Verbesserte Straftatenbekämpfung auf Kosten der Medienfreiheit? Die neuen EU-Vorschläge (e-evidence und TCO) in der Kritik

Keynote

M. Cornils, Mainz

MAINZER MEDIENINSTITUT

Enhancing strategies, mechanisms and instruments to combat illegal, criminal or „terrorist“ content on the net: Necessity and risks

(nearly) everybody agrees:

- If terrorists (or other) criminals are acting by using communication facilities on the net (and they do) it is **necessary to (better) control these communications,** within a legal framework of unique principles and rules in Europe – for purposes of prevention and persecution.
- So (nearly) every comment – even the critical ones – on new EU-proposals begins like: “**Yes to the goal and policy objective** (tackling terrorism and dissemination of criminal/terrorist content online)

- But many comments than continue – more or less harshly:

– “**No** to these now proposed legal instruments which are likely to endanger free communication and fundamental rights ”

Harsh criticism: some examples

"The Regulation, as proposed, would introduce **serious risks of arbitrariness and have grave consequences for freedom of expression and information**, as well as for civil society organisations, **investigative journalism and academic research**, among other fields." *(Civil Society open letter, december 2018 concerning TCO-regulation)*

"EU Terrorist Content regulation **will damage the internet in Europe** without meaningfully contributing to the fight against terrorism" *(letter of pioneers, technologists, and innovators to the EP-Rapporteurs, april 2019)*

"the proposal – as presented by the European Commission – would pose an **unacceptable threat for the freedom of press and media, the freedom of expression as well as the freedom of information"** *(ACT, EU, EFJ, EMMA and others regarding the e-evidence-regulation: "A call for protection of the free and independent media in Europe")*

A specific need to protect media and journalism

Acknowledged by European Law

- For example: Article 9 former Data Protection Directive, now **Article 85 GRDP**
  - ECJ decisions Satamedia and Buivids (2018)
- and especially: the Right to **protect the sources of the media**
  - ECtHR – Sanoma Uitgievers (2010): “The right of journalists to protect their sources is part of the freedom to receive and impart information and ideas without interference by public authorities protected by Article 10 of the Convention and serves as one of its important safeguards. It is a cornerstone of freedom of the press, without which sources may be deterred from assisting the press in informing the public on matters of public interest.”

- But does this mean **that any communication (of suspect persons) with journalists on the net has to be respected as strictly confidential**?

Focus: Two proposals

- Regulation (EU) on Preventing the dissemination of terrorist content online, COM 12.9.2018 COM(2018)640 final
  - **Status: EP First Reading**
- Regulation (EU) on European Production and Preservation Orders for electronic evidence in criminal matters **“e-evidence-regulation**”, COM 17.4.2018 COM(2018) 225 final
- [in combination with: Proposal COM(2018) 226 final **(“e-evidence directive –** laying down **harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings]**
  - **Status: General approach (Council)**

Regulation on preventing the dissemination of terrorist content online

Article 1 Subject matter and scope

1. This Regulation lays down uniform **rules to prevent the misuse of hosting services for the dissemination of terrorist content online**. It lays down in particular:

(a) **rules on duties of care to be applied by hosting service providers in order to prevent the dissemination of terrorist content** through their services and ensure, where necessary, its swift removal;

(b) **a set of measures to be put in place by Member States** to identify terrorist content, to enable its swift removal by hosting service providers and to facilitate cooperation with the competent authorities in other Member States, hosting service providers and where appropriate relevant Union bodies.

2. This Regulation shall **apply to hosting service providers offering services in the Union**, irrespective of their place of main establishment.

TCO-Regulation

Article 2 Definitions

For the purposes of this Regulation, the following definitions shall apply:

1. **'hosting service provider'** means a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to third parties;

[…]

4. **'terrorist offences'** means offences as defined in Article 3(1) of Directive (EU)

2017/541;

5. **'terrorist content'** means one or more of the following information:

(a) **inciting or advocating**, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;

(b) **encouraging** the contribution to terrorist offences;

(c) **promoting** the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541;

(d) **instructing on methods or techniques for the purpose of committing terrorist offences**.

TCO-Regulation

Article 4 Removal orders

1. The competent **authority** shall have the power to issue a **decision requiring the hosting service provider to remove terrorist content or disable access to it.**

2. Hosting service providers **shall remove terrorist content or disable access to it within one hour** from receipt of the removal order. […]

Article 5 Referrals

1. The competent **authority or the relevant Union body** may **send a referral** to a hosting service provider.

2. Hosting service providers **shall put in place operational and technical measures facilitating the expeditious assessment of content** that has been sent by competent authorities and, where applicable, relevant Union bodies for their voluntary consideration. […]

Article 6 Proactive measures

1. Hosting service providers **shall, where appropriate, take proactive measures to protect their services against the dissemination of terrorist content**. The measures shall be effective and proportionate, taking into account the risk and level of exposure to terrorist content, the fundamental rights of the users, and the fundamental importance of the freedom of expression and information in an open and democratic society. […]

TCO-Regulation: problems and criticism

- **no necessity (proportionality), missing evidence for a need to establish this instrument**
- **broad and unclear scope (esp. obliged host providers [cloud services?] and „terrorist content“)**
- **cross-border-removal orders within the EU endangering freedom of communication**
- **proactive filtering (Article 6):** filter systems not able to identify terrorist content, overblocking
- **„concentration“ of services**: esp. SME unable to comply with obligations

TCO-Regulation

AEP (First Reading, April 2019) some (out of a lot) amendments

am 42 (scope)

This Regulation shall not apply to content which is disseminated for educational, artistic, journalistic or research purposes, or for awareness raising purposes against terrorist activity, nor to content which represents an expression of polemic or controversial views in the course of public debate.

am 55 (more precise definition of terrorist content)

~~promoting~~ ***soliciting another person or group of persons to participate in*** the activities of a terrorist group, ~~in particular by encouraging the participation in or support to a terrorist group~~ ***including by supplying information or material resources, or by funding its activities in any way*** within the meaning of Article ~~2(3)~~ ***4*** of Directive (EU) 2017/541***, thereby causing a danger that one or more such offences may be committed intentionally***

am 88 (proactive measures, no automated tools)

~~Where no agreement can be reached within the three months from the request pursuant to paragraph 3~~ ***After establishing that a hosting service provider has received a substantial number of removal orders***, the competent authority referred to in Article 17(1)(c) may ~~issue a decision imposing specific additional~~ ***send a request for*** necessary ~~and~~***,*** proportionate ~~proactive~~ ***and effective additional specific*** measures ***that the hosting service provider will have to implement. The competent authority shall not impose a general monitoring obligation, nor the use of automated tools***.

e-evidence regulation

Proposal COM 17.4.2018 COM(2018) 225 final

aim:

- "targets the specific problem created by the volatile nature of electronic evidence and its international dimension. It seeks to adapt cooperation mechanisms to the digital age, giving the judiciary and law enforcement tools to address the way criminals communicate today and to counter modern forms of criminality."
- "growing need for timely cross-border access to electronic evidence"
- "fragmentation" (national tools), legal uncertainty

instruments:

- **European Production** and **Preservation Orders:**
- can be issued to seek preservation or production of data that is stored by a service provider located in another jurisdiction and that are necessary as evidence in criminal investigations or criminal proceedings

In connection with:

- Proposal COM(2018) 226 final **("e-evidence directive –** laying down **harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings**

e-evidence regulation

definitions

- ‘European Production Order’: a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence;
- ‘European Preservation Order‘: a binding decision (…) to preserve electronic evidence in view of a subsequent request for production;
- ‘service provider’: any natural or legal person that provides one or more of the following categories of services
  - electronic communications service (EECC [Dir. EU 2018/1972]
  - information society services (Dir. EU 2015/1535)
  - internet domain name and IP numbering services

possible subject of an EPOC/EPOC-PR:

- ‘subscriber data’, ‘access data’, ‘transactional data’ , ‘content data’ (means any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data)

e-evidence regulation

Issuing authority (Article 4):

- either: a judge or court (and prosecutor)
- or: any other competent authority, but under condition of validation by judge, court (prosecutor)
- differentiation between EPOC (here: no prosecutor as authority, validator regarding subscriber data and/or access data) and EPOC-PR:

	subscr. data access data	transaction data content data
PO	authority or validation: judge, court, investigating judge, *prosecutor*	authority or validation: judge, court, inv. judge
PO-PR	authority or validation: judge, court, investigating judge, *prosecutor*	

e-evidence regulation

Conditions for issuing a European Production Order (Article 5)

(…)

2. The European Production Order shall be **necessary and proportionate for the purpose of the proceedings referred to in Article 3 (2)** and may only be issued **if a similar measure would be available for the same criminal offence in a comparable domestic situation** in the **issuing State**.

3. European Production Orders to produce **subscriber data or access data** may be issued for **all criminal offences**.

4. European Production Orders to produce **transactional data or content data** may only be issued

for criminal offences punishable in the issuing State by a custodial sentence of a maximum of **at least 3 years**, or

for the following offences, if they are wholly or partly committed by means of an information system: as defined in Articles 3, 4 and 5 of the CFD 2001/413/JHA, in Articles 3 to 7 of Directive 2011/93/EU, in Articles 3 to 8 of Directive 2013/40/EUl;

for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541

e-evidence regulation

Obligation (service provider) (Article 9)

requested data **is transmitted directly** to the issuing authority or the law enforcement authorities as indicated in the EPOC **at the latest within 10 days** upon receipt of the EPOC, unless the issuing authority indicates reasons for earlier disclosure

In emergency cases the addressee shall transmit the requested data without undue delay, at the latest within 6 hours

Sanctions (Article 13)

Member States shall lay down the **rules on pecuniary sanction**s applicable to infringements of the obligations pursuant to Articles 9, 10 and 11 of this Regulation and shall take **all necessary measures to ensure that they are implemented**. The pecuniary sanctions provided for shall be **effective, proportionate and dissuasive.**

e-evidence regulation

Safeguarding fundamental rights (?)

COM: “tools are conditional on their being subject to strong protection mechanisms for fundamental rights”

(ex ante) obligation of the issuing authority

Article 5 (7)

If the **issuing authority has reasons to believe** that, **transactional or content data** requested is **protected by immunities and privileges** granted under the law of the Member State where the service provider is addressed (…), the **issuing authority has to seek clarification** before issuing the European Production Order, including by consulting the competent authorities of the Member State concerned (…) If the issuing authority finds that the requested access, transactional or content data is protected by such immunities and privileges or its disclosure would impact fundamental interests of the other Member State, it shall not issue the European Production Order.

e-evidence regulation

Safeguarding fundamental rights (?)

(ex ante) rights of the service provider

Article 9 (5)

In case the addressee considers that the EPOC cannot be executed because based on the sole information contained in the EPOC it is **apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive**, the addressee shall also send the Form in Annex III to the competent **enforcement authority** in the Member State of the addressee. In such cases the competent **enforcement authority may seek clarifications** from the issuing authority on the European Production Order(…)

Article 14 (procedure of enforcement)

(4) The addressee may only **oppose the enforcement** of the European Production Order on the basis of the following grounds (...)

f) based on the sole information contained in the EPOC, it is **apparent that it manifestly violates the Charter or that it is manifestly abusive**.

Remedies: only in cases of conflicting obligations from **third countries** (Articles 15, 16)

e-evidence regulation

Safeguarding fundamental rights (?)

(ex post) right to remedies of persons whose data was obtained

Article 17

(2) Where the person whose data was obtained is **not a suspect or accused person in criminal proceedings** for which the Order was issued, this person **shall have the right to effective remedies against a European Production Order in the issuing State**, without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.

3. Such right to an effective remedy **shall be exercised before a court in the issuing State in accordance with its national law** and shall include the possibility to challenge the legality of the measure, including its necessity and proportionality.

e-evidence regulation
possible problems and criticism

- no sufficient **notification regime** (about informing or not informing the person whose data is sought), risk of getting information far too late to defend rights efficiently
- **weak position of the state of enforcement** (which is involved actively only in the case of non-compliance of the service provider)
- precarious **ability of service providers to protect fundamental rights** of data subjects
- no sufficient **regime on protecting data of third parties** (esp. media and journalists!)
- no possibility to challenge an EPOC in a **court of the residence state** of the affected person
- no remedies against EPOC-PR

Thank you very much!

cornils@uni-mainz.de