EUROPEAN JUDICIAL NETWORK

Fiches Belges on electronic evidence

Belgium

1. Definition of electronic evidence

There is no internationally accepted definition of electronic evidence. However, in all countries there are regulations containing precepts which, in some way, refer to electronic evidence. Also in Belgian legislation a legal definition of 'electronic evidence' is not to be found. The "definition" in the Council of Europe Guide, endorsed by Belgium, is: "*Any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings*".

The sources of electronic evidence can be any electronic device (such as but not limited to: an external case housing circuit boards, microprocessors, hard drives, memory and connections for other devices, a monitor or other display device, a keyboard, a mouse, externally connected drives, peripheral devices, software, …).

Belgian legislation does provide definitions for specific types of data :

- **Subscriber data:** data identifying the user or subscriber and the means of communication (*art 46bis 1° of Belgian Code of criminal procedure*);
- **Traffic data:** data related to the access to and connection of the terminal equipment to the network and to the service and relating to the location of that equipment (*art. 126 of Belgian Law on electronic communication 13 June 2005*);
- **Location data:** data related to the origin or the destination of electronic communications (*art. 88bis of Code of criminal procedure*);
- **Content data:** data related to the content of electronic communications (*art 90ter of Belgian Code of criminal procedure*).

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

In Belgium, the following measures are possible :

- Expedited preservation (*Art. 29 of Budapest Convention*);
- Expedited disclosure of traffic data (*Art. 30 of Budapest Convention*);
- Production orders/access to data (*Art. 31 of Budapest Convention*);
- Gathering of electronic evidence through MLA-request or EIO.

In the absence of bilateral/multilateral agreements on mutual legal assistance, the options to base the sending or receiving of requests on for retained data are:

- Spontaneous information (*Art. 26 of Budapest Convention or Art. 7 of EU MLA Convention, Art. 18.4-5 of the United Nations Convention against Transnational Organized Crime*): if there is a Belgian interest, a mirror investigation could be possible from which a spontaneous exchange of information could be considered;
- Trans-border access (*Art. 32 of Budapest Convention*);
- Reciprocity.

3. Procedure for obtaining electronic evidence

a. National procedures

Articles 46bis, 88bis, 90ter and 90quater of the Belgian Code of Criminal Procedure (BCCP) are the legal bases for issuing an order for identification of data, metadata, localization data, traffic data, access data and content data. Article 39bis BCCP regulates the open (not covert) search in seized computer systems. Article 88ter BCCP regulates the (open – not covert) remote search and seizure in computer systems.

Based on the level of intrusion on privacy of the user, specific procedural conditions and safeguards have been put in place for the different types of measures:

- **Procedure art. 39bis BCCP on search and seizure in computer systems**: The prosecutor can order an open (not covert) investigation to search seized or seizable computer systems (under conditions and safeguards). In certain circumstances also a police officer is allowed to initiate a search in a computer system (for example: in case of red-handedness).
- **Procedure art. 46bis BCCP on subscriber data:** In accordance with article 18, b of the Budapest Convention, a public prosecutor may order a service provider, offering services on the Belgian territory, to submit subscriber information, i.e. the identification of the user and the services used. The order should include a reasoning concerning its compliance with the principles of proportionality and subsidiarity. This procedural power should be interpreted in accordance with the T-CY Guidance Note #10 on Production orders for subscriber information (*Article 18 Budapest Convention*).
- **Procedure art. 88bis BCCP on location and traffic data:** An investigating judge may order a service provider to submit location and traffic data related to electronic communications.
- **Procedure art. 88ter BCCP on remote search and seizure in computer systems**: In an open (not covert) investigation, an investigating judge can issue a warrant for a remote search and seizure of a computer system that is not in the physical possession of the investigators, but is reachable from a distance (this measure can also be executed across borders). Conditions and safeguards are in place.

- **Procedure art. 90ter BCCP (and following) on content data:** Interception of communication and access to stored content data can be ordered by an investigating judge. This judge may, in exceptional cases, order a service provider to intercept information not accessible to the public or to submit stored content data or communication data. This procedural power also allows for an investigating judge to warrant a legal hacking of computer systems (as a covert measure). This warrant can only be issued for specific crimes (inventory of 45 types of crimes). Conditions and safeguards are in place, more specifically, the principles of proportionality and subsidiarity should be complied with.

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)

- **Judicial 24/7 channel/network (Budapest Convention**): urgent preservation requests to seize volatile subscriber information/traffic data/content (only possible with MLAT-guarantee). The available data will be preserved/seized and will only be provided after receiving the MLAT/EIO in 60 days (can be renewed). The Belgian 24/7 SPOC is the Federal Computer Crime Unit: DJSOC.FCCU.Perm@police.belgium.eu;
- **Article 18 of Budapest Convention:** as far as they are offering services in another country, Belgian service providers could respond to a direct production order of a foreign judicial authority from that other country, although they also might require an EIO or MLA-request (to be assessed provider by provider);
- **Spontaneous information sharing** (Art. 26 of Budapest Convention or Art. 7 of EU MLA Convention or Art. 18.4-5 of the United Nations Convention against Transnational Organized Crime). Note: if there is a Belgian interest, a mirror investigation could be possible from which a spontaneous exchange of information could be considered;
- **General MLAT** (COE treaties, EU treaties, UN treaties and bilateral treaties) **and EIO**.

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

With regards to (EU Member) states that have implemented the same instruments, the following legal framework is applicable:

- Budapest Convention;
- EU Directive 2014/41/EU on the European Investigation Order (EIO), implemented in Belgian legislation by the law of 22 may 2017.

For countries who have not ratified nor implemented the above mentioned instruments, the following legal framework(s) can be applicable:

- 2000 EU Convention on Mutual Assistance in criminal matters between the Member states of the European Union;
- 1959 European Convention on Mutual Assistance in criminal matters and its additional protocols;
- 2000 United Nations Convention against Transnational Organized Crime;
- Other bilateral treaties[1];
- Other multilateral treaties[2].

5. Competent authority to receive and execute your request

a. The competent authority to receive the request/decision for judicial cooperation:

In relation with EU Member States, the request/decision has to be sent to the local public prosecutor's office of the geographical area where the investigating measure has to be executed.
Requests/decisions may also be sent to the Federal Prosecutor, in particular in the following cases:

- urgency;
- the location of the investigative measure needs to be determined;
- coordination of the execution of the measures is needed.

In relation with third countries, the Minister of Justice (Central Authority for international cooperation in criminal matters, Waterloolaan 115, 1000 Brussels) is the competent authority for receiving requests from non-EU states. When allowed under the applicable mutual legal assistance Treaty, the request may be sent directly to the local prosecutor's office (if localized) or the Federal Prosecutor's Office (if not localized or if urgent or if national coordination is needed).

In case of doubt on the competent authority, requests may be sent to the central authority of the Ministry of Justice, Waterloolaan 115, 1000 Brussels, Belgium (centralauthority.iccm@just.fgov.be), or the Federal Prosecutor's Office, Wolstraat 66-1, 1000 Brussel (federaal.parket@just.fgov.be).

b. The competent authority to execute the request/decision for judicial cooperation:

[1] Belgium has concluded a number of bilateral agreements on mutual legal assistance in criminal matters. These instruments do not have any specific provisions related to electronic evidence, therefore the same regime applies as for requests for 'traditional' investigative measures.

[2] For example:

- Agreement between the European Union and the United States on mutual legal assistance
- Agreement between the European Union and Japan on mutual legal assistance in criminal matters

The public prosecutor is the competent authority to recognise and execute measures related to the obtaining of subscriber data. The investigating judge is competent to recognise and execute measures related to the obtaining of location, traffic and content data. For all measures requested by non-EU states (house searches, …), the Minister of Justice has to give clearance prior to the execution.

6. Accepted languages

Languages in which requests under the Budapest Convention and EIOs can be handled in Belgium are :

- Dutch
- French
- German
- English

Important remark : the EIO or MLA-request will be internally translated if the language is not the language of the judicial area where the decision/request has to be executed. In case of urgency, it is recommended – where possible – to translate the decision/request in the language of the region.

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

a. Subscriber data (article 46bis):

The request can be done by the public prosecutor. However, if the criminal act cannot be punished with imprisonment of 1 year or higher, the prosecutor can only go back in time 6 months, starting from his request. If the investigated crime is punishable with imprisonment of 1 year or more, data retention up to 12 months is possible. *(see also answers to questions 1 & 3)*

b. Location and traffic data (article 88bis BCCP):

The request can be done by an investigating judge when there are serious indications that the criminal act can be punished with imprisonment of 1 year or higher. However, in cases of red-handed acts, the prosecutor can do the request if it concerns criminal acts as listed in article 90ter, §2 BCCP (a list of 45 crimes for which a wire-tap/legal hacking can be ordered). Depending on the type of crime, the investigating judge or the prosecutor can go back in time in a time-fork of 6 to 12 months (art. 88bis, §2 BCCP).

The following conditions have to be fulfilled:

- there are serious indications to believe that the alleged criminal activities are punishable by a maximum penalty of at least 1 year of imprisonment;

- based on the factual circumstances, this measure is deemed necessary to establish the truth; and
- the use of measure is compliant with the principles of proportionality and subsidiarity.

c. Content data:

- *Retrieve content data from a seized/seizable computer system in an **open** investigation (art. 39bis BCCP):*

A police officer can execute a search on a computer system/device if legally seized (when executing a house search, situation of red-handedness, …).
The prosecutor can order a search of a computer system/device in an open investigation if the computer system is seized or can be seized (for example: in an internet café or bank. When it is not reasonable to seize, the prosecutor can order the search without seizing). If a house search has to be done in order to reach the computer system, the investigating judge will be in charge.
This measure can be ordered for any type of crime. Remote search is however not possible.
Conditions and safeguards are put in place: the responsible/user of the computer system is informed in due time, special safeguards for lawyers and medical professions, the prosecutor is responsible for assuring the integrity of the evidence.

- ***Remote** search in a computer system in an **open** investigation (art. 88ter BCCP):*

The investigating judge can order in an open investigation the remote search in a computer system if this is necessary in pursuit of the truth and if other measures would be disproportional. The search can only be granted within the access possibilities of the user of the computer system. If the electronic evidence is stored abroad, the data can only be copied. Conditions and safeguards are in place.

- *Legal hacking and data interception (also remote) in a **covert** investigation (article 90ter BCCP):*

Only an investigating judge can request the interception of content data and legal hacking, solely for criminal acts as listed exclusively in §2 of article 90ter BCCP (a list of 45 crimes).
Further, the following conditions have to be fulfilled:

- there are serious and precise indications and facts available to believe that it concerns one of the listed serious offences for which this measure is possible (for example terrorism, human trafficking or murder);
- based on the factual circumstances, this measure is deemed essential to establish the truth;
- there are precise indications that the target of the interception is a suspect or a person who is regularly in contact with the suspect; and
- the measure is compliant with the principles of proportionality and subsidiarity.

Conditions and safeguards are put in place for documents from lawyers and medical professionals, the integrity of the electronic evidence and the rights of defence.

8. Voluntary – disclosure

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

Article 32 of the Preliminary Title of the Belgian Code of Criminal Procedure stipulates that evidence is inadmissible only if:

- the law explicitly sanctions the disrespect of formal conditions by the inadmissibility of the evidence; or
- the irregularity committed puts into question the reliability of the evidence; or
- the use of the evidence would be contrary to the right of a fair trial.

Article 32.b of the Budapest Convention is fully respected. The prior written consent of the responsible (user) of the computer system makes all searched and seized data admissible. Council of Europe T-CY Guidance Note #3 on Trans border access to data (Article 32) is in that regard respected by Belgium.

Belgian law obliges service providers, hosting companies, mere conduit, …, to spontaneously preserve data on behalf of the public prosecutor and warn the public prosecutor, when they discover or are being notified that their networks or servers are being abused for criminal means (chapter XII of the Economic Law Code).

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

In Belgian law, only the obtaining of data by foreign authorities by means of judicial cooperation, i.e. mutual legal assistance or European investigation order, is stipulated. The Belgian Law of 13 June 2005 on electronic communication, explicitly stipulates which authorities are competent to directly request data from a provider. Foreign authorities are formally not included in this list.

However, Belgium complies with article 18.b of the Budapest Convention and direct cooperation between Belgian hosted OSP's and foreign authorities are not excluded, but they will be reluctant to collaborate in some cases without notifying the Belgian judicial authorities and asking permission.

9. Data retention periods (including procedures for extensions)

Based on art. 126 of the Belgian Law on electronic communication , a **data retention** period of 12 months is applicable for subscriber, traffic and location data.

As to **access to data**, different regimes are applicable, depending on the criminal offence for which access to the data is requested. These regimes can be found in the Belgian Code of Criminal Procedure:

- Subscriber data – art 46bis:
    1. Access to data up to **12 months** prior to the decision: the public prosecutor can order access to subscriber data up to 12 months prior to this decision for criminal offences, punishable with imprisonment of more than one year.
    2. Access to data up to **6 months** prior to the decision: the public prosecutor can order access to subscriber data up to 6 months prior to this decision for criminal offences, not punishable with imprisonment of minimum one year or a heavier sentence.
- Traffic and location data – art 88bis (§2):
    1. Access to data up to **12 months** prior to the decision: the investigating judge can order access to both traffic – and location data up to 12 months prior to this decision for criminal offences with a terroristic motive as defined in art 137 §2 & §3 of Belgian Criminal Code.
    2. Access to data up to **9 months** prior to the decision: the investigating judge can order access to both traffic – and location data up to 9 months prior to this decision for:
        - criminal offences as described in art. 90ter §2-§4 (excluding crimes with a terroristic motive) as well as ;
        - criminal offences committed in the context of a criminal organisation (as defined in art 324 of Belgian Criminal Code) and ;
        - criminal offences that are punishable with imprisonment of minimum 5 year or more.

    3. Access to data up to **6 months** prior to the decision: the investigating judge can order access to both traffic – and location data up to 6 months prior to this decision for criminal offences punishable with imprisonment of at least one year or a heavier sentence.
    4. No access to data: for criminal offences punishable with imprisonment of less than one year, ordering access to traffic – and location data, based on art 88bis, is not possible.

10. Procedure for data preservation/execution deadline

Articles 29 and 30 of the Budapest Convention are fully implemented in article 39quater of Belgian Criminal Code of Procedure. Preservation requests in the framework of the 24/7 network can be made

to the Belgian Federal Computer Crime Unit (FCCU) which is the SPOC and which is reachable 24/7 at DJSOC.FCCU.Perm@police.belgium.eu. Preservation is done in real time.

11. Procedure for data production/ execution deadline

The procedure for data preservation and production is described under titles 3 to 7 and 10. Preservation is done in real time through the 24/7 SPOC. The obtaining is done through MLA or an EIO or - in agreement - based on spontaneous information sharing.

12. Concise legal practical information

Every measure is duly described above. The Belgian judicial and police authorities are open to look for any possible international cooperation and assistance and to look into adequate solutions for specific concerns flagged by our counterparts in other (Member) states.

However, a brief description of the case, the necessity for the obtaining of the data and an indication of the sense of urgency would be useful. Moreover, every request should at least contain all necessary technical information needed to execute the request.

If possible we advise to send an advanced copy to and have prior contact with the executing judicial authorities or LEA's.

On a police level, the 24/7 SPOC can be addressed. On the judicial level, the Belgian Federal Prosecutor's Office has a unit devoted to facilitate swift international cooperation. Advise or guidance can be sought there: Secretariat.International@just.fgov.be

The contact points of the European Judicial Network may also be contacted.