EUROPEAN
JUDICIAL NETWORK

Fiches Belges on electronic evidence

1. Definition of electronic evidence

It is any data or information which is generated, stored or transmitted in digital form by electronic devices that are relevant in investigating and prosecuting criminal offences.

"For the purposes provided for in this article, electronic traffic, or associated, data are understood to be all those created as a result of the communication travelling down an electronic communications network, of it being made available to the user, and the provision of a similar information society or telematic communication service" (art.588 ter Spanish Procedural Code)

Electronic evidence refers to various types of data in electronic form (historical or streaming) - including 'content data' such as e-mails, text messages, photographs and videos - often stored on the servers of online service providers, as well as other categories of data, such as subscriber data or traffic information regarding an online account (IP addresses, user name…)

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

Any of the measures provided for in the third chapter of the 2001 Budapest Cybercrime Convention are possible, that is:

- Expedited preservation of stored computer data.(Art. 29 Budapest Convention)
- Expedited disclosure of preserved traffic data (Art. 30 Budapest Convention)
- Production orders/access to data (Art. 31 Budapest Convention)
- Spontaneous information (Art. 26 Budapest Convention)
- Trans-border access to store computer data with consent or where publicly available (Art. 32 Budapest Convention)
- Real time collection of traffic data (Art 33 Budapest Convention)

3. Procedure for obtaining electronic evidence

a. National procedures

Investigative measures involving the interception and registration of electronic devices and telematic communications are regulated in Ley de Enjuiciamiento Criminal; - this is the code of criminal procedure-, in articles 588 bis to 588.8ª.

In general, only measures to investigate crimes are possible (not to prevent them), and taking into account the principles of exceptionality and proportionality (the severity of the fact, the intense evidence of criminality, the relevance of the result, etc. are taken into account (article 588 bis.a).

In general, the investigating judge is the competent authority to authorize the investigation measures (article 588 bis .b).

Must be taken into account:

1. The interception of telematic communications that entail obtaining content data, is only possible when the investigation is aimed at prosecuting (art 588.3º.a):

- Intentional crimes punished with a maximum of at least three years.
- Offenses committed by criminal organizations
- Terrorism crimes
- Crimes committed by computer means or by information technology.

2. The judicial intervention of the terminals or the media of the victim may be authorized in case of serious risk to his life or integrity is foreseeable.

3. The judicial intervention of the communications emitted from terminals or means of communication of a third party can be authorized as long as there is evidence that the investigated subject uses the communication means to transmit information, the owner of the terminal or means of communication collaborate with the person investigated in the commission of the crime or benefit from the activity or finally when the device has been used maliciously by third parties without the owner's knowledge. (art 588 3º.c).

4. All service providers have the duty to cooperate with the judge, the public prosecutor and the judicial police. Non-cooperation is punished as a crime of disobedience. (588 3º.e).

5. The time limit (maximum duration)of the intervention from the judicial authorization is three months, extendable for successive periods of three months up to a maximum of 18 months (art 588.3º.g).

6. The identification of terminals or devices and their holders can be carried out by the judicial police or by the public prosecutor who can go directly to the service providers (588 3º l and 588 3º m).

7. The registration of the information of seized computer equipment requires judicial authorization although in urgent cases the judicial police can carry out the registration communicating it to the judge within a maximum period of 24 hours in a reasoned brief and the judge will revoke and confirm the duration in 72 hours (art 588.6ª).

8. It is possible to remotely register computer equipment with judicial authorization for a maximum duration of one month, extendable up to a maximum of three months, and only for certain crimes such as: terrorism, committed against minors, committed by criminal organizations, against the Constitution, treason or related to the national defense or those committed through computerized means or telecommunication or communication services (art 588. 7º)

9. The public prosecutor and the police can require to any natural or legal person the preservation of data up to a maximum of 90 days, extendable to a maximum of 180 days (art588.8º)

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)

- **Police channels: Europol/Interpol/Sienna/Liaison and foreign liaison officers.**

- **Budapest Convention 24/7 Network:** urgent preservation requests to seize volatile subscriber information/traffic data/content (only with MLAT-guarantee:, the available data will be preserved/seized and will only be provided after receiving the MLAT/EIO in 60 days).

- **EIO/MLAT (COE and EU Treaties; UN Treaties and Bilateral Treaties).**

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

- 2001 Budapest Cybercrime Convention
- EU Directive 2014/41/EU,(The European Investigation Order)
- 2000 EU Convention on Mutual Assistance in criminal matters between the Member States of the European Union) for Member State who have not implemented EIO
- European Convention on Mutual Assistance in criminal matters (Strasbourg, 1959 and additional protocols);
- Other bilateral and multilateral treaties.

5. Competent authority to receive and execute your request

If a European Investigation Order is issued, the competent authority to receive is the State Prosecution Office and to execute Prosecution Office or an Investigative Court depending on the type of data requested. The Atlas of the European Judicial Network should be consulted.

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 " Subdirección General de Cooperación Jurídica Internacional del Ministerio de Justicia (c. San Bernardo 62. Madrid 28071), who in turn will forward to the competent authority to execute the request.

6. Accepted languages

Spanish and Portuguese (Only from Portugal)

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 data** – simply saying: personal and some metadata/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 (e.g. 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 etcetera.

- **Traffic data** – all (transactional) data that relates to the (provision of a) service and its distribution e.g.: the source and destination of the IP address, source and destination port (tcp/udp), timestamp, size IP packet (bytes). (Simply saying: log files: date, time, duration, route, date, time of use).

- **Content data** – any stored data in a digital format (text, voice, videos, images, and sound other than subscriber or traffic data).

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

As a general rule, judicial authorization is required (art. 588.a Criminal Procedural Law). However, the Public Prosecution Service or the Judiciary Police may go directly to the service providers to obtain the owner of a telephone number or any other means of communication, or, conversely, need the telephone number or identity details of any means of communication (art. 588 ter m).

It applies to all type of crimes committed using computer equipment or any other information or communication service technology, and also intentional crimes punished with a maximum sentence of, at least, three years imprisonment; crimes committed as a member of a criminal group or organization; or crimes of terrorism.

According to its intrusive nature, when it comes to traffic data and content data, an explanation from the issuing state with regard to the necessity of the data sought in relation to the investigation is required.

8. Voluntary-disclosure:

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

Voluntary disclosure of electronic evidence by the online service provider is only admissible when it is related to data where no judicial authorization is needed according to the Spanish legislation. For this reason, its admissibility is limited to data related to subscriber data alone, not to traffic data or content data.

   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

The Spanish legislation does not foresee the possibility that OSP can provide data directly to other Member States, regardless of the category of such data.

In practice, in order to circumvent or bypass cumbersome judicial cooperation mechanisms for the gathering of subscriber data (the only situation where no judicial authorization is needed) requests for such data are channelled via the 24/6 Network; in these cases, upon request of authorities in other Member States or third States, the contact points (law enforcement officials only in Spain) address directly the OSP based in Spain, request the needed information and, one received, forward it to the requesting authority.

9. Data retention periods (including procedures for extensions)

Pursuant to Article 5 of Law 25/2007, on electronic communications and public communications networks data retention, OSP providing communication services or engaged in communications public networks are bound by the obligation to retain traffic data for a period of 12 months, such traffic data are related to those produced in the course of the communication process. This period starts from the moment the communication process have taken place. This article allows the Government, by way of regulations, to extend the period for a maximum of two years or to limit it to a shorter period not less than 6 months. For such purpose, the Government will take into consideration the data storing costs and the relevance of such data for the purpose of detection, investigation and bringing to trial serious forms of criminal activities. Due to the guarantees and safeguards provided for in this law, it has not been affected by the judgements of the CJUE.

10. Procedure for data preservation/execution deadline

Article 16 of the Budapest Convention was transposed into national law in Article 588.g of the Criminal Procedural Law, according to which:
The Public Prosecution Service, or the Judicial Police, may require any individual or legal entity to preserve and protect specific data or information included on a computer information system which they have access to until the relevant judicial authorisation is obtained for its production, in accordance with the provisions of the preceding articles.

The data will be preserved for a maximum period of ninety days, which may only be extended once until its production is ordered or one hundred and eighty days have elapsed.

The requested entity or individual will be bound by the obligation to cooperate and must ensure confidentiality in the course of the execution of this measure and will be subject to liability in case of non-compliance.

The Spanish legislation does not foresee the situations referred to in Article 17 of the Budapest Convention, when different OSPs are involved in the communication process storing data related to the investigation. Nevertheless, when in the course of a criminal investigation a OSP is requested to preserve data and the data is not being held by such OSP, Article 17 of the Budapest Convention is the legal basis to request such OSP to identify the OSP that is actually the owner of the data. Such is the case where the requested OSP informs that it has only taken part in the communication process to a limited extent and that the data is being held by another OSP; in these situations the requested OSP needs to provide sufficient information for the requesting authority to be able to identify the OSP which is the real target of the investigation.

11. Procedure for data production/ execution deadline

Pursuant to the Criminal Procedural Law, the requirements needed for the production of data held by individuals or OSP differed depending on the type of data or the place where such data are stored:

a) Art. 588.b.x. Electronic data held by OSP or persons facilitating communication in compliance with the legislation on data retention or on their own initiative for commercial reasons, or other type, and which are linked to communication processes, may only be produced if a judicial authorization has been issued for such purpose.
b) Art. 588.b.xiii. Subscriber data (identification of telephone or other means of communications numbers holders or vice versa, the identification of the telephone numbers a concrete person is owner of) may be requested by the Prosecution Service or the Judicial Police and no judicial authorisation is needed.
c) Art 588.e.i,ii and iii. Gathering of evidence related to content data stored in a mass storage device always requires judicial authorization. Nevertheless, in duly justified emergency cases access to such data by law enforcement units is permitted without a prior judicial authorisation. The competent court has to be notified within 24 hours; the court will have to either validate the access or declare it invalid within the following 72 hours.

12. Concise legal practical information

The procedural regulation of the technological investigation measures aimed at the gathering of electronic evidence was introduced in the Spanish legal framework by Law 13/2015 amending the Criminal Procedural Law on the strengthening of procedural guarantees and technological investigative measures.

Due to the fact that gathering of electronic evidence has a high impact in fundamental rights of the suspects (privacy, secrecy of communications or data protection issues), safeguards and guarantees have been foreseen in Article 588.a.i. The guiding principles are: specialty, adequacy, exceptionality, necessity and proportionality; as for the latter, one of the circumstances the court needs to weigh is the severity of the crime.

In addition, Article 588.b.i, limits the scope of the technological investigative measures to those crimes punished with deprivation of freedom for a maximum of at least 3 years, crimes committed in the context of a criminal organisation and terrorist crimes. Nevertheless, since it is obvious that some crimes cannot be investigated unless having recourse to a technological investigative measure, such measures are also applicable to any other crimes committed or facilitated by means of an electronic device or any information or telecommunication technology, provided that the guiding principles are met, in particular, the proportionality principle; an assessment on a case-by-case basis is always needed.

The Spanish procedural framework also foresees the trans-border access to stored computer data (Article 588.f..i,ii and iii) regulated in Article 32 of the Budapest Convention. The adoption of this investigative tool is subject to very strict requirements and supervision mechanisms, even to a higher extent than the abovementioned technological investigative measures.

Finally, the Spanish criminal procedural legislation foresees the possibility for online undercover agents (Article 282.a) which may be even authorised to exchange illicit files for the purpose of the investigation.