



Recommendations from La Quadrature du Net on the Draft Report on the **Directive on Combating Terrorism**

The Civil Liberties, Justice and Home Affairs Committee (LIBE) voted a mandate for the rapporteur to start negotiations in trialogue between the Commission, the Council and the Parliament - through the shadow rapporteurs - to reach a draft compromise. As a result of its involvement on the subject in the French policy making for the last two years La Quadrature du Net (LQDN) has been particularly active during the negotiations in the LIBE Committee and would like to keep sharing its recommendations during the trialogue negotiations.

For years, LQDN has been constantly defending at the national level fundamental rights against regular attacks carried through the multiple anti-terrorist laws adopted by France. This is why LQDN invites the European Institutions to learn from the French experience in order to avoid reproducing the mistakes of the dangerous measures that have been made at the French level.

La Quadrature du Net
60 rue des Orteaux - 75020 Paris
0033 972 294 426 - contact@laquadrature.net

1. General comments on definitions

Overall, several key concepts are not well defined and create legal grey areas.

The term "radicalisation" has been introduced by the version of the LIBE Committee (recitals 6a, 17c, 17d, articles 21b, 21f). However this trendy word has no legal basis and cannot become a key concept of the directive without a clear definition of it.

Furthermore the way the term "glorification" currently used in the draft directive (recital 7 and article 5 of the Council's version) goes against the Special Rapporteur on Human Rights and counter terrorism's opinion¹. According to the latter "the offence of incitement to terrorism [...] must be prescribed by law in precise language, and avoid vague terms such as "glorifying" or "promoting" terrorism".

The European legislator should agree on a phrasing that "expressly refer to intent to communicate a message and intend that this message incite the commission of a terrorist act".

2. Measures against illegal terrorist content on the Internet

2.1 Blocking: an inefficient, disproportionate and dangerous measure

The version of the draft directive on combating terrorism adopted by the LIBE Committee on 4 July 2016 contains new provisions about illegal terrorist content on the Internet. Recital 7b as well as article 14 both created by the LIBE Committee mention clearly the blocking of websites as a potential measure that Member States may adopt.

Websites blocking is all at once inefficient, disproportionate and infringe fundamental rights. Other solutions exist but the lack of impact assessment of proposed measures,

¹ [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session31/Documents/A.HRC.31.65_AU V.docx](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session31/Documents/A.HRC.31.65_AU.V.docx)

as well of evaluation of similar measures existing in Member States such as France has not - until now - incited the LIBE Commission to go further. The arguments below going against blocking shall lead the European legislator to remove this useless and dangerous provision from the draft directive.

- Firstly **blocking is indeed simply not efficient**. This is easy to bypass any blocking by using very common and widespread tools and encrypted protocols such as a Virtual Private Network (VPN) service or the Tor Browser. The only way to have a strong blocking solution is to build a system of censorship like in China or other countries where Internet access is under surveillance. Provided that nobody wants to go in that direction, such a blocking system will remain relatively ineffective.
- Moreover **websites dedicated to the incitement of terrorism are increasingly rare**. Today the propagation of illegal terrorist content is mostly done via social networks and nobody can imagine blocking the full social network. Blocking measures against illegal terrorist content on the Internet have been introduced in France in 2014. At the beginning of 2016 the assessment of these measure made by the Commission Nationale de l'Informatique et des Libertés (CNIL) is enlightening: only 68 websites blocking had been done (against 1080 removal of content)². **The result of this measure show its deeply inappropriate and inefficient**.
- **Blocking may even be counterproductive**. Studies have shown that a big part of accused websites do not contain any illegal content and have been blocked by mistake: the risk of overblocking is obvious. In Finland several websites that criticized blocking have been blocked³. The safeguards set by the LIBE Committee in its version are not sufficient to prevent all infringements of fundamental rights that blocking represents.

2 Qualified person's report on measures to withdraw, block and declassify unlawful websites through administrative channels:

http://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_blocage_sites_internet_2016_0.pdf

3 Save the Children Finland involved in distribution of child porn : <http://ak-zensur.de/2010/04/save-the-children.html>

Thus the removal of illegal content does work more efficiently and can be - on the contrary to blocking - a more proportionate measure as specified by the 14th article added by the LIBE Committee. However, the safeguards shall be strong enough to avoid any infringement to freedom of expression and freedom of the press.

2.2. Removal must be subject to strong safeguards

Even if the European legislators only keep the "removal" as a measure against illegal terrorist content on the Internet, this should be better defined, as the current draft leave too much leeway to the Member States for the implementation of such a measure.

Today, the enforcement of the Directive 2000/31/EC on electronic commerce establish the responsibility between hosting companies and content publishers. Hosting companies must promptly remove any apparently illegal content that has been reported. This measures gives private entities a strong power to decide whether the content is illegal or not. Content inciting to terrorism offences should be precisely analysed to ensure its illegality. Legislator should always give priority to the judicial authority to make a removal order. The latter is able to assess the legality of the content and the impact of the removal on fundamental rights such as freedom of expression and information as well as to ensure the rights of the defence. A "review" procedure (as proposed by the parliament in the AM 18 adding the article 14a), understood as an *ex post* procedure, cannot sufficiently ensure fundamental rights and freedom especially when ensured by an administrative body. Indeed, an *ex post* review has not the same impact in terms of respecting freedom of expression and rights to the defence.

It is essential to work towards **better judicial procedures and international cooperation to achieve content removals respecting fundamental rights**. This would ensure a long term efficiency in a democratic system, better than delegating the arbitration and judicial power to private hosting companies or platforms.

Proposal for an alternative phrasing about illegal terrorist content on the Internet:

Recital 7 (Council version)

~~(7) The offences 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 including those related to the victims of terrorism as a way to gain publicity for the terrorists cause or seriously intimidating the population, provided that such behaviour causes a danger that terrorist acts may be committed.~~

To strengthen actions against public provocation to commit a terrorist offence, ~~and also taking into account the increased use of technology, in particular the Internet, it seems appropriate for Member States *may* to take measures to remove or to block access to webpages~~ *content* publicly inciting to commit terrorist offences. Where such measures are taken, they must be set by transparent procedures and provide adequate safeguards, in particular to ensure that restrictions are limited to what is necessary and proportionate.

(7b) An effective means of combating terrorism on the internet is to remove illegal terrorist content at source. 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 illegal content. Member States should take all necessary measures to remove ~~or to block access to web pages~~ *content* publicly inciting others to commit terrorist offences.

Where such measures are taken, they should be in line with transparent procedures and subject to adequate safeguards under the *prior* control of independent *judicial* authorities. Member States should use their best endeavours to cooperate with third countries in seeking to secure the removal of such content from servers within their territory. ~~However, when removal of illegal content at its source is not possible,~~

~~Member States should be able to put in place measures to block access from Union territory to web pages identified as containing or disseminating terrorist content. 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 illegal content extolling terrorism from their internet platforms after being duly notified about such content. Any refusal should be punishable by effective, proportionate and dissuasive sanctions. The right to judicial review should be guaranteed to the internet and social media companies and service providers.~~

Article 14a - Measures against illegal terrorist content on the Internet (EP version)

1. Member States shall take the necessary measures to ensure the prompt removal of illegal content publicly inciting others 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. ~~Where that is not feasible Member States may take the necessary measures to block the access to such content.~~
2. Those measures must be in line with transparent procedures and subject to 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. Measures on removal ~~and blocking~~ shall be ~~subject to judicial review.~~ **decided by a judicial authority, according to the rights of the defence and freedom of expression and information.**

3. Aiding and abetting terrorism: "intention" is essential

The recital 11 of the initial draft version of the Commission stated that "the provision of material support for terrorism through persons engaging in or acting as intermediaries in the supply or movement of services, assets and goods [...] should be punishable in the Member States, as aiding and abetting terrorism [...] if performed with the knowledge that these operations or the proceeds thereof are intended to be used, in full or in part, for terrorist purposes or will benefit terrorist groups".

The European Parliament by means of the LIBE Committee added an essential notion: the "intention" and thus voted a new version of the text "should be punishable in the Member States as aiding and abetting terrorism or as terrorism financing if performed with the clear intention or knowledge that these operations or the proceeds thereof are intended to be used, in full or in part, for terrorist purposes or will benefit terrorist groups".

If the Parliament was obviously going to the right direction, both versions remain dangerous and must to be modified. Indeed the only "knowledge" that a service could be used by a terrorist group makes the service provider aiding and abetting terrorism. This endangers a large number of service providers. To name but a few all encrypted communication services could fall under this provision in case of an extensive enforcement of this provision by member States. It must not be forgotten that encryption and anonymity services provide a secure and essential communication channel which is strongly defended and recommended among others by the UN Special Rapporteur on freedom of expression⁴, the European Data Protection Supervisor⁵ and they should not be endangered by any provision by the European legislator.

4 <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>

5 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22_Opinion_ePrivacy_EN.pdf

Proposal for an alternative phrasing of the recital 11 :

- (11) The provision of material support for terrorism through persons engaging in or acting as intermediaries in the supply or movement of services, assets and goods, including trade transactions involving the entry into or exit from the Union, should be punishable in the Member States as aiding and abetting terrorism or as terrorism financing if performed with the clear intention ~~or~~ **and** knowledge that these operations or the proceeds thereof are intended to be used, in full or in part, for terrorist purposes or will benefit terrorist groups.

Annex

COM proposal (doc. 14926/15)	Council GA (doc. 6655/16)	LIBE orientation vote (A8-9999/2016)	Amendments proposed by La Quadrature du Net
Recital 7			
(7) The offences 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 including those related to the victims of terrorism as a way to gain publicity for the terrorists cause or	(7) The offences 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 including those related to the victims of terrorism as a way to gain publicity for the terrorists cause or	(7) The offences 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 as a way to gather support for a terrorist cause or seriously intimidating the	(7) The offences 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 including those related to the victims of terrorism as a way to gain publicity for the

<p>seriously intimidating the population, provided that such behaviour causes a danger that terrorist acts may be committed.</p>	<p>seriously intimidating the population, provided that such behaviour causes a danger that terrorist acts may be committed. To strengthen actions against public provocation to commit a terrorist offence, and also taking into account the increased use of technology, in particular the Internet, it seems appropriate for Member States may to take measures to remove or to block access to webpages publicly inciting to commit terrorist offences. Where such measures are taken, they must be set by transparent procedures and provide adequate safeguards, in particular to ensure that restrictions are limited to what is necessary and proportionate.</p>	<p>population. Such behaviour should be punishable when it causes a danger in a concrete case that a terrorist offence may be committed.</p>	<p>terrorists cause or seriously intimidating the population, provided that such behaviour causes a danger that terrorist acts may be committed. To strengthen actions against public provocation to commit a terrorist offence, and also taking into account the increased use of technology, in particular the Internet, it seems appropriate for Member States <i>may</i> to remove or to block access to webpages content publicly inciting to commit terrorist offences. Where such measures are taken, they must be set by transparent procedures and provide adequate safeguards, in particular to ensure that restrictions are limited to what is necessary and proportionate.</p>
		(7a)Where an information society	(7a)Where an information society

		<p>service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States should ensure that the service providers not liable for the information transmitted or stored in accordance with Directive 2000/31/EC of the European Parliament and of the Council</p>	<p>service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States should ensure that the service providers not liable for the information transmitted or stored in accordance with Directive 2000/31/EC of the European Parliament and of the Council</p>
		<p>(7b) An effective means of combating terrorism on the internet is to remove illegal terrorist content at source. 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</p>	<p>(7b) An effective means of combating terrorism on the internet is to remove illegal terrorist content at source. 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</p>

		<p>flagging illegal content. Member States should take all necessary measures to remove or to block access to web pages publicly inciting others to commit terrorist offences.</p> <p>Where such measures are taken, they should be in line with transparent procedures and subject to adequate safeguards under the control of independent authorities. Member States should use their best endeavours to cooperate with third countries in seeking to secure the removal of such content from servers within their territory. However, when removal of illegal content at its source is not possible, Member States should be able to put in place measures to block access from Union territory to web pages identified as containing or disseminating terrorist content.</p>	<p>flagging illegal content. Member States should take all necessary measures to remove or to block access to web pages content publicly inciting others to commit terrorist offences.</p> <p>Where such measures are taken, they should be in line with transparent procedures and subject to adequate safeguards under the prior control of independent judicial authorities. Member States should use their best endeavours to cooperate with third countries in seeking to secure the removal of such content from servers within their territory. However, when removal of illegal content at its source is not possible, Member States should be able to put in place measures to block access from Union territory to web pages identified as containing or disseminating terrorist content.</p>
--	--	--	--

		<p>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 illegal content extolling terrorism from their internet platforms after being duly notified about such content. Any refusal should be punishable by effective, proportionate and dissuasive sanctions. The right to judicial review should be guaranteed to the internet and social media companies and service providers.</p>	<p>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 illegal content extolling terrorism from their internet platforms after being duly notified about such content. Any refusal should be punishable by effective, proportionate and dissuasive sanctions. The right to judicial review should be guaranteed to the internet and social media companies and service providers.</p>
<p>Article 14a Measures against illegal terrorist content on the internet</p>			
		<p>1. Member States shall take the necessary measures to ensure the prompt removal of illegal content publicly inciting others to commit a terrorist offence, as referred to in Article 5, that is hosted in their territory. They shall</p>	<p>1. Member States shall take the necessary measures to ensure the prompt removal of illegal content publicly inciting others to commit a terrorist offence, as referred to in Article 5, that is hosted in their territory. They shall</p>

		<p>also endeavour to obtain the removal of such content hosted outside of their territory. Where that is not feasible Member States may take the necessary measures to block the access to such content.</p> <p>2. Those measures must be in line with transparent procedures and subject to 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. Measures on removal and blocking shall be subject to judicial review.</p>	<p>also endeavour to obtain the removal of such content hosted outside of their territory. Where that is not feasible Member States may take the necessary measures to block the access to such content.</p> <p>2. Those measures must be in line with transparent procedures and subject to 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. Measures on removal and blocking shall be subject to judicial review <i>decided by a judicial authority, according to the rights of the defence and freedom of expression and information.</i></p>
Recital 11			
(11) Furthermore, the provision of material support for	(11) Furthermore, the provision of material support for	(11) The provision of material support for terrorism	The provision of material support for terrorism through

<p>terrorism through persons engaging in or acting as intermediaries in the supply or movement of services, assets and goods, including trade transactions involving the entry into or exit from the Union should be punishable in the Member States, as aiding and abetting terrorism or as terrorism financing if performed with the knowledge that these operations or the proceeds thereof are intended to be used, in full or in part, for terrorist purposes or will benefit terrorist groups.</p>	<p>terrorism through persons engaging in or acting as intermediaries in the supply or movement of services, assets and goods, including trade transactions involving the entry into or exit from the Union, such as sale, acquisition or exchange of a cultural object of archaeological, artistic, historical or scientific interest illegally removed from an area controlled by a terrorist group at the time of the removal, should be punishable in the Member States, as aiding and abetting terrorism or as terrorism financing if performed with the knowledge that these operations or the proceeds thereof are intended to be used, in full or in part, for terrorist purposes or will benefit terrorist groups. Further measures may be necessary with a view to effectively combat the illicit trade in cultural</p>	<p>through persons engaging in or acting as intermediaries in the supply or movement of services, assets and goods, including trade transactions involving the entry into or exit from the Union, should be punishable in the Member States as aiding and abetting terrorism or as terrorism financing if performed with the clear intention or knowledge that these operations or the proceeds thereof are intended to be used, in full or in part, for terrorist purposes or will benefit terrorist groups.</p>	<p>persons engaging in or acting as intermediaries in the supply or movement of services, assets and goods, including trade transactions involving the entry into or exit from the Union, should be punishable in the Member States as aiding and abetting terrorism or as terrorism financing if performed with the clear intention and or knowledge that these operations or the proceeds thereof are intended to be used, in full or in part, for terrorist purposes or will benefit terrorist groups.</p>
--	--	--	--

	goods as a source of income for terrorist groups.		
--	--	--	--

La Quadrature du Net
60 rue des Orteaux - 75020 Paris
0033 972 294 426 - contact@laquadrature.net