EUROPEAN JUDICIAL NETWORK

EJN Fiches Belges on electronic evidence
www.ejn-crimjust.europa.eu

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:

e. Reciprocity
f. Spontaneous information (Art. 26 Budapest Convention)
g. Trans-border access (Art. 32 Budapest Convention)
h. Spontaneous information (Art. 7 EU Convention)

3. Procedure for obtaining electronic evidence

a. National procedures

In general criminal investigations and prosecution procedures are regulated in the the Dutch Code of Criminal Procedure (Wetboek van Strafvordering, DCCP). 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 the Netherlands is that the crime allows pre-trial detention, which is generally the case for crimes carrying a maximum of at least four years' imprisonment (art. 67, para. 1 under a DCCP), and for certain specifically mentioned offences (art. 67, para. 1 under b DCCP). Because digital investigation powers may also be required for "simple" cyber crimes, for example hacking without aggravating circumstances, the Computer Crime Act II has inserted almost all cyber crimes specifically into art. 67, para. 1 under b DCCP. As a result, for most cyber crimes, pre-trial detention is allowed, regardless of their maximum penalty, and most investigation powers can be used to investigate them.

In January 2006 the Data Production Orders Act (Wet bevoegdheden vorderen gegevens) enacted several powers to order the production of data. The powers were placed in the DCCP. The powers make a distinction of identifying data, other data and sensitive data. The orders can

be given to persons who process the data in a professional capacity; an order for "other" stored data and sensitive data can, however, also be directed at persons who process data for personal use.

According to art. 126nc DCCP identifying data can be ordered by an investigating officer in case of a crime (not a misdemeanor). Identifying data are name, address, zip code, date of birth, gender, and administrative numbers. In the case of international legal assistance, data mostly can be ordered by a public prosecutor, so that a judicial request from the issuing state is required often.

According to art. 126nd/ng lid 1 DCCP other data can be ordered by the public prosecutor in cases for which pre-trial detention is allowed. Moreover, future data can also be ordered, including – in urgent cases and with permission of the investigation judge – real-time delivery of future data, for an extendible period of four weeks (art. 126ne DCCP). This enables law enforcement officers to require production of all data that will come into being in future weeks.

According to art. 126nf DCCP sensitive data can be ordered by the investigation judge in case of a pre-trial detention crime that seriously infringes the rule of law. Sensitive data are data relating to religion, race, political or sexual orientation, health, or labor union membership.

Stored (content) data at a public telecommunications provider may only be ordered with consent of a judge (art. 126ng, para 2 DCCP).

In order to obtain user data art. 126na DCCP provides for an investigating officer the possibility to order a communications service provider, in case of a crime, to produce user data (if possible, because of reseller constructions). User data are name, address, telecommunications number, and type of service. Art. 126n DCCP, concerning traffic data (infra), also comprises the collection of user data. Other information pertaining to the identity of a person may be ordered under art. 126nc DCCP.

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:** to obtain (basic) subscriber information
- **Dutch (judicial) 24/7-channel/network (Budapest Convention):** 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)
- **Article 18 Budapest Convention:** on a voluntary basis (most companies established in the Netherlands supply, however, only on the basis of a request for judicial assistance – to cover themselves against the customer and because of GPDR-issues)
- **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

Public prosecutor's office. The competent authorities are the regional International Legal Assistance Centres (the IRCs) and the National Legal Assistance Centre (LIRC).

Besides the LIRC is AIRS (the Central authority for requests from non-EU states) also a competent authority to receive requests (MLA).

6. accepted languages

Dutch, English

Otherwise: One of the official languages of the Council of Europe, but preferably in English or German or a translation in the Dutch language.

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.

Tresholds: because of many reseller-constructions within the businesses of hosting providers, this data is often in possession or control of the (foreign) reseller. The service provider established in the Netherlands regularly has no access to these subscriber information. If the issuing state gives explicit permission (because of risk of damage by an unreliable reseller and given the confidentiality), we can ask (with a Dutch claim/warrant) the reseller to cooperate and provide subscriber data on voluntary basis. Any necessary certificates of authenticity of business documents will also be sent to the reseller. Cooperation depends of the reseller in question (mainly good experiences).

- **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: logfiles: date, time, duration, route, date, time of use).

Tresholds: in the absence of a data-retention obligation in the Netherlands, it depends of the (systems and settings of the) service provider whether there is any logging information (logfiles) available, for what purpose (billing) and for what period. Most service providers don't have logfiles available. If they have it, service providers tend to keep those records mostly for a short time (varying between 30 and 90 days).

Depending on the available traffic data (with or without content included), permission to obtain/tap the data is needed of the examining magistrate. For non-EIO countries permission of the court is sometimes required to provide the obtained data.

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

Tresholds: because of this intrusive measure (and invasion of privacy), content data can only be obtained by serious offences (preventive custody allowed for any criminal offence with a 4 year prison sentence) and if proportionate. An explanation from the issuing state with regard to the necessity of content in relation to the investigation is requested.

Not all content is located on Dutch servers or is not always accessible by the service provider. In many cases, the cooperation of the resellers is required, so that the service provider in the Netherlands can indicate the physical location of the server (which rack) for creating an image. In the case of VPS servers, the resellers often has to cooperate in order to obtain the content through providing a download link (snapshot). In these cases, explicit permission from the issuing state (because of the risk of damage by an unreliable reseller and given the confidentiality) is required to ask the reseller (with a Dutch claim/warrant) to cooperate. Any necessary certificates of authenticity of business documents will also be sent to the reseller. Cooperation is voluntary and depends on the reseller in question (mainly good experiences).

8. Voluntary-disclosure:
   a. As issuing state: Admissibility of the electronic evidence obtained by voluntary disclosure. Admissible, if the conditions of subparagraph (b) below are fulfilled (the service provider abroad has access to the subscriber data and provides also services in the Netherlands, and if there is no violation of sovereignty).

   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. Only on a voluntary basis (in the light of article 18 Budapest Convention), no enforcement action will be taken. Only in cases where it concerns subscriber information, of a service provider established in the Netherlands, requested by a judicial authority of another contracting party, and when the service provider has also access to these data. Without infringing the sovereignty of the other contracting party.

      Treshold: because of many reseller constructions in the Netherlands, in most cases the service provider doesn't have actually access to the data or can't easily breach the contract with the customer, so that a MLAT is required to provide the data and ask the reseller – with permission of the issuing state – to cooperate and give access to the data (also on voluntary basis).

9. Data retention periods (including procedures for extensions)

No mandatory retention system. Providers differ in their business processes when it comes to (the term of) keeping records for their administrative and, or, billing purposes.

10. Procedure for data preservation/execution deadline

Because of many reseller-constructions the service provider often don't have access to the data. In such a case the Dutch authorities don't preserve/freeze the data, but demand the requested data, by sending a claim to the service provider or reseller (after permission of the issuing state because of potential risk of damage).

The authorities in the Netherlands can not compel the service provider or reseller and enforce such a request. If the reseller abroad is non-cooperative, the (L)IRC will advise the issuing state to send an EIO/MLAT to the country where the reseller is located.

Execution deadline: the deadlines mentioned in the Budapest Convention or the EU Directive 2014/41/EU (EIO).

11. Procedure for data production/ execution deadline

The procedure for data production is the same as data preservation; see answer question 10. As explained, due to the many reseller-constructions, the public prosecutor's office immediately secure/demand the available requested data, where possible and with permission of the issuing state by contacting the reseller abroad.

Execution deadline: the deadlines mentioned in the Budapest Convention or the EU Directive 2014/41/EU (EIO).

12. Concise legal practical information

The measure has to regard available (and regularly volatile) subscriber information, traffic data or content of service providers, established or offering services in the Netherlands, that are used for:

- communication purposes (including providers of telecommunications services and other electronic communications services, including interpersonal communications services);
- information society services that facilitate interactions between users and that are used for the storage of data (including online marketplaces that facilitate peer-to-peer transactions and providers of cloud computing services);
- and for providers of internet infrastructure services (including registries that assign domain names and IP addresses important for the functioning of the internet).

Furthermore the public prosecutor can choose another measure then asked for in the EIO (or previous 24/7), if the requested measure does not exist in Dutch law or would not be applicable or proportionate.

It is important to thoroughly explain the necessity for the measure in relation to the investigation, in particular for content requests (to obtain permission from the examining magistrate).

A 24/7-request should include (to send a claim to the service provider):

- which specified stored computer data need to be seized (subscriber/traffic or content);
- period of interest of the requested data (subscriber/traffic);
- in case of content data: the necessity for the preservation in relation to the investigation;
- IP-address with timestamp;
- a sufficient description of the case (‘modus operandi’, (un)known suspect, date on which the offence was committed, damage/scale/size of the case (consequences victims);
- any available information identifying the custodian of the stored computer data or the location of the computer system;
- MLAT-guarantee (that the party intends to submit a MLAT/EIO);
- In case of a reseller-construction: explicit permission of the issuing state to proceed with the execution (to contact the reseller to obtain the requested data) despite possibly risk of damage.