Fiches Belges on electronic evidence

France

1. Definition of electronic evidence

Electronic evidence is any probative information which is generated, stored or transmitted in digital form by electronic devices that are relevant in investigating and prosecuting criminal offences (to identify or localize a suspect and obtain information about their activities or determine the extent of the damage/victims, to use the information as evidence in a case etc.). 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.

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

a. Expedited preservation (Art. 29 Budapest Convention)
b. Expedited disclosure of traffic data (Art. 30 Budapest Convention)
c. Production orders/access to data (Art. 31 Budapest Convention)
d. General MLA or EIO

In case of absence of bilateral/multilateral agreements on mutual legal assistance, could be the options for sending or receiving request for retained data:

a. Reciprocity
b. Spontaneous information (Art. 26 Budapest Convention)
c. Trans-border access (Art. 32 Budapest Convention)
d. Spontaneous information (Art. 7 EU Convention)

3. Procedure for obtaining electronic evidence

a. National procedures

In general criminal investigations and prosecution procedures are regulated by the French Code of Criminal Procedure (Code de procedure pénale, CPP). Investigation powers can be used, depending on the invasiveness of the investigation power at hand and the seriousness of the offence under investigation. A threshold for allowing special investigation powers which is commonly used in France is that the crime is linked to organized crime, and only applicable for certain specifically mentioned offences (art. 706-73 and 706-73-1 CPP). The special investigation measure of computer data capture is possible under 706-102-1 CPP. You can also order production of stored content data (like email, “correspondences”) under 706-95-1 and 706-95-2 CPP, however the wiretap technique should be used for future email (not stored) (art 100 and 706-95 CPP).

Because digital investigation powers may also be required for “simple” cybercrimes, for example only using means of digital communication, the technique of investigation under pseudonym (undercover operation) is possible under 230-46 CPP (the offence should be punished with imprisonment).

In general, Data requisition could be made under articles 60-1, 60-2, 77-1-1, 77-1-2 and 99-3, 99-4 (investigations) depending on the stage of the investigations. However the execution of this data requisition is on a voluntary basis concerning providers located abroad.

In order to obtain user metadata, legal obligations impose a retention period of one year on electronic communication operators.

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: all information that can be exchanged between police agencies.

Police cooperation covers information provided voluntarily by private partners (without requisition or coercion)

The cooperation channels (concentrated within the national 24/7 POC of the OCLCTIC) are:

- Budapest network (data preservation, general information) with the 65 members of the network.

- G7 network (data preservation, general information) with 23 network members from 88 countries which are not in the Budapest network.

- BCN / Interpol network (police and general cooperation) with all the member countries of the organization.

- EUROPOL / Siena network (police cooperation) with EU partners.

- EU network of directive 2014/41 / EU (cyberattacks)

- DCI / embassies network (general cooperation, police cooperation, see judicial cooperation relay in some countries), for cooperation not covered by the previous channels.

General MLAT (CoE and EU Treaties; UN Treaties and bilateral treaties)

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

- Budapest Convention
- EU Directive 2014/41/EU, with the European Investigation Order (EIO), was implemented in Dutch law, effective from June 17th 2017.

For countries who have not implemented this EU Directive:

- 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 (Strasbourg, 1959 and additional protocols);
- Several other bilateral and multilateral treaties.

5. competent authority to receive and execute your request

Data preservation requests (art 29) are received and processed by POC24 / 7, located at OCLCTIC

EIO are received and processed directly by the courts.

MLA requests are received by the French ministry of Justice and executed by the Courts.

6. accepted languages

Requests addressed to the POC 24/7 (emergency preservation, general information, police cooperation) are processed in French and English.

EIO and MLA requests have to be translated in French.

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 at the time of registration.

Elements that serve to identify a subscriber or customer, such as the (user)name, ID given by ISP, date of birth, postal address, gender, type and kind of service (e.g. network provider, physical location of the server), administrative features (sometimes: bank account), telephone number, SIM number, email address or IP address at the time of registration, registration date.

Tresholds: all offenses.

- 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), MAC address (device), timestamp, size IP packet (bytes). (Simply saying: log files: date, time, duration, route, date, time of use). See for detail decree n°2011-219 (25th February 2011). Could include geolocalisation data.

Tresholds: For stored data, all offenses. Different legal framework for real time interception.

- Content data – any stored data in a digital format (text, voice, videos, images, and sound other than subscriber or traffic data), also queries on search engine (consulted informations).

Tresholds: For stored communications ("correspondences") data, serious offense, need the agreement of a judge (706-95-1 and 706-95-2 Code of criminal procedure). Different legal framework for real time interception.

8. Voluntary-disclosure:

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

Admissible

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

No legal Framework for voluntary disclosure. It is a question of sovereignty. However, the practice is not yet formally prohibited.

9. Data retention periods (including procedures for extensions)

The legal general retention period for data (connection / traffic) is one year. Following the implementation of the preservation measure, the data retained will remain so for the time necessary for the investigation.

10. Procedure for data preservation/execution deadline

In accordance with article 16 of the agreement, the POC 24/7 asks the data provider concerned to keep data for 90 days, (renewable once by the requesting partner). At the end of the 180 days, this last is then no longer required to keep the required data. The renewal by the requesting party is absolutely necessary before the first 90 days. The request must be addressed to POC24 / 7.

11. Procedure for data production/ execution deadline

Data production requires receipt of a request for international judicial assistance. This one must therefore be sent before the 90 days.

12. Concise legal practical information

N/A