Electronic evidence in criminal cases: proper handling and admissibility

Brussels – the Hague, 26.04.2022

AGENDA

- What is electronic evidence?
- Proper handling of electronic evidence and lifecycle of electronic evidence
- Admissibility
- Chain of custody

Electronic Evidence v. Digital Evidence

- *Electronic Evidence* is any data resulting from the output of an analogue device and/or a digital device of potential probative value that are generated by, processed by, stored on or transmitted by any electronic device.

- *Digital Evidence* is that electronic evidence which is generated or converted to a numerical format.

- In general, most definitions seem to summaries that electronic or digital evidence is electronic or digital data that can be used to help establish (or refute) whether a crime has been committed

Subscriber, Traffic and Content information

- *Subscriber*, *traffic* ("transactional information") and *content information (data)* defined by the *Budapest Convention on Cybercrime* and Art 1.d and Explanatory Report to the Council of Europe Convention on Cybercrime, Chapter II, Title 5.

- These notions are also defined through Article 2 of the European Commission *Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters.*

- https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF

Stored data

- Information that is already **stored on the servers** of the Internet Services Providers (ISP), before the request (MLA or exchange of information):
  - **Basic Subscriber Information (BSI) –** contains the IP address of the first login, the name of the subscriber/user and may include the time - how long the subscriber has used that specific service
  - **Traffic Data** known as transactional information/data show when users logged into their account, who they sent a message to, when they sent it and where they sent it from
  - **Content Data -** the body or text of an email, message, blog or post

Real-time communications

- Information that is no yet stored on the servers, but that investigators and prosecutors hope to obtain in real time, for instance the time (when) and the location (from where) a terrorist logs in to his/her account.

  - **Traffic Data** - Interception of whom a subject is contacting and where from (IP address)

  - **Content Data** - Interception of the body or text of an email message, blog or post

DIGITAL EVIDENCE

STORED E-EVIDENCE	
BASIC SUBSCRIBER INFORMATION - BSI	Information on the identity of the subscriber/user, address, IP address of the first login, billing and payment information, any other information on the site of the installation of communication equipment, how long the service has been used. Art. 18. n. 3 Budapest Convention
TRAFFIC DATA – NON CONTENT DATA	Any computer data relating to a communication indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service – ex. IP or MAC addresses (metadata), access logs, transaction logs. Art. 1. al. d) Budapest Convention
CONTENT DATA	Body or text contained in the communication, such as an e-mail, post, image, video...
REAL TIME GATHERING OF E-EVIDENCE	
TRAFFIC DATA	Interception of who the suspect is contacting and where from – ex. with reference to IP addresses. Art. 20. Budapest Convention
CONTENT DATA	Interception of the body or text contained in the communication, e-mail text, post, image, video... Art. 21. Budapest Convention

Why it is so puzzling to deal with e-evidence?

- Fragmentation: definitions of e-evidence at domestic, European and international level
- Possible wide descriptive perspective to include digitized evidence
- Different legal approaches: general or specific principles and rules on collection, exchanges and probative value

Instruments for gathering cross border evidence

- EIO
- MLA
- Direct access; extraterritorial application of domestic decision

Further issues of ELECTRONIC EVIDENCE

- **Volatility vs MLAs**

The format and procedures involved in mutual legal assistance treaties are not suitable for the volatility of electronic evidence. Why?

- **Extraterritorial application of coercive powers**

CAN LEAs force the disclosure of communications data and/or the simultaneous interception of data in transit when data are stored abroad?

Handling of electronic evidence (1)

- Maintaining the integrity of electronic evidence throughout the process of examination presents different problems from those encountered when handling traditional physical or documentary evidence
- If relevant information are contained in seized media the forensic procedures used to examine that media must not alter the evidence (since it was seized). After seizure, ensuring that the traditional **chain of custody remains unbroken is necessary but not sufficient** to establish the authenticity of the data or evidence obtained from the forensic examination. In addition to the traditional chain of custody, **auxiliary precautions** may be required for handling electronic evidence.

Handling of electronic evidence (2)

- Tools recognized by the forensic community should be used in the recovery of electronic evidence from the source or the media
- The process used to acquire the data is itself electronic
- Both the evidence and the process may be subject to **legal challenges**
- Additional expertise may be required to authenticate the machine, applications, and forensic tools

Life cycle of electronic evidence: PRESERVATION

- Expedited preservation of data prior to MLA
- Possible live forensics to ensure potential evidence is not lost when switching off a device
- Tools used for live forensics may modify the computer system and the electronic forensic examiner must be able to explain the potential impacts of such modifications on the electronic evidence

Provide complete chain of custody

FOUNDATION FOR THE EVIDENCE 1

Electronic evidence may have been intentionally or unwittingly altered before it was secured by LEAs. Evidence turned over to the prosecuting authorities for examination ultimately may not be useful without establishing the authenticity and chain of custody of the evidence

FOUNDATION FOR THE EVIDENCE 2

Prosecutors must show in court that the information obtained from the media is a true and accurate representation of the data originally contained in the media, irrespective of whether the acquisition was done entirely by law enforcement or in part or entirely by a civilian witness or victim

DOCUMENTATION

Document the date and time when the evidence was gathered (include a reference to time zone if necessary)

Careful documentation of each step of the life cycle of electronic evidence

Careful documentation will enable the prosecutor and the prosecution witnesses to demonstrate at trial how evidence was collected

Well-documented case is much more likely to result in a guilty plea, saving valuable prosecutorial and court resources

VALIDATION

- Validation procedure to ensure that the methods for the acquisition and analysis of electronic evidence are adequate for the purpose and fulfil the needs of the investigation
- The objective of the authenticity is foreseen by law but not how to get to it
- Different tools have different features and bring different results
- Challenges from the defence

Admissibility 1

In cross-border cases, when the evidence was collected under the rules of a different jurisdiction, the question rises if the evidence is admissible in Court

Admissibility 2

Some countries have specific best practices and practical guidelines (including technical procedures) that are used in practice in the collection, preservation and exchange of electronic evidence

Others countries do not have any publicly available information on operational guidelines or on specific codes of conduct

Admissibility of electronic evidence evaluated by complying with general rules on the collection of evidence. This includes rules that require the evidence to be collected in respect of certain procedural requirements and in a lawful manner, i.e. legal safeguards to avoid breach of fundamental rights.

Admissibility 3

- National legal frameworks set the standards
  - Also for voluntary direct cooperation with ISPs
  - Based on respect to international cooperation mechanisms

- Traditional rules need to be adapted to electronic environment
  - *Preservation of evidence*
  - *Role of forensic labs*
  - *Secure transmission*
  - *Authenticity and integrity of the evidence*

- **ALWAYS** under judicial control

Teresa Magno

Assistant to the National Member for Italy

tmagno@eurojust.europa.eu

+31 70 412 5205

www.eurojust.europa.eu

Follow Eurojust on Twitter and LinkedIn @ *Eurojust*