EUROPEAN JUDICIAL NETWORK

Fiches Belges on electronic evidence

ITALY

1. Definition of electronic evidence

The Italian system does not define what "electronic evidence" is in general. This concept is not even legally defined in the CoE Convention on Cybercrime, where only "computer data" are defined, although the definition above is useful to understand what "digital evidence" is. We retrieve the definition of "digital evidence" from the practice and doctrine. According to the CoE electronic evidence guide, which represents a valid point of reference on this matter: "digital evidence is an information generated, stored or transmitted using electronic devices, that may be relied upon in a trial".

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)

3. Procedure for obtaining electronic evidence

a. National procedures

The discipline for the collection of electronic evidence is outlined, in general, in the criminal procedure code, whilst a special regime is foreseen for the telecommunication providers in a separate law text (Legislative Decree no 196/2003).
As general rule, there are not threshold for the collection of stored electronic evidence, depending on the seriousness of the crime investigated. All the legal tools provided for by the CPC and Legislative Decree no 196/2003, are suitable for all the offences. Only regarding the real-time gathering of digital evidence (interceptions) threshold are envisaged in the CPC.

According to the CPC digital evidence may be collected *ex officio* by the Judicial Police in case of urgency, where the intervention of the Public Prosecutor may jeopardize the collection of the digital evidence or when the sensitiveness of the data sought is low (subscriber data) and an order of the Prosecutor or of the Judge is not required.

As per the power of the Judicial Police in case of urgency, Articles 352 and 354 CPC respectively provide as follows.

Article 352 CPC. In case of *flagrante delicto* or in case of escape, if criminal police officials have reasonable grounds to believe that data, information, software or traces anyhow related to the offence which may be deleted or lost are hidden in IT or electronic systems, they shall search them, even if they are protected by security measures. In these cases, criminal police officials shall adopt technical measures aimed at guaranteeing the preservation of original data and preventing their alteration.

Article 354 CPC is dedicated to urgent verification on the spot by the Judicial Police. It foresees that "If there is a danger that the objects, traces and the scene… may be altered, lost or anyhow modified and if the Public Prosecutor is not able to intervene promptly or has still to undertake the management of the investigations, criminal police officials shall carry out the necessary ascertainments and checks on the conditions of the scene and objects thereof. **In relation to data, information, software and IT or electronic systems, criminal police officials shall also adopt the technical measures or establish the obligations necessary to ensure their preservation and prevent them from being altered or accessed and, if possible, take care that they are copied on appropriate media, following a procedure that ensures that the copies are identical to the original and that they cannot be modified**".

In both of the cases, when the Judicial Police search and seize electronic evidence, those acts should be validated by the Prosecutor within a strict time limit.

Regarding the power assigned to the Public Prosecutor during the investigation phase, he/she may carry out or delegate the Judicial Police to carry out inspections (Article 244 CPC), searches (Article 247 CPC) and seizure (Article 253 and 254-bis CPC), or may issue a production order to professionals (like lawyers, medical doctors, etcetera) and public officials (Art. 256 CPC).

Inspection (Article 244 CPC). The judicial authority may order that inspection be performed by means of descriptive and photographic tools and any other technical operation, **also by means of computer or electronic tools, by adopting technical measures capable of guaranteeing the preservation of the original data and preventing their alteration.**

Search (Art. 247 par. 1-bis CPC). If there are reasonable grounds to believe that **data, information, software or any other traces relating to an offence are stored in a computer or electronic system, even if protected by security measures, a search shall be ordered adopting technical measures capable of guaranteeing the preservation of the original data and preventing their alteration.**
Before initiating the search, the judicial authority or the delegated judicial police may invite the person present in place to hand over the searched items. In this case the search may not be carried out (Article 248 CPC).

Seizure (Article 253 CPC). It relates to every object which come into consideration as *corpus delicti*, as well as other material items related to the offence necessary to ascertain the facts of the case. **This provision covers also the seizure (following or not to a search) of data stored in a computer system, electronic devices or storage medium**. Article 254-bis CPC outlines a specific methodology to be followed when the seizure concerns computer data stored by IT providers or Telecommunications providers. The general rule is to take a faithful and not alterable copy of the data and put it on a device.

Production order (Article 256 CPC). It concerns only the order directed to persons exercising a certain profession or public officials and persons entrusted with a public service, who must, upon the order of the Judicial Authority (Public Prosecutor during the investigation phase) to **hand over data, information or software, also by copying them on a suitable medium**, except if they declare in writing that they are covered by either State, public service or professional secret.

Internet service providers and telecommunications service providers

Only with reference to telecommunication service providers a special regulation is provided for by Article 132 Legislative Decree no 196/2003 (Personal Data Protection Code), concerning traffic data: during the investigation phase the Public Prosecutor is entitled to gather traffic data stored by the service providers ("*the data may be acquired from the provider by means of a **reasoned order issued by the public prosecutor** also at the request of defence counsel, the person under investigation, the injured party, or any other private party*").

Although the special regulation refers only to traffic data, also content data, if stored by the service providers and with the exclusion of phone calls and SMS (which are not stored), could be gathered by the Prosecutor by means of a reasoned production order issued according to Article 256 CPC or a seizure order issued according to Article 253 and 254-bis CPC.

As per subscriber data, as mentioned above, they may be collected even by an order issued by the Judicial Police in relation to a criminal investigation.

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.** Service for International Police Cooperation (SCIP) within the Ministry of Interior: it is an inter-force police central structure, which receives and forwards the requests for police cooperation at international level. Subscriber data may be requested through this channel without issuing a MLA request or EIO to obtain **(basic) subscriber information**.
- **Italian 24/7-channel/network (Art. 35 Budapest Convention).** By declaration on 19 June 2009 Italy designated as Italian 24/7 channel/network the following structure: Servizio di Polizia Postale e delle Comunicazioni, whose address is Rome, Via Tuscolana no 1548 and e-mail htemergency@interno.it. That structure is only dedicated to urgent preservation requests aimed at gathering subscriber/traffic/content data (the available data will be preserved for a time limit of 90 days, suitable to be prolonged up to a maximum of 6 months). A MLA request or EIO is needed in order to gather traffic and content data. Subscriber data may be obtained even through direct police cooperation channel. The 24/7 network provided for by Art. 35 of the Budapest Convention is integrated with the 24/7 Network established by G7 High Tech Crime Sub Group (HTCSG) of the Rome-Lyon Group of G7 Countries.
- **EIO or MLAT requests (Art. 31 Budapest Convention).** CoE Conventions and EU treaties; UN Treaties and bilateral treaties. Subscriber data, traffic data and content data may be collected by accessing, seizing or anyway gathering the data by issuing the relevant order by the competent executing authority.
- **Trans-border access to stored computer data with consent or where publicly available (Art. 32 lett. b) Budapest Convention).** Collection of stored electronic data on a voluntary basis is always possible under the conditions outlined in Article 32 lett. b) of the Budapest Convention. Italian operators in most of the cases require an order issued by a judicial authority (Prosecutors or Judges) in order to disclose the data. For subscriber data, instead, usually they disclose them upon a request by the Judicial Police.

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

Directive 2014/41/EU. The European Investigation Order (EIO) Directive was implemented in the Italian law as of July 2017 by the Legislative Decree no 108/2017.

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 (20 April 1959) and its Additional Protocols;
- many other bilateral and multilateral treaties;
- Budapest Convention (Article 27) when no other Convention or Treaty is applicable.

5. Competent authority to receive and execute your request

District Prosecutor Office (i.e. the Prosecutor Office attached to the Court of first instance of the main city of the Court of Appeal District).

6. Accepted languages

Italian.

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

The definition is envisaged in the Budapest convention: "Any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a) the type of communication service used, the technical provisions taken thereto and the period of service;

b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement".

Examples:

- user's account or login name;
- user's name, vanity name;
- user's telephone number or numbers;
- user's email address;
- Internet Protocol (IP) address used for registration, day and time frame, and MAC address;
- billing information;
- date and time of password/contact details change;
- IP address used for the change of password/contact details.

The definition covers any other information pertaining to the identity of the subscriber, including, but not limited to billing information (including type and number of credit cards, or other identifying information).

Traffic data

As envisaged in the Budapest Convention, the definition of Traffic data refers to any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Traffic Data is the information that includes records identifying with whom a user communicated with, what websites a user visited, and similar information about a user's online activity, including all IP addresses used to log into the account, session times, dates and durations.

Types of specific datasets considered to be Traffic Data may include, but are not limited, to:

for E-mail or Web Hosting Accounts:
- destination or source of connection with timestamps; disconnect time and date; method of connection to system; data transfer volume and other routing information;
- e-mail header including source and destination, the date, time, and data volume;
- metadata of images or other documents uploaded to the account, and the sizes of the files (not including the content);
- accounts that accessed a specific file or webpage on a specific timeframe;

for Social Media and online messaging services:
- applications;
- connection logs;
- notification settings;
- privacy settings/blocks;
- machines/Cookies;
- websites;
- subscribed to;
- pokes;
- activity log.

Content data
The definition is in the Budapest Convention, or better in the explanatory report to it. Paragraph 209 of the Explanatory Report to the Convention on Cybercrime states that Content Data "refer to the content of the communication; i.e. the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)".
Hence, Content data usually relate to the information sent in an e-mail, via a social media account or communication service, as well as data stored in a cloud or in remote computing services from the sender to the recipient.

Content Data category includes, but is not limited, to:
- written messages;
- embedded photographs or images;
- video files;
- attached files;
- posts;
- purchase history.

It is worth to stress that Content data consisting in phone communications (voice and SMS) are not available. In order to gather them a phone interception in real-time is required.

8. Voluntary-disclosure

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

According to the Italian CPC, as modified according to Article 32 letter b) of the Budapest Convention, electronic documents and data stored abroad may always be gathered. If such data are not publicly available, they shall be gathered upon consent of their lawful owner (Art. 234-bis CPC).

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.

It is always possible for the OSP located in Italy to disclose data (according to Articles 18 and 32 of the Budapest Convention) on a voluntary basis, even though usually OSPs require an order to disclose them.

9. Data retention periods (including procedures for extensions)

A mandatory data retention period is established only for traffic data regarding Internet service providers and telecommunication service providers, while the other operators are free to choose their own policy on data retention of computer data.
For the first ones, the legal regime may differ depending on the seriousness of the crime investigated. On this regard the standard regime is ruled by Art. 132 Legislative Decree no. 196/2003 (Personal Data Protection Code), according to which the retention period is as follows:

a) telephone traffic data: 24 months;
b) unsuccessful/missed calls traffic data: 30 days;
c) electronic communications traffic data: 12 months.

When the crime investigated is one of those included in the list below, all the time-periods above are extended to 72 months (Art. 24 Law no 167/2017):

1) crimes referred to in Articles 285 (devastation), 286 (civil war), 416-bis (mafia-type criminal organization) and 422 (massacre) of the Criminal Code; 291-ter (smuggling of tobacco products), limited to the aggravating circumstances provided for in letters a) d) and e) of paragraph 2, and 291-quater (association aimed at smuggling tobacco products) paragraph 4 of the Consolidated Text approved by Decree No 43 of the President of the Republic of 9 October 1973;
2) completed or attempted crimes referred to in Articles 575 (homicide), 628 paragraph 3 (aggravated robbery), 629 paragraph 2 (aggravated extortion) and 630 (kidnapping for extortion scope) of the Criminal Code;
3) crimes committed making use of the conditions provided for in Article 416-bis of the Criminal Code (mafia-type criminal organization), or crimes aimed at facilitating the activity of the associations provided for in the same Article;
4) crimes committed for purposes of terrorism or subversion of the constitutional system which are punishable by law with the penalty of imprisonment for a minimum term of at least five years or a maximum term of at least ten years, as well as crimes referred to in Articles 270 paragraph 2 (subversive association) and 306 paragraph 2 of the Criminal Code (armed gang);
5) crimes concerning the illegal manufacturing, selling, cession, possession and carrying in a public place or a place open to the public or introduction into the State of weapons of war or war-like weapons or parts thereof and explosives, illegal weapons as well as ordinary fire arms, except for those provided for in Article 2 paragraph 3 of Law no 110 of 18 April 1975;

6) crimes referred to in Articles 73, limited to the aggravating circumstances provided for in Article 80 paragraph 2 (huge quantity), and 74 (association aimed at smuggling drugs) of the Consolidated Text of the laws on narcotic or psychotropic substances, prevention, treatment and rehabilitation of the related states of drug addiction approved by Decree No 309 of the President of the Republic of 9 October 1990, as afterwards amended;
7) crime referred to in Article 416 (criminal organization) of the Criminal Code in the cases requiring mandatory arrest in *flagrante delicto*;
8) crimes provided for in Articles 600 (reduction to slavery), 600-bis paragraph 1 (exploiting prostitution of minors), 600-ter paragraphs 1 and 2 (child pornography), 601 (traffic in human beings), 602 (purchasing or selling of slaves), 609-bis in the aggravated circumstances provided for in Articles 609-ter, 609-quater, 609-octies (aggravated or gang sexual assault) of the Criminal Code, as well as crimes provided for in Article 12 paragraph 3 (smuggling of human beings) of the Consolidated Text referred to in Legislative Decree no 286 of 25 July 1998, as afterwards amended.

10. Procedure for data preservation/execution deadline

A dedicated procedure and regulation is provided only for preservation of traffic data regarding Internet service providers and telecommunication service providers, according to Article 132 paragraph 4-ter Legislative Decree no 196/2003 (Personal Data Protection Code):
"*The Minister of Home Affairs or the heads of the central offices specialising in computer and/or IT matters from the State Police, Carabinieri and the Financial Police …, where delegated by the Minister of Home Affairs, may order Internet service providers and telecommunications operators to preserve and protect electronic traffic data, except anyway for contents data, …* ***for no longer than ninety days, also in relation to requests lodged by foreign investigating authorities****.* ***The term*** *referred to in the order in question* ***may be extended****, on grounds to be justified,* ***up to six months*** *whilst specific arrangements may be made for keeping the data as well as for ensuring that the data in question are not available to the IT and/or Internet service providers and operators and/or to third parties*".
It is worth to note that shall be notified in writing without delay, and in any case by forty-eight hours as from service on the addressee(s), to the public prosecutor that is competent for the place of enforcement, who shall endorse them if the relevant preconditions are fulfilled. The measures shall cease to be enforceable if they are not endorsed.
Within the original or extended preservation time limit the EIO or a MLA request should be issued, transmitted and executed.

It is worth to stress out that a similar procedure is not provided for operator other than those specified above. That implies that a request coming from a foreign investigative authority aimed to freeze computer data hosted by a company (not an internet service provider or telecommunication service provider), will not be executed in that way. At this purpose is needed an order issued by the competent Judicial Police.
A practical arrangement could consist in using information provided by a foreign investigation authority via law enforcement channels (i.e. Interpol, Europol, 24/7 Network) or via Eurojust to open a case in Italy, in order to use a search and seizure order issued by the Public Prosecutor and preserve electronic evidence.

11. Procedure for data production/execution deadline

As per the production of data, the execution of the MLA request or EIO will be carried out through:

1) a reasoned production order issued according to Art. 132 Legislative Decree no 196/2003 or Art. 256 CPC by the competent Public Prosecutor when dealing with traffic data stored by Internet service providers or telecommunication service providers;
2) search and/or seizure order issued by the competent Public Prosecutor in order to gather available content data or when traffic data do not regard internet service providers or telecommunication service providers.

Subscriber data, when not collected through police international cooperation channels, may be gathered through one of the two tools specified above.
Specific formalities required by the requesting authority to be observed during the execution, shall be followed if compatible with the fundamental principles of Italian law.

Execution deadline: the deadlines mentioned in the Budapest Convention or in the Directive 2014/41/EU (EIO), as implemented by Legislative Decree no 108/2017.

12. Concise legal practical information

//