Traffic data - crimes referred to in article 187.º of the Criminal Procedure Code	Six months
Traffic data – crimes mentioned in the special regime (*crimes of terrorism, violent crime, highly organized crime, kidnapping, kidnapping and taking hostages, crimes against cultural identity and personal integrity, against state security, counterfeiting currency or currency-related securities and crimes covered by an air navigation safety convention or maritime)*	One year

10. Procedure for data preservation/execution deadline

If in the course of the case, it is necessary to produce evidence, with a view to discovering the truth, obtaining specific computer data stored in a computer system, including traffic data, in relation to which there is fear that they may be lost, changed or when they are no longer available, the competent judicial authority orders whoever has availability or control of such data, namely the service provider, to preserve the data in question.

Preservation may also be ordered by the criminal police body with the authorization of the competent judicial authority or when there is an urgency or danger in the delay, in which case the latter shall immediately report the fact to the judicial authority and transmit a report from the situation.

The preservation order discriminates, or is rendered null and void:

a) The nature of the data;

b) Its origin and destination, if known; and

c) The period of time for which they must be preserved, up to a maximum of three months.

In compliance with a preservation order addressed, whoever has availability or control over these data, namely the service provider, **immediately preserves the data in question**, protecting and preserving its integrity for the fixed time, in order to allow competent judicial authority to obtain it, and is obliged to ensure the confidentiality of the application of the procedural measure.

The competent judicial authority may order the renewal of the measure for periods subject to the limit of three months, provided that the respective admissibility requirements are verified, **up to a maximum limit of one year.**

11. Procedure for data production/ execution deadline

If in the course of the case it becomes necessary to produce evidence, with a view to discovering the truth, obtaining specific and determined computer data, stored in a given computer system, the competent judicial authority orders whoever has availability or control of that data to communicate it to the case or that allows access to them, under penalty of punishment for disobedience.

The order identifies the data in question.

In compliance with the order, **whoever has availability or control of such data communicates these data to the competent judicial authority** or allows, under penalty of punishment for disobedience, access to the computer system where they are stored.

There is no execution deadline. Nevertheless, it may be taken into account the periods of data retention or preservation.

12. Concise practical information

Cybercrime Department

Address: Rua do Vale de Pereiro, n.º 2 - 2.º, 1269-113 Lisboa-Portugal

Contacts:

+351 213 921 900

Fax:

+351 213 975 255

Email:

cibercrime@pgr.pt

Site:

http://cibercrime.ministeriopublico.pt

Our main service providers:

- MEO – Serviços de Comunicações e Multimédia, S.A.

Address: Rua Andrade Corvo, nº 6, 3º, Bloco B, 1050–009 LISBOA

- NOS, Comunicações, S.A.

Address: Rua Ator António Silva, nº 9, Campo Grande, 1600-404 LISBOA

- VODAFONE Portugal Comunicações Pessoais S.A.

Address: Av. D. João II Lt 1.04.01 8º Sul, 1998-017 LISBOA