Erasmus School of Law

Electronic documents

Service of Documents & Taking of Evidence Abroad: Judicial Training

Elena Alina Ontanu

5 February 2020
Ljubljana, Slovenia

Overview:

1. Electronic evidence
2. Electronic discovery/ disclosure
3. Electronic signature / keys
4. Evaluation of evidence

Erasmus School of Law

Electronic Evidence

Erasmus University Rotterdam

1. Electronic Evidence: An Introduction

- Usually not defined
- Civil procedural & criminal codes specifically refer to electronic documents or other digital materials => National legal frameworks are divergent among jurisdictions
- EU Competition law Directives (2019/1 & 2014/104) refer to type of electronic documents or documents/objects containing information irrespective of form they have
- Guides (EU & Hague Conference)
- Comprehensive international framework is lacking
- Private initiative for a Convention on Electronic Evidence (draft published in 2016)
  - ✓ Pursues a common policy as regards electronic evidence: promoting the understanding of electronic evidence, fair & adequate proceedings, & international cooperation
  - ✓ Definitions, proposes rules on admissibility & authentication of electronic evidence
  - ✓ Best evidence (common law concept referring to the original document – proof of authenticity)
  - ✓ Digital evidence practitioners
  - ✓ Use of good practices guidelines
  - ✓ Treatment of electronic evidence

1. Electronic Evidence: Definition (1)

- Council of Europe **Convention on Cybercrime** (Budapest Convention) refers to 'evidence in electronic format'
- **IBA Evidence Rules** (2010): 'documents' broadly defined (include electronic documents)
  - ✓ 'a writing, communication, picture, drawing, program or data of any kind, whether recorded or maintained on paper or by electronic, audio, visual or any other means'
- **eIDAS Regulation** (Reg. (EU) No 910/2014) defines 'electronic document'
  - ✓ Art. 3(35): 'any content stored in electronic form, in particular text or sound, visual or audiovisual recording'
- **Private Damage Directive in competition law (**Dir. (EU) 2014/104) defines evidence broadly
  - ✓ Art. 2(3): including electronic documents
- **Directive making competition authorities more effective enforcers** (Dir. (EU) No 2019/1) refers to the use of electronic evidence if this is considered relevant
  - ✓ Art 32: 'electronic messages, recordings and all other objects containing information irrespective of the form'
- **2018 EU Proposal Production and Preservation Orders for Electronic Evidence in Criminal Matters**
  - ✓ Art. 2(6): 'evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored *subscriber data*, *access data*, *transactional data* and *content data*'

1. Electronic Evidence: Definition (2)

- Divers national approaches:
  - ✓ define it (e.g. England & Wales, Italy) or
  - ✓ referring to this type of evidence without defining it (e.g. Germany, Norway)

- Draft Convention on Electronic Evidence (promoted by Mason) defines it as ‘evidence derived from data contained in or produced by any device the functioning of which depends of a software program or from data stored on or communicate over a computer system or network’

- Literature (Mason & Seng, 2017) propose defining electronic evidence as ‘data (comprising the output of devices or data in digital form) that is manipulated, stored or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence

1. Electronic evidence: Potential Issues

- **Privacy issues**: particularly relevant when it concerns personal devices and social media: GDPR Regulation & Art. 8 ECHR on the right to private life
- **Preservation issues**: spoliation of electronic material, volume of data
- **Diversity of sources issue**: computers/laptops, usbs, clouds, apps, emails, chatrooms, databases, audio
- **Authenticity & integrity issues**: alterations, manipulation, electronic signatures & seals
- **Legality issues**: illegally obtained evidence
- **Evaluation issues:** transparency
- **Practical issues:** standards, technical equipment, budget

1. Electronic Evidence: International & European Cooperation in Evidence Collection

Hague Evidence Convention (1970)

- No reference to electronic evidence …But expert group and country reports on use of videolinks & other technology, as well as a guide are available on the Evidence Section
  - ✓ Consideration of amending the Hague Evidence Convention or Guide on video-link and use of technology

Evidence Regulation (1206/2001)

- No reference to electronic evidence …but proposal to review the Regulation
- Practical guide to using videoconferencing

European Small Claims Procedure (861/2007, reviewed in 2015 – 2015/2124)

- Refers to electronic communications => enabling taking of witness statements using videoconferencing and other means of distance communication (Art. 9 conj. Art. 8)

Competition law enforcement Directives (2019/1 & 2014/104)

- 2019 Directive: type of proof including electronic messages & recordings
- 2014 Directive: evidence irrespective of medium on which information is stored;

without prejudice to Regulation 1206/2001

Erasmus School of Law

Electronic Discovery/ Disclosure

Erasmus University Rotterdam

2. Discovery or Disclosure: An Introduction

- What is discovery?

- Functions of discovery?
  - ✓ Achieve equality of access to information
  - ✓ Facilitate settlement of disputes
  - ✓ Avoids ‘trial by ambush’
  - ✓ Assists court in reaching accurate determinations of facts when entering judgment on merits

- When?
  - ✓ Pre-trail
  - ✓ During main proceedings

- Against who?
  - ✓ Inter-party discovery
  - ✓ Non-parties

- Privileges against self-incrimination, legal professional privilege, ‘without prejudice’ communication public interest immunity

2. From Discovery/ Disclosure to Electronic Discovery/ Disclosure

2. Electronic Disclosure or Discovery

- Does it exist as such in civil law countries?
- **Common law concept** (England & Wales, Ireland, US, Canada)
- **Some civil law countries** have something similar, but more **limited mechanisms to disclose** information (e.g. Netherlands – a request can be made pre-trail to order a party to produce evidence; draft proposal to expand this is currently under discussion)
- In **international litigation** rules related to disclosure or discovery can come into play
- **EU**: Private Damage Directive (2014/104) on certain rules governing actions for damages under national law for infringements of competition law of MS and of EU (Art. 2(13) & 5-6)
- Due to volume of information & time burden => **Technology Assisted Review** (TAR) software has been considered in e-discovery processes (US) (coding, machine learning techniques)

2. Electronic Discovery/ Disclosure: Characteristics

- Party should focus on key documents which are likely to be required/necessary at trial
- When litigation is contemplated: parties' representative to notify clients of need to **preserve disclosable documents**
- Documents may need to be presented in their **original format/electronically searchable** format - not paper format, as this affects the **metadata**
- Once a **listing of responsive documents** has been prepared an officer of the company, a senior representative or the person with the most knowledge of the proceedings swears the affidavit of discovery
- **Affidavit of discovery** sets out details of the searches undertaken, the categories of discovery, & details regarding withheld documents
- Two listings are appended: (1) all documents; & (2) privileged documents

2. Use of Technology in Search for Electronic Discovery

- Sheer volume of electronic documents may present huge logistical challenges => use of automated search

- How?
  - ✓ Use of key word to electronically filter a large volume of data so as to identify documents requiring disclosure. (e.g. identify all emails passing between key protagonists or between certain dates or in which certain terms appear)
  - ✓ Care required in selecting the key words - if too broad they may generate huge numbers of "false positives",
  - ✓ Ideally before either side makes discovery, they should agree on the appropriate key words to be employed (selection of key words needs to be discussed with all stakeholders in the process)

- More advanced alternatives:
  - ✓ Use of software programs, AI, machine learning to reduce discovery burden, expenses, avoid unnecessary & repetitive discovery

2. Electronic Discovery/ Disclosure: Dealing with Queries

- Once parties received and reviewed the furnished e-discovery, (possibly) raise queries & comments on each other's discovery
- Party making discovery should provide responses to the queries
- If necessary, party reviewing the discovery can apply to the court for various remedies, such as:
  - ✓ seek further and better discovery
  - ✓ test the claim of the privilege
  - ✓ strike out the other party's claim/defence for failure to make adequate discovery

2. Electronic Disclosure: Some Insights into Common Law Perspective

England & Wales

- PD 31 (introduced on 1 Oct. 2010) – in cases likely to be allocated to multi-track
- Keep costs in proportion: parties & legal advisers are required to discuss use of technology for managing discovery
- Electronic devices concerned: e.g. PCs, laptops, PDAs, mobile phones, email accounts (including restoring of email accounts), social media accounts, USBs, cloud platforms
- Unless otherwise agreed, documents should be disclosed in their native form (i.e. preserving any metadata)
- Technology to access documents not available to counterparty – duty to cooperate
- Penalties for discovery failings

Ireland

- S.I. No. 93 of 2009: Rules of the Superior Court (Discovery) 2009 - an order for discovery of documents could include Electronically Stored Information (ESI)
- Keep costs under control: use of software for deduplication of documents
- Type of electronic devices concerned: e.g. servers/decommissioned servers, laptops, mobile phones, backup tapes, repositories, cloud services
- Penalties for discovery failings

2. Electronic Discovery/ Disclosure: Civil Law Countries Perspective?

- **France**: general obligation to cooperate with the instructing judge and to contribute to clarification of the dispute's factual basis (see Art. 11 Code of civil procedure & Art. 10 Civil Code)

- **Italy**, **Germany** & **Spain**: rules on production of documents & things relevant to a party's case (Art. 118, 210 & ss., 258 & ss. Italian Code of Civil Procedure; Art. 142-144, 371-372, 424-427 German Code of Civil procedure; Art. 317 & ss., 324 & ss., 353 & ss. Spanish LEC)

- **The Netherlands**: Dutch Supreme Court ruled that despite the present limited possibilities of obtaining evidence pre-trial in NL, evidence obtained in US discovery proceedings is admissible in Dutch civil proceedings (*Hoge Raad, 6 Febr 1998, NJ 1999*, 479); Rotterdam District Court dismissed request for an order to forbid discovery (the claimant arguing that it was against the rules of Dutch Code of Civil Procedure) which had been ordered by US District Court at the request of a Dutch party against a US Party (*Rechtbank Rotterdam, 8 June 2012*; ECLI:NL:RBROT:2012:BX4521)

2. Electronic Discovery/ Disclosure: Any Duty under Taking of Evidence Regulation?

- Art 4(1) (f): Special requests – for the production of documents or the inspection of objects?
- Art 4(1) (g): requesting court calls for the requested court to execute in accordance with a special procedure provided for by its own law? – this could cover the manner in which the evidence is to be recorded or way a witness is examined/parties are heard/expert is appointed & heard or **documents are produced** etc. (see Practice Guide)
- If procedure of MS of requesting court is incompatible with law of MS of requested court, requested court can refuse to comply with such requirement (Art. 10(3))
- **Grounds for refusal** are **exceptional** and **strictly limited**:
  - ✓ Request does not fall within scope of Regulation (Art. 1)
  - ✓ Requested court does not have the power to instruct the requested measure (Art. 14(2)(b))
  - ✓ Requesting court does not comply with the request of the requested court to complete the request within 30 days from request (Art. 8)
  - ✓ Deposit or advance asked (Art. 18(3)) is not made within 60 days after requested court asked for such deposit/advance
  - ✓ **No public policy exception**

2. Electronic Discovery/ Disclosure: Any Duty under Hague Evidence Convention?

- Art. 3(i): any special method or procedure to be followed under Article 9?
- Art 9: will follow a request of requesting authority that a special method or procedure be followed, unless this is incompatible with its internal law or is impossible of performance by reason of its internal practice and procedure or by reason of practical difficulties
- Art. 23: 'A Contracting State may at the time of signature, ratification or accession, declare that it will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents as known in Common Law countries'
- **Grounds for refusal**:
  - ✓ Request does not fall within the scope of the Convention (Art. 1)
  - ✓ Reservation for obtaining pre-trail discovery (Art. 23)
  - ✓ Request that a special method or procedure be followed, but this is incompatible with the internal law of the State of execution or is impossible of performance by reason of its internal practice and procedure or by reason of practical difficulties (Art. 9(3))

2. Electronic Discovery/ Disclosure: Damages under National Law for infringements of competition law

- Private Damage Directive (2014/104) – applicable since 27 December 2016
- Art. 2(13) 'evidence' definition
  - ✓ all types of means of proof admissible, in particular documents & all other objects containing information, irrespective of the medium on which the information is stored
- Art. 5: Disclosure of evidence
  - ✓ (1) order defendant/claimant or third party; no prejudice to Taking of Evidence Reg.
  - ✓ (2) specified items circumscribed as precisely & as narrowly as possible on basis of reasonably available facts
  - ✓ (3) proportionality of order to disclose information => legitimate interest
  - ✓ (4) power to order disclosure of evidence containing confidential information – national courts have at their disposal effective measures to protect information
  - ✓ (7) those from whom disclosure is sought – opportunity to be heard by court before it orders disclosure
- Art. 6: Disclosure of evidence included in files of competition authority: in addition to Art. 5
  - ✓ (6) national courts cannot order a party or a third party to disclose leniency states and settlement submissions
  - ✓ (10) only where no party or third party is reasonably able to provide that evidence
  - ✓ (11) competition authority willing to state views on proportionality - submit observations

Erasmus School of Law

Electronic Signatures/ Keys

3. Electronic Signature: Legal Framework

- **eSignature Directive** 1999 (Directive 1999/93/EC): repealed by eIDAS

- Present **eIDAS Regulation** (Regulation (EU) 910/2014): applicable since 1 July 2016
  - ✓ Sets the rules on legal recognition of electronic signature for various purposes (including for evidence)
  - ✓ Creates an European internal market for **electronic trust services** – namely, **electronic signatures**, **electronic seals**, **time stamp**, **electronic delivery service** and **website authentication** – by ensuring that they will work across borders and have the same legal status as traditional paper based processes
  - ✓ Predictable regulatory environment to enable secure & seamless electronic interactions between businesses, citizens & public authorities

- UNCITRAL Model Law on Electronic Signatures (2001)

3. Electronic Signature: eIDAS

- **Scope**:
  - ✓ Conditions under which **MS recognise** electronic identification means of natural & legal persons under a **notified electronic identification scheme of another MS**
  - ✓ Rules for trust services (particular electronic transactions)
  - ✓ Legal framework for: **electronic signature**, **electronic seals**, **electronic time stamps**, electronic document, electronic registered delivery service & certificate services authentication

- **Definitions:**
  - ✓ **Electronic signature**: 'data in electronic form (…) attached to or logically associated with other data in electronic form and which is used by the signatory to sign' (Art.3(10))
  - ✓ **Advanced Electronic Signature**: an electronic signature which **meets the requirements of being uniquely linked to the signatory**, capable of identifying him & created using electronic signature creation data that the signatory can use under his sole control (Art. 3(11) conj. Art 26)
  - ✓ **Qualified Electronic Signature**: 'an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures' (Art. 3(12))
  - ✓ **Electronic signature creation data**: 'unique data which is used by the signatory to create an electronic signature' (Art. 3(13));

3. Electronic Signature: Legal Effects under eIDAS

Art. 25 eIDAS:

- Electronic signature shall **not be denied legal effect and admissibility as evidence in legal proceedings** solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures

- **Qualified electronic signature** equivalent legal effect of a **handwritten signature**

- A qualified electronic signature based on a qualified certificate issued in a MS to be recognised as a qualified electronic signature in all other MS

3. Electronic Seals: Definitions under eIDAS

- **Electronic seal:** data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity (Art.3(25))
- A**dvanced electronic seal**: an electronic seal, which meets the requirements set out in Art. 36 (Art.3(26))
  - ✓ Art. 36 requirements: seal is (1) uniquely linked to creator of seal, (2) capable of identifying the creator, (3) created using electronic seal creation data that creator of the seal can, with a high level of confidence under its control, use for electronic seal creation, & (4) linked to data to which it relates in such a way that any subsequent change in the data is detectable
- **Qualified electronic seal**: an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal
- **Electronic seal creation data**: unique data, which is used by creator of electronic seal to create an electronic seal (Art.3(28))
- **Certificate for electronic seal**: an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person (Art.3(29))

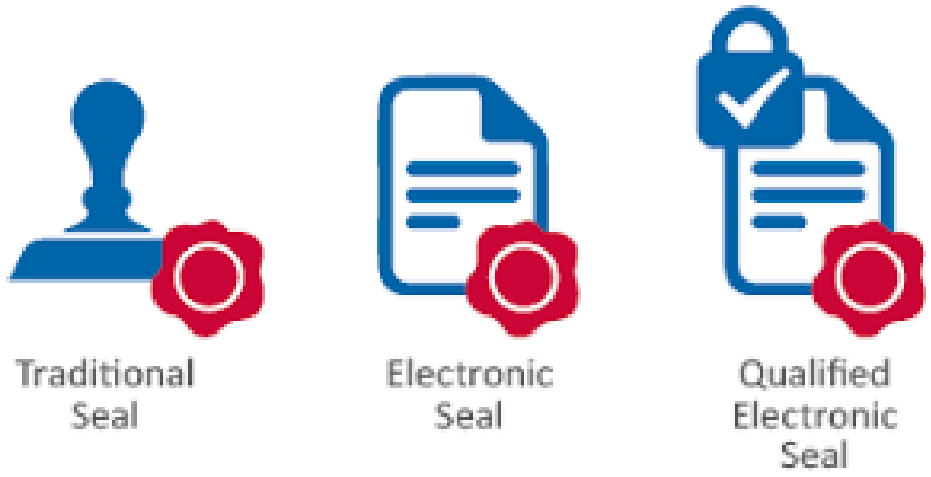
3. Electronic Seals: Legal Effects under eIDAS

Art. 35 eIDAS:

- **Electronic seal** shall **not be denied legal effect and admissibility as evidence** in legal proceedings solely on grounds that it is in an electronic form or that it does not meet requirements for qualified electronic seals

- **Qualified electronic seal** enjoys the presumption of integrity of data and of correctness of origin of that data to which qualified electronic seal is linked

- A qualified electronic seal based on a qualified certificate issued in one MS be recognised as a qualified electronic seal in all other MS



3. Electronic Time Stamps: Definitions under eIDAS

Definitions:

- **Electronic time stamp**: data in electronic form which binds other data in electronic form to a particular time establishing evidence that latter data existed at that time (Art.3(33))
- **Qualified electronic time stamp**: an electronic time stamp which meets the requirements laid down in Article 42 (Art.3(34))

- **Qualified electronic time stamp** (Art. 42): binds the date & time to data in manner that reasonably precludes possibility of data being changed undetectably, based on accurate time source – Coordinated Universal Time, & is signed using and advanced electronic signature/seal

3. Electronic Time Stamps: Legal Effects under eIDAS

Art. 41 eIDAS

- **Electronic time stamp not be denied legal effect & admissibility** as evidence in legal proceedings solely on the grounds it is in electronic form or that it does not meet the requirements of qualified electronic time stamp
- A **qualified electronic time stamp** enjoys the **presumption of accuracy of date & time it indicates & integrity** of the data to which date and time are bound
- A qualified electronic time stamp issued in one MS shall be recognised as qualified electronic time stamp in all MS
- Qualified electronic time stamp (Art. 42): binds the date & time to data in manner that **reasonably precludes possibility of data being changed undetectably**, based on accurate time source – Coordinated Universal Time, & is signed using and advanced electronic signature/seal

Erasmus School of Law

Evaluation of Evidence

4. Evaluation of Evidence Equivalence: Digital vs. Paper

- Despite limited legislative framework & lack of rules on electronic evidence (at times) – electronic documents can be considered to be **on equal footing with paper documents**
- … **But** issues related to **reliability** & **authenticity** of electronic forms of evidence remain
- Technology advancements & IT forensics: easier to **review authenticity & origin of documents**; but not always easy to establish origin of information shared through social media
- Rules of **electronic signatures** have been crucial in validating & securing the authenticity of electronic documents
- **Electronic documents & signatures** have been **validated at European & international level** in context of contract law (particularly e-commerce), arbitration agreements & choice of court agreements
- **Assessing degree of probability**: standard differs btw. civil & common law countries

3. Evaluation of Electronic Evidence: **Issues of Reliability & Document Integrity**

- Affect admissibility of electronic evidence
- **Principle of free evaluation** of evidence in civil procedure => necessary flexibility to decide on a case-by-case basis whether materials are trustworthy
- Legal perspective, most important response to authenticity issues is regulation of e-signature => **eIDAS Regulation**
- **Evidence obtained** from various **social media** raises issues of admissibility => US: is relevant, not hearsay, is probative, & authentic
- **Admissibility** of electronic evidence lies in how far illegally obtained evidence can be excluded
- Very important courts & lawyers have **sufficient knowledge of technical aspects** => understanding of how to preserve evidence & how to evaluate & interpret the materials presented => required basic knowledge of the technicalities of software use in discovery process as well as understanding of the social media, technical options (e.g. privacy settings) & way people use these media