TREIO
TRaining on European Investigation Order

TRAINING STRATEGIES: WAY FORWARD AND TRANSFERABILITY OF OUTCOMES

25 JANUARY 2024

Teresa Magno

Assistant to National Member for Italy, Eurojust

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 882068

AGENDA

Specificities of TrEIO in addressing following issues and some future perspectives – Areas/topics relevant for training and skills developing purposes

- Legacy of COVID-19 pandemic
- Secure means of communication
- Digital court proceedings
- Regulation on the digitalisation of judicial cooperation: some issues of concern regarding these developments
- Electronic evidence
- Evaluation/assessment of electronic evidence
- Artificial Intelligence impacting Cross-border Digital Criminal Justice

ADDED VALUE OF TREIO

- Combined efforts of three projects - EXEC, EVIDENCE2e-CODEX and e-Evidence
- Useful and practical tailored made training (digital + legal components)
- Self paced e-learning course, eEDES similator of the EIO flow and full eCODEX infrastructure to provide realistic flows

FIRST RELEVANT STEP OF A LONGER JOURNEY

What's here/ahead?

-digitalisation

-exchange of judicial cooperation instruments in a digitalised way

-exchange of digital evidence (only via secure and reliable digital channels)

-use of artificial intelligence

-respect of rights of those concerned (private and family life/protection of personal data)

Topics and consequent needs constantly evolving (COVID 19 pandemic – digitalisation – technologies)

COM Communication on a European judicial training strategy 20-24

BROAD PICTURE 1

- COM Communication on a European judicial training strategy 20-24
- Regulation on the digitalisation of cross-border judicial cooperation and access to justice and the accompanying directive were adopted. They will facilitate electronic communication in the context of cross-border judicial cooperation procedures in (civil, commercial and) criminal matters
- The regulation refers to the creation, development and maintenance of a reference implementation software, in accordance with the principles of data protection by design and by default and with accessibility requirements. A level of security and interoperability which is appropriate for the exchange of information in the context of cross-border judicial procedures has to be ensured. (Interoperability with national IT systems has to be ensured as well)

BROAD PICTURE 2

- Secure data exchange between MSs judicial authorities and EU Agencies
- It is understood that this system of communication has to be mastered by the judiciary and/or administrative staff
- Effectiveness and efficiency of court proceedings can be enhanced by further digitalisation of Member States' judicial systems (digital tools used in court proceedings, electronic communication between parties, electronic transmission of documents, use of video-hearing and conferencing)
- Specific criminal phenomena: increase in offences involving cybercrime, online criminal activities and health (cyber attacks on sensitive infrastructures), new forms of terrorism and violent extremism

Training as a follow up action aimed at speeding up the digitalisation process and the use of digital services in the justice area

TRAINING ON INSTRUMENTS

When to use:

- EIO
- MLA
- European Preservation/production order

RELEVANT TRAINING TOPICS

- 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

Life cycle of electronic evidence

Documentation, validation and admissibility of electronic evidence

AI impacting cross-border cooperation

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 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 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

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

AI IMPACTING CROSS-BORDER COOPERATION

Biometric recognition and forensic analysis

Awareness of specificities of biometric recognition system

CCTV videos and images analysed by computer vision systems to identify victims in recorded or live-streamed media

Dedicated video/image enhancing algorithms developed to tackle the video quality issue (no live biometric recognition)

Mistakes and machine learning algorithms (narrowly defined application + good quality data – datasets may contain biases)

Awareness of deep fakes and identification of deep fakes

AI may have an impact of HRs: biases should not be embedded in evidence resulting from AI application; judiciary should be trained to recognise biases so that they are not introduced and proper action can be taken to avoid distorting the decision making process (judicial oversight to be supported and trained)

The nature of algorithmically generated results has to be understood by the prosecutor/judge (topics: what do the algorithms mean; what are their weaknesses; to what extent is it useful/dangerous to use?)

CONCLUSIONS

- Profound digital transformation of the field of justice
- Need to adapt to digital and secure communication channels
- Need to adapt to digital proceedings
- Consequential skills and critical thinking
- Awareness of the impact of digital technologies on the field of judicial cooperation in criminal matters
- Familiarity with the specificities of electronic evidence (no matter where collected)
- AI applications- Generative AI
- Training needs and consequential skills: can a TrEIO 2.0 help?

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*