



LAW ENFORCEMENT AGENCIES' DATA EXCHANGE WITHIN AND OUTSIDE THE EU

Judicial Cooperation: Practical and
Legislative Aspects

Challenges for Law Enforcement in the digital World

Digital revolution

- Increased need to secure electronic evidence in criminal proceedings
- Providers have their seat anywhere
- Data is stored anywhere
- Time limitations for data storage – no data retention for electronic communication data
- Gathering e-evidence more and more cross border nature
- Time consuming MLAT-procedure
- Seized amount of data makes it more difficult to find relevant evidence
- Lack of personnel resources

Current situation – production of traffic data

Prosecution service Vienna is conducting an investigation into an Austrian group of criminals selling drugs in Austria.

→ This group is using a local telecom provider to organise its criminal business. The prosecution service issues an order to produce traffic data. The local telecommunication provider is obliged to comply with the order under national law and will be subject to sanctions if it doesn't. The prosecution service will receive the data within several days.

→ This group is using an ISP established in the US to organise its criminal business. The prosecution service will have to submit an MLA request to the US and it will take 6 months before it can resume with the investigation.

What practitioners do to overcome the problems

- Investigations take longer or are even terminated at an early stage because MLA procedures are too lengthy
- In urgent cases sometimes voluntary cooperation is used:
→ legal basis/foreseeability? → Predictability of action by service provider? → No control by another authority apart from the investigating authorities?
- Countries that face an extraordinary number of requests for MLA have to find ways to reduce administrative burden (direct cooperation with service providers located on their territory already exists)
- Some countries refuse to grant MLA with regard to minor cases – problem: legality principle

Voluntary cooperation with international service problems

Recurring Problems

- No legal certainty for LEA/ISPs/user – rule of law!
- No standardised forms
- Content requirements for an order varies from ISP to ISP – national law is not taken into account
- Differences regarding confidentiality/user information
- In case of subsidiaries: where should data be sought by LEA?

New legislative approaches - EU

E-Evidence proposals

- Regulation and Directive
- Regulation = mutual recognition instrument regarding cross-border gathering of evidence
- Directive (legal base: internal market) to compel service providers to nominate a legal representative, if they conduct business in more than 1 MS irrespective of location of the SP's seat

Content of e-evidence Regulation

- Applicable to **electronic communication services, internet domain name and IP numbering services** and other **information society services** that provide possibility of communication between users or to process or store data on behalf of the user → a lot of SP
- For preservation/gathering of electronic evidence, namely **subscriber, access, transactional and content data** (no real time collection of data)
- Main feature: judicial authority of one MS issues Preservation/Production Order and submits it directly to SP located in another MS or legal representative of SP (see Directive)
- E-codex? Could play an important role in providing secure channels of communication and proof of authenticity of the order

Notification procedure

- Critical point of negotiations in the Council and in upcoming trilogue with EP
- Which MS should be notified?
- In which cases – for all or only for content data/ transactional data?
- What about purely national situations?

New legislative approaches – Council of Europe

- Negotiations on a 2nd additional Protocol to the Cybercrime Convention
- Convention is the one of the most important
- Ratified by currently 64 State Parties

Direct disclosure of subscriber information

- direct cross border cooperation with SP, but limited to subscriber data
- new definition of subscriber data, including “information needed for the purpose of identifying a subscriber of a service may include certain Internet Protocol (IP) address information” → may contain communication meta data under the law of some Parties → more sensitive data
- Possibility to make a declaration
- Again: notification procedure

Your views on use of notification procedures?

- Will it make MLA procedure more efficient and less burdensome?
- Will it protect fundamental rights equally good – considering the increasing amount of cross border situations and of notification procedures?
- Personnel resources?
- Other ideas/ are there alternatives?



Thank you for your attention!