12 July 2016

State of play analysis

- **E-evidence:** the text of the Parliament appears to undermine the right of businesses and citizens to use cybersecurity tools, such as encryption.

- **Investigative tools:** the tools listed in recital 15a of the Council's position go way too far. The Parliament's text is broader.

- **Impact report:** it's good that in Article 26(2), the Parliament asks the Commission to assess the impact of the Directive on fundamental rights and the rule of law. In the absence of an impact assessment and due to the lack of respect of the Better Regulation principles, this is good news.

- **Definition of terrorism:** On the one hand, the Parliament has rightly narrowed down the definition of Article 3(1)(b) by making sure somebody using violence or threatening to use violence will be punished. This would prevent threats to freedom of expression, in line with the good safeguard introduced by the Council in recital 20a. On the other hand, the Parliament wrongly broadens the definition of terrorism by including "cyber or any other form of attack" (whatever that may mean?) and **attacks to information systems:** by including these "new" offences as terrorist acts, you'd be broadening the scope of Article 3.1 and have the potential to include acts that are not necessarily a terrorist act. There's already a Directive dealing with this issue that is quite recent, Directive 2013/40/EU, and the Council of Europe's Cybercrime Convention.

- **Public provocation to commit a terrorist offence**: In Article 5, the Parliament narrows down the text to making sure speech is criminalised if it causes a danger in a concrete way. The Council, however, introduced a reference to "glorification of terrorism". It's not very clear whether this can lead to the criminalisation of legitimate forms of speech that would not fall under "incitement to terrorism".

- **Undefined terms that could lead to abuse**, such as "radicalisation", are used by in LIBE's report. This concept is not defined in Article 2 (definitions) and it clearly falls outside of the scope of the Directive, which is to define terrorist offences and the corresponding sanctions, and protect victims of terrorism (cf. Article 1).

- **Travelling**: if safeguards are not put in place in the final text, it won't be in compliance with the UN Security Council Decision 2178 (2014), which *"in accordance with Member States International obligations"* [which would include the respect for human rights], *"encourages Member States to employ* ***evidence-based*** *traveller risk assessment and screening procedures including collection and analysis of travel data,* ***without resorting to profiling based on stereotypes founded on grounds of discrimination prohibited by international law.****"*

12 July 2016

- **Cooperation to combat "online radicalisation and incitement to terrorism":** the Parliament's text (Article 21f) asks the Commission to launch a joint initiative between the Commission and internet service providers to combat (non-defined) radicalisation and (also non-defined) "incitement to terrorism". This approach fails completely to take into account the internet governance principle of multistakeholderism and doesn't have a requirement to make this type of mechanisms in a transparent way. Why only include ISPs? What about civil society organisations? And what would the Commission and companies understand by "radicalisation"? This can only lead to arbitrariness, impunity, lack of accountability, breach of the Charter of Fundamental Rights and legal uncertainty, as the recently adopted Code of Conduct on hate speech has shown.

- **Blocking and removal of content**
  - The Commission's impact assessment for amending the Council Framework Decision 2002 rules out measures for blocking and removing of content. The Commissions' assessment of the available evidence was that they are inefficient, bypass the rule of law, have counter-productive effects and obstruct investigations and prosecutions (cf. pages 29 and 41). In addition, Article 19 of the proposed Directive deals with the responsibility of legal persons already.

  - If the EU wants nonetheless to put something on blocking and removal of illegal content, then it should put safeguards in place. With regards to the Parliament's text, while Article 14a is less objectionable, **Recital 7b (new)** contradicts the Article. The most problematic sentences are:

  1: "In that context, this Directive is **without prejudice to voluntary action** taken by the Internet industry **to prevent the misuse of its services or to any support for such action** by Member States."

  According to this text, the safeguards put in place could be disregarded when it comes to "voluntary" arrangements. The text refers to removal of content not on the basis of the law, but on the basis of the terms of service of the internet company in question. In addition, these mechanisms are usually not, in reality 'voluntary', but the result of a degree of state encouragement or coercion. The Internet industry is receiving more and more pressure from public authorities to deal arbitrarily with terrorist content, without safeguards or even certainty that the measures taken will not be counterproductive. Indeed, the European Commission's own impact assessment of 2007 ruled out the inclusion of these practices in the reform of the Framework Decision 2002 for being inefficient, unduly restricting fundamental rights and ***even obstructing prosecutions and investigations****: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2007:1424:FIN:EN:PDF (see in particular pp. 29 and 41).*

12 July 2016

2: "However when removal of illegal content at its source is not possible, MS may put in place measures to block access from the Union's territory to Internet pages identified as containing or disseminating terrorist content".

The first half of the sentence is clear - it refers clearly to content that is (and therefore must have been credibly adjudged to be) illegal. The second half of the sentence is unclear. The drafting does not simply say 'to such Internet pages' and chooses instead to refer to pages 'identified' (by whom?) as containing, not illegal material but content 'containing or disseminating terrorist content'. The second half of the sentence is therefore in clear contradiction and appears to cover some form of arbitrary regulation.

3: "Member States should consider legal action against internet and social media companies and service providers, which deliberately refuse to comply with a legal order to delete from their internet platforms illegal content extolling terrorism after being duly notified about such specific content..."

This sentence has no obvious meaning or purpose. Furthermore, it either contradicts the proposed Article 19 of the draft Terrorism Directive, which deals with the responsibility of legal persons or, at best, duplicates it. In addition, it is not clear whether "legal order" might cover other measures other than judicial orders. In addition, the level of coercion Member States can exert to over-remove/block is also not adequately addressed.

"The right to judicial review should be guaranteed to the internet and social media companies and service providers"

This right, even if it were to be accessible in reality, is being accorded to the wrong party. Neither 'the internet', social media companies or service providers are the injured party if legal content is deleted or blocked. As currently phrased the text explicitly excludes the authors of unlawfully removed/blocked content from redress.