Working Paper Seminar: The Digital Services Act and the e-Evidence Regulation: what role for private actors?

(ILPC Seminar Series)

24 October 2023

Marine Corhay, PhD Candidate ULiège

Chair: Dr Nóra Ní Loideáin

Discussant: Dr Martin Husovec

PhD Thesis

- The role of service providers in the context of
  - direct cross-border cooperation
  - with law enforcement authorities
  - access to electronic communications data.
- Through the lens of the right to respect for private life and the right to the protection of personal data (Arts 7 and 8 CFREU)
- Broader issue of whether private actors can and should play a role in the protection of fundamental rights and how this role should be (re)framed.

Working Paper: Presentation

- Trend to involve private actors in cross-border enforcement
- multifaceted but targeted analysis of the e-Evidence Regulation and the Digital Services Act :
  - role of private actors when they cooperate with law enforcement authorities
  - division of responsibilities between public authorities and private actors in the protection of fundamental rights.

Aim = provide an answer to the following question: Are service providers the guardians of fundamental rights or the King’s hand?

Role of private actors: Origins

- Development and spread of Information and Communications Technologies (ICTs)
- Cross-border nature of the Internet and ‘big players’
- Necessity of cross-border cooperation (from a law enforcement perspective)
- (Pro)active role of private actors (Tosza 2021)

e-Evidence framework: Paradigm shift

- Regulation 2023/1543
  - institutionalises a new criminal justice paradigm = direct cross-border cooperation between judicial authorities and the private sector, i.e. service providers.
    - ‘Privatisation’ of mutual recognition (Tosza 2019, Mitsilegas 2018)
  - European Production orders (EPO) and Preservation orders (EPO-PR) for stored data
  - Enforcement
  - Penalties
- Directive 2023/1544
  - designated establishment or legal representative in a Member State

e-Evidence Regulation: role of service providers

- = most **controversial** topic surrounding the negotiations of the e-Evidence framework (Christakis; Robinson; a.o.)
- Overarching principle = service providers must comply with orders
- Execution and enforcement stages : justifications and grounds for refusal
- Information provided in the certificate
- Confidentiality of orders

e-Evidence Regulation: role of service providers (1)

- Information provided in the certificate
  - Omitted: proportionality and necessity assessment of the order and a summary description of the case
  - But still possible to ‘spot’ problematic orders
- grounds for justification for non-compliance – execution stage
  - Mainly technical and practical issues but also …
  - immunities and privileges or the rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media
  - ‘other reasons’
    - Recital 58
- Grounds for refusal to execute – enforcement procedure
- Confidentiality of orders (Art. 13)
  - Role of issuing authority

e-Evidence Regulation: actors and division of responsibilities

- Potentially 3 actors involved : issuing authority, service provider and enforcing authority => delineation of each actor's role
- Responsibility of the issuing authority
  - Remedies (Art. 18)
    - Challenge the legality of measure (incl. necessity and proportionality)
- Enforcing authority:
  - notification and enforcement
  - 'extra layer'
- Service provider:
  - Exemption of liability for prejudice caused that exclusively results from compliance in good faith(Art. 15(2))
  - Penalties for non-compliance (Art. 15(1))

e-Evidence Regulation: actors and division of responsibilities (1)

EPO-PR and EPOs for subscriber data and data requested for the sole purpose of identifying the user + EPOs for traffic and content data -national cases

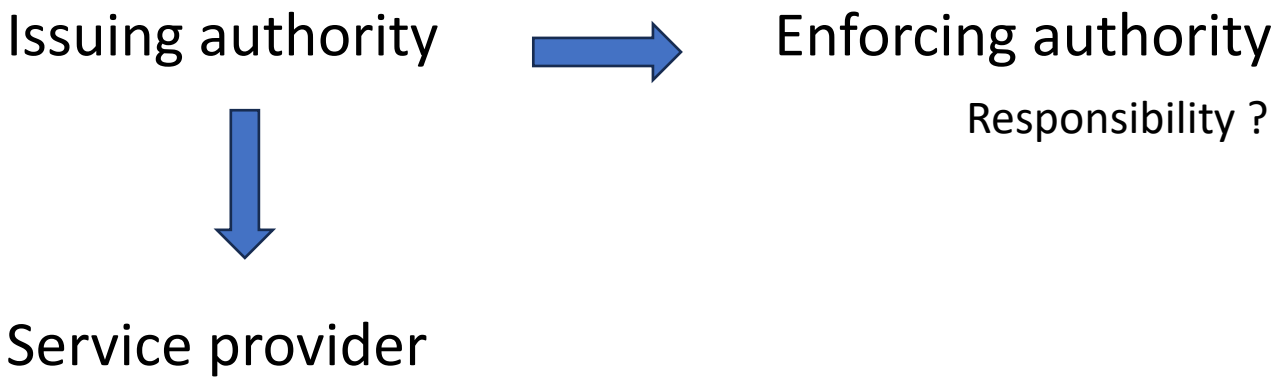
Issuing authority

Service provider (complies)

Quid Article 18(1)? ‘without prejudice to the right to seek a remedies under the GDPR and the LED’

e-Evidence Regulation: actors and division of responsibilities (2)

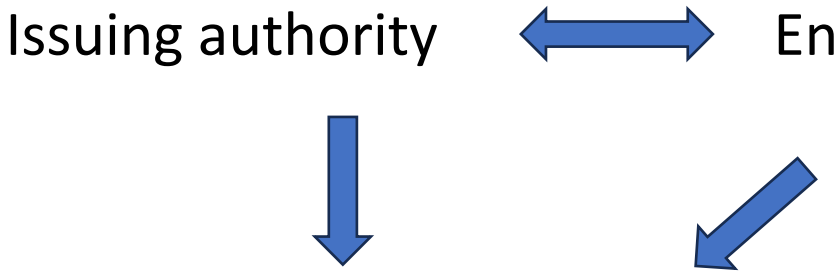
EPOs for traffic and content data
Notification to enforcing Member State (not in emergency cases)



- Certificate sent simultaneously (Art. 8(1))
- Suspensive effect – 10 days (max.) (Art. 10(2))
- Grounds for refusal (Art. 12)
- Limited ‘protective functions’ of the enforcing authority
  - Sovereignty
  - Wording of the fundamental rights clause

e-Evidence Regulation: actors and division of responsibilities (3)

Procedure of enforcement (EPO + EPO-PR) (Art. 16)



- Grounds for refusal – enforcing authority
- Possibility to object – service provider
  - No fundamental rights clause
- Final decision: enforcing authority
- Penalties (Art. 15) : 2% total worldwide annual turnover of service provider's preceding financial year
- Final decision taken by enforcing authority BUT only the service provider can provide the data…

The Digital Services Act

- Comprehensive set of rules regulating the responsibilities and due diligence obligations of providers of intermediary services, including obligations to cooperate in enforcement
  - Gradual approach
- Objectives
  - reduce harms and counter risks online
  - promote transparency and accountability about intermediaries' practices, terms of services and content moderation processes
  - = meant to safeguard users' fundamental rights and freedoms online and facilitate innovation

The Digital Services Act: ‘cooperation duties’

Orders to act against illegal content (Art. 9)

Orders to provide information (Art. 10)

Notification of suspicion of criminal offences (Art. 18)

The Digital Services Act: cooperation duties (1)

- **orders to act against illegal content** (Art. 9) and **orders to provide information** (Art. 10) - all intermediaries
  - Minimum conditions to be met (e.g information provided, territorial scope)
  - Legal basis in national law
  - ≠ with e-Evidence:
    - 'orders' but no obligation for intermediaries to give effect, only to inform of any-follow-up given to orders
    - Margin of appreciation/discretion for intermediaries
  - Interaction with other instruments ? 'without prejudice …' => includes e-Evidence Regulation
  - Information provided to intermediaries
  - Adaptations required for criminal law purposes = reduces the margin of manœuvre
    - Notification to the person(s) concerned

The Digital Services Act: ‘cooperation duties’ (2)

- **orders to act against illegal content** (Art. 9) and **orders to provide information** (Art. 10) - all intermediaries
  - Effect ?
    - e.g. disabling or removing content?
    - Quid territorial scope ?
    - ‘specific information’ ? Recital 37 : aim = enabling the identification of the recipients of the service concerned
    - Only information already collected for the purposes of providing the service and which lies within their control but ‘without prejudice to retention and preservation rules under applicable national law, in compliance with Union law’ (recital 34)

The Digital Services Act: ‘cooperation duties’ (3)

- **notification of suspicion of criminal offences** (Art. 18) - hosting services, including online platform
  - ‘crime reporting’ obligation
  - information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place
  - Broad scope
    - suspicion must be reasonably justified, having regard to all relevant circumstances of which the intermediaries is aware (recital 56)
    - ‘all relevant information available’ : content in question, time when the content was published, explanation of its suspicion and information to necessary to locate and identify the relevant recipient of the service (recital 56)
  - Sentinel ?

The Digital Services Act: division of responsibilities

- Risks for freedom of expression, right to respect for private life and protection of personal data
- Limited set of conditions imposed by the DSA: discretion left to Member States and space for self-regulation may blur the lines but …
- ‘delegated enforcement’
  - situation where the law expects private actors (e.g. platforms), to act as enforcers of the law, by entrusting them with various tasks (e.g. removal of content) (Husovec 2023)
    - ECtHR case-law (content moderation – ‘over-blocking’ of content)
    - CJEU Case C-401/19 and AG Opinion (in the context of Art. 17 Directive on Copyright in the Digital Single Market)
    - => responsibility remains with the state

The Digital Services Act: division of responsibilities

- Orders to act against illegal content (Art. 9) and Orders to provide information (Art. 10)
  - ≠ e-Evidence: no procedure of enforcement => in accordance with the issuing Member State's national law
  - Liability regime

- Notification of suspicion of criminal offences
  - Penalties for violation of due diligence obligations (Art. 52) // Art. 15 e-Evidence Regulation : 6% company's global revenue

e-Evidence and DSA: Different approaches

- E-Evidence Regulation
  - overarching goal of the framework = to improve access to electronic evidence in cross-border situations
  - no longer contain a mere request but an explicit order to cooperate
  - Little to no margin of manœuvre
- DSA
  - Some minimum requirements
  - Space intermediaries to decide and self-regulate
  - Discretion and implementation by Member States

Private actors: guardians of fundamental rights or the King's hand ?

- Calls for a nuanced answer….
- e-Evidence
  - 'orders'
  - Penalties and exemption of liability
  - Theory v. practice
- DSA
  - Intermediaries still in the driving seat?
  - Imprecise scope of obligations = risk
  - Balance of interests and strategic choices

Discussion and questions