11 October 2016

COMMENTS ON THE TERRORISM DIRECTIVE - 4th TRILOGUE

As indicated in the multi-column document for the 4th Trilogue, "Council text is marked **in bold;** EP text is marked in ***bold italic***; new text is marked in **bold underlined**". EDRi suggestions appear in red, following the same logic.

Main request: EDRi strongly urges the institutions – e.g. by formally asking the Council Legal Services – to assess all additions proposed by the Council and Parliament with a view to confirming their compatibility with the legal basis of the Directive. We are of the opinion that there are many of them which would fail such a test. It is imperative for the legislation to be legally sound.

Comments on Council's drafting suggestions:

- **Article 5. Public provocation to commit a terrorist offence**

Member States shall take the necessary measures to ensure that the distribution, ~~or otherwise making available~~ ***by any means, whether on- or offline***, of a message to the public, with the clear intent to incite the commission of one of the offences listed in points (a) to **(i)** of Article 3(2), where such conduct, expressly or not ~~directly or indirectly, such as by the glorification of terrorist acts,~~ advocat**es the commission of** terrorist offences, **thereby** caus**ing** a danger that one or more such offences may be committed, is punishable as a criminal offence when committed intentionally and unlawfully.

=> EDRi comments:
- "**or otherwise making available**": The Commission, for example in the proposed Copyright Directive, appears to be redefining this concept. If successful, this will have major consequences for internet intermediaries and would give this text a much more expansive meaning, to the detriment of freedom of communication, democracy and the rule of law.
- "**clear intent**": the liability must lie on the speakers' intent, not on the illegality of the content, in line with the recommendations of the UN Special Rapporteur on Human Rights and Combating Terrorism.
- "**expressly or not**": "indirect advocacy" is too broad. The UN Special Rapporteur on Counter-Terrorism and Human Rights recommends this wording.
- The use of "glorification of terrorist acts" without defining what this means goes against basic criminal law principles. Why is this not defined in Article 2? This lead to non-harmonisation and will lead to abuses, as we already see in some Member States.
- "**Unlawfully**" is part of the acquis: it's part of Article 5 of the Council of Europe's Convention on the Prevention of Terrorism. If not included, you would be excluding criminal liability exemptions and legal defences against it.

Recital 7

The offenses related to public provocation to commit a terrorist offence act ~~comprise, inter alia, the glorification and justification of terrorism or the dissemination of messages or images *on- and*~~

~~*offline* including those related to the victims of terrorism as a way to~~ **gather support** for the terrorists cause or seriously intimidat~~e~~ ~~ing~~ the population. Such behaviour ***should be punishable when it*** causes a danger that terrorist acts may be committed. **In each concrete case, when considering whether such danger is caused the specific circumstances of the case should be taken into account, such as the ~~nature of the~~ author and ~~of~~ the addressee of the message, as well as the context in which the ~~offence~~ act is committed. The significance and the credible nature of the danger should be also considered when applying this provision in accordance with national legislation.**

=> EDRi comments:
Generally, this recital makes the text even less clear. According to the proposal, individuals sharing images of victims of terrorism can be criminally liable for public provocation, depending the ill-defined "credible" nature of the ill-defined "danger". This is not a coherent approach. Again, using undefined concepts has proven to lead to abuse in some Member States (cf. "glorification and justification of terrorism"). This will lead to more non-harmonisation, contrary to the harmonisation aims of the Directive.

- **Article 8 Receiving training for terrorism**

Member States shall take the necessary measures to ensure that to receive instruction ***(...)*** in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing of or contributing to the commission of one of the offences listed in points (a) to **(i)** of Article 3(2) is punishable as a criminal offence when committed intentionally.

Recital 9
Criminalisation of the receiving training for terrorism complements the existing offence of providing training and specifically addresses the threats resulting from those actively preparing for the commission of terrorist offences, including those ultimately acting alone. **Receiving of training for terrorism *includes the obtaining of knowledge, documentation or practical skills.* Self-study, including through the Internet or consulting other teaching material, should also be considered training for terrorism, when committed with the intent to commit or contribute to the commission of a terrorist attack. ~~In the context of the specific circumstances of the case, this intention can for instance be inferred from the type of materials and the frequency of reference.~~**
~~Thus, downloading a manual to make explosives for the purpose of committing a terrorist offence could be considered as receiving training for terrorism. By contrast, t~~**The mere fact of visiting websites or collecting materials for other purposes, such as academic or research purposes are not covered by this Directive.**

=> EDRi welcomes the new text added to prevent abuses. However, the text is still dangerously unclear – on the one hand, specific types of content will directly contribute to an individual being found guilty, on the other hand, they should not be found guilty if these specific types of content are download for unspecified "other" purposes. This does not realistically provide enough protection for academic or research work, as the risk of accessing content is too great. Would somebody

providing a general training that *could* be misused for terrorism purposes be covered by this proposal? Sadly, this already appears to be the case in other jurisdictions. The EU must remain vigilant to the risk of creating overwhelming chilling effects for education and speech: https://twitter.com/josephfcox/status/785609699152498688

- Article 14a Measures against illegal terrorist content on the internet

1. Member States shall take the necessary measures to ensure the prompt removal of illegal online *content* constituting ~~*a public provocation to commit*~~ *a terrorist offence*~~*, as referred to in Article 5,*~~ *that is hosted in their territory. They shall also endeavour to obtain the removal of such content hosted outside of their territory.*
2. Member States may take measures to ~~*block*~~ restrict *the access to content* referred to in paragraph 1 towards the Internet users within their territory. *These measures must be* set by *transparent procedures and* provide *adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate and that users are informed of the reason for the restriction.* Safeguards relating to removal or blocking shall also include the possibility of judicial redress.

Recital 7b (new) - based on recitals 46 and 47 of Directive 2011/92/EU
(7b) *An effective means of combatting terrorism on the Internet is to remove terrorist content at source. Member States should use their best endeavours to cooperate with third countries in seeking to secure the removal of* illegal *online content constituting* ~~*a public provocation to commit*~~ *a terrorist offence from servers within their territory. However, when removal of such content at its source is not possible, mechanisms may also be put in place to block access from Union territory* to such content.
The measures undertaken by Member States in accordance with this Directive in order to remove illegal online content constituting ~~a public provocation to commit~~ a terrorist offence or, where appropriate, ~~block~~ restricts access to such content must be based on the law ~~could be based on various types of public action, such as legislative, non-legislative, judicial or other~~. ~~*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, such as detecting and flagging terrorist content*~~. Whichever basis for action or method is chosen, Member States should ensure that it provides an adequate level of legal certainty and predictability to users and service providers and the possibility of judicial redress in accordance with national legislation. Any such measures must take account of the rights of the end users and comply with existing legal and judicial procedures and the Charter of Fundamental Rights of the European Union.

11 October 2016

Recital 7 (c) New on E-commerce Directive

(7c) Removal or where appropriate blocking of webpages in accordance with this Directive should be without prejudice to the rules laid down in Directive 2000/31/EC (E-Commerce Directive). In particular, no general obligation should be imposed on service providers to monitor the information which they transmit or store, nor should a general obligation be imposed upon them to actively seek facts or circumstances indicating illegal activity. Furthermore, hosting service providers should not be held liable as long as they do not have actual knowledge of illegal activity or information and are not aware of the facts or circumstances from which the illegal activity or information is apparent.

=> EDRi comments:
The reference to "blocking" in the E-Commerce Directive relates to hosted content that is not deleted but made unavailable while remaining on the servers of the hosting provider. This is entirely different to the access blocking referred to in Article 14a – using the same word to mean two entirely different things in one legal instrument should be avoided.

It is logically impossible for it to be necessary and proportionate to delete or restrict content that is legal. Therefore, it makes sense to be clear that the content in question is illegal.
"Blocking" is an undefined term that covers a wide range of restriction techniques, ranging from less intrusive but very ineffective with high degrees of false positives and false negatives to extremely intrusive but more efficient approaches. It is not possible to definitively "block" any freely available online content, so "restrict" is more correct.
It is not legally possible for this Directive to prejudice internet providers' implementation of their contracts with their customers in the way implied in this recital. Keeping this text creates interpretative confusion and suggests a lack of legal expertise on the part of the drafters.

Referring to removal and/or blocking of content that constitutes "public provocation on terrorism" is too broad. If the purpose is to delete illegal content that constitutes a terrorist offence, this should be what the Directive should say – despite evidence from the European Commission acknowledging that these measures are ineffective, counterproductive and technically circumventable. According to the EU Regulation on open internet access, blocking of content bust have a legal basis. This Directive cannot contradict that approach. Our edits fix this. Finally, EDRi welcomes the references to the E-commerce Directive.

11 October 2016

Comments on Council's observations

Article 3. Terrorist Offences

3.2. b) "***using violence or the threat of violence to compel or seek to*** compel a government or international organisation to perform or abstain from performing ANY act".

=> EDRi comments: Without the addition of the LIBE text "using violence...to compel" would mean that any attempt at influencing governmental policy could in theory qualify as terrorism. In addition, it risks affecting legitimate forms of protest and civil disobedience. This is contrary to the United Nations Human Rights Committee and the UN Special Rapporteur on Human Rights and Countering Terrorism's recommendations.

3.2.h: cyber attacks:

=> EDRi comments: we agree with the Council that there is no need to include the addition of the LIBE text in letter h. The LIBE text is not technology neutral and it's not based on evidence.

3.2. (ha)/(i) attacks to information systems:

=> EDRi comments: there's no need to include this in the Directive as recent Directive already deals with this issue. The Council's observation (only focusing on the most serious crimes of Directive 2013/40/EU constitutes a step towards the right direction). However, this is not enough. It would be penalising certain attacks to information systems as terrorists attacks. This would lead to consider individuals that are not linked to terrorism as terrorists. This would also increase the sanction – contrary to the principle of legality, necessity and proportionality. It's not the same to kill people than to hack.

3.2. i - LIBE text (serious threat, based on objective, factual circumstances):

=> EDRi comments: it's very important that the LIBE proposal makes it to the final text to prevent the potential for abuses of power or arbitrary sanctions in the Member States.

Article 16. Aiding or abetting, inciting and attempting:

=> EDRi comments: LIBE's approach is correct. Article 5 must be excluded from the scope of this article. Article 16(2) is redundant as Article 5 is the provision dealing with incitement to terrorism.