MUNI
FI

Selected legal aspect of electronic evidencing

Pavel Loutocký

Intro?

- **The session will focus on the discussion of legal issues related to selected issues of electronic evidence and further related to cyber security. Current selected trends will be presented and problematic aspects will be discussed. So please feel free to prepare questions of interest as well!**

3 areas of legal regulation

1. **Civil law**
2. **Administrative law**
3. **Criminal law**

– **There is no explicit mentioning, how the evidence should look like**

Electronic evidence?

- **NO DEFINITION…**

- ***Evidence may be obtained by any means which may be used to establish the state of the case, in particular by examination of witnesses, expert opinion, reports and statements of authorities, natural and legal persons, notarial or executor's records and other documents, inspection and examination of the parties. If the manner of taking evidence is not prescribed, the court shall determine it.***

What is interesting in Civil Law

Section 562/2, Civil Code:

The records of data on legal transactions in the electronic system are considered reliable if they are made systematically and sequentially and are protected against alteration. If the record was made during the operation of the plant and is relied upon by the other party for its own benefit, the record shall be presumed to be reliable.

No such alternative in other areas of law, however INTEGRITY is the KEY!

Electronic documents?

- All the evidences are heavily related to the term of „electronic document“ and connected with „trust services“ = electronic signature, seal, timestamp etc.

- Incorporated in the regulation No 910/2014 on electronic identification and trust services for electronic transactions (eIDAS)

- Important:
  - Level of trust = qualified services, advanced tools, non-discrimination of electronic document
  - Archivation, integrity, preservance

Specific procedural approaches

Mainly in Criminal Law (Act on Criminal Procedure):

- **Interception (Sec. 88)**
- **Data Retention (Sec. 88a)**
- **Tracking people and things (Sec. 158d/3)**
- **Cooperation (Sec. 8/1)**
- **etc.**

Cybersecurity?

- Not so specific rules, we have to follow if it is private (civil) or public (administrative, criminal) agenda
- It depends always on the character of data
- Connected with „lawful / unlawful evidence“

Specifics and quality of data?

There is usually no legal rule on the demand on quality of data – it „just“ has to be correct and true (which can be part of poving – is the IS working properly or not?)

Some hints can be found for specific situations e.g. here:
Decree on the storage, transmission and disposal of traffic and location data (https://www.zakonyprolidi.cz/cs/2012-357)

MUNI
FI

Thank you for your attention!
Questions?

loutocky@muni.cz