Council of the European Union
General Secretariat

Interinstitutional files:
2018/0331(COD)

Brussels, 26 February 2020

WK 2085/2020 ADD 1

LIMITE

CT
ENFOPOL
COTER
JAI

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a Regulation on preventing the dissemination of terrorist content online - further comments by Member States

Delegations will find in Annex a courtesy translation of the comments received from France.

Council of the European Union

Brussels, 20 February 2020
(OR. fr, en)

SN 1627/20

LIMITE

NOTE

From:	General Secretariat of the Council
On:	20 February 2020
To:	Delegations
Subject:	Comments by France concerning the draft Regulation on preventing the dissemination of terrororist content online

Note with comments

Comments by France concerning the draft regulation on preventing the dissemination of terrorist content online, following the meeting of JHA TCO counsellors on 13 February 2020.

Following the meeting of JHA TCO counsellors on 13 February 2020, the Presidency invited the Member States to submit their comments on the compromises circulated at that meeting. The compromises relate to three things:

- a proposed rewording in order to merge Articles 3, 6 and 9 into a single article on specific measures
- a clarification on Article 1 regarding the concept of 'dissemination to the public'
- new wording regarding the transparency obligations for competent authorities.

Generally speaking, the compromises are a step in the right direction and reassert certain basic principles.

Dissemination to the public *(Articles 1 and 2)*

Explanations given by the Commission in support of the Presidency's compromise proposal

The Commission itself recognises that the content disseminator's ability to choose the people to whom the content is addressed via the hosting service provider is a commonly applied criterion in Community legislation, particularly as regards interpersonal communication services. However, this criterion is not included in the concept of 'dissemination to the public' in the proposed compromise, which is based solely on the 'potentially unlimited number of persons' who might access the content.

The comparison made by the Commission with copyright *acquis* does not seem pertinent as the logic in that case is different to the logic underlying the prevention of the dissemination of terrorist content online. Nevertheless, as regards this issue, it can be noted that the Court did indeed acknowledge and recall in the *Reha Training* judgment the logic of applying a *de minimus* threshold to determine if there is a public and, therefore, a communication to the public, but that it did not require that the communication necessarily be addressed to the general public in its entirety. On the contrary, by introducing the concept of a 'new public' to determine in some cases whether or not a communication to the public took place, it acknowledged that the extent of the concept of 'public' is variable. More generally speaking, the assessment of an act of communication to the public depends on a variety of parameters. And the judgment referred to by the Commission, and particularly the reasoning developed in points 40 to 45 thereof, says nothing to the contrary.

Wording proposed by the Presidency for the concept of 'dissemination to the public'

We consider that the wording provides a good basis for negotiation but that it would benefit from being clarified.

We consider that the phrase 'to a potentially unlimited number of persons' as it appears in Article 2(6) and within the context of recital 10a is problematic; this is because it causes confusion by possibly suggesting that the concept of public dissemination is limited to cases in which the dissemination is addressed to the totality of internet users.

This wording could be interpreted to mean that the mere fact of placing certain limits on the visibility of content would result in it not being possible to ever consider it public. Such limits may have been planned by the hosting provider (a number of people in a group) or by the user (limited dissemination within a restricted circle of friends, friends of friends, etc.).

It must therefore be possible to assess the public nature of the dissemination on a case-by-case basis, with due regard in particular for the visibility parameters and the potential audience, which need not be unlimited. By way of example, French case-law has held that content posted on a Facebook wall open only to 'friends' is not public since it is accessible only to a limited number of persons approved by the account holder (Court of Appeal of Versailles, Third Chamber, 18 June 2015, 13-03453); **on the other hand, however, where it is also accessible to 'friends of friends' - the number of whom cannot be controlled**, and who do not constitute a community of interests - such content is public (Court of Appeal of Douai, 11 September 2014, no 14/02540).

The value of this approach is that it prevents the text from having the effect of - for example - excluding from the scope of application messaging services such as Telegram (which can host up to 230 000 participants, and which may be accessed via a simple hyperlink, without the approval of the group's moderators) or Rocket.Chat, or a platform which might decide that content should be visible only to x number of persons, where x represents an extremely large number. Finally, and by way of example, a Telegram user can also create a channel, whose function is equivalent to that of a platform insofar as it enables content to be shared with an unlimited number of recipients.

We therefore take the view that it would be appropriate to delete the words '*to a potentially unlimited number of persons*' in the definition and in recital 10a, to delete the third and fourth sentences of proposed recital 10a and to adapt the latter to specify other criteria which may be used to assess the public or non-public nature of dissemination on a case-by-case basis. Such assessment could cover such factors as the limited number of persons approved, the community of interests which may or may not be formed by the members of a group on a platform such as Facebook, or the question of whether the content may be accessed only by persons approved by the account holder.

We therefore reiterate our amendment to the compromise proposal as follows:

Compromise proposal on "public"

Art. 1

Para. 1:

This Regulation lays down uniform rules to prevent the misuse of hosting services for the dissemination ***to the public*** *of terrorist content online. It lays down in particular [etc.]*

Para. 2:

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

Art. 2

Para. 1:

*'hosting service provider' means a provider of information society services consisting of the storage of information provided by and at the request of the content provider [****rest deleted****]*

Para. 6:

'dissemination to the public' means ~~the~~ making ~~available of~~ information ***easily accessible to users without further action by the content provider being required, irrespective of whether one or more users actually access the information in question*** ***~~, at the request of the content provider, to a potentially unlimited number of persons.~~***

Recitals

(10) In order to effectively tackle terrorist content online, while ensuring respect for the private life of individuals, this Regulation should apply to providers of information society services which store and disseminate to the public information provided by a recipient of the service at his or her request, irrespective of whether this activity is of a mere technical, automatic and passive nature. The concept of "storage" should be understood as holding data in the memory of a physical or virtual server. Providers of "mere conduit" or "caching" services as well as of other services provided in other layers of the internet infrastructure, which do not involve such storage, such as registries and registrars as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services therefore fall outside the scope of this Regulation.

(10a) The concept of "dissemination to the public" should entail ~~the making available of information to a potentially unlimited number of legal or natural persons that is~~, making the information easily accessible to users ~~in general~~ without further action by the content provider being required, irrespective of whether ~~those persons~~ one or more users actually access the information in question. ***While in many cases, the dissemination of terrorist content to a group of individuals approved by the account holder on a social network and bound by a community of interest should not be considered as public dissemination, the mere possibility to create groups of users of a given service does not, in itself, mean that this Regulation does not apply****.*

The public nature of the dissemination shall be assessed on a case by case basis. ~~*However, the Regulation does not apply to closed groups consisting of a finite number of pre-determined persons*~~. *Interpersonal communication services, as defined in [the Telecommunications Code (Dir. 2018/1972)] such as emails or private messaging services,* ***should in principle*** *fall outside the scope of this Regulation* ***as it relates to private correspondence. However, such services should be included in the scope of the Regulation when a content is made available to the public at the direct request of the content provider.*** *Information should be considered stored and disseminated to the public within the meaning of this Regulation only where such activities are performed upon direct request by the content provider. Consequently, providers of services such as cloud infrastructure, which are provided at the request of other parties than the content providers and only indirectly benefit the latter, should not be covered by this Regulation. By way of example, included in the scope of this Regulation are providers of social media, video, image and audio-sharing, as well as file-sharing and other cloud services, in as far as those services are used to make the stored information available to the public at the direct request of the content provider. Where a service provider offers several services, some of which fall within the scope of this Regulation, this Regulation should be applied only in respect of the services that fall within its scope.*

(10b) Terrorist content is often disseminated to the public through services provided by service providers established in third countries. In order to protect users in the Union and to ensure that all service providers operating in the Digital Single Market are subject to the same requirements, this Regulation should apply to all providers of relevant services offered in the Union, irrespective of their country of main establishment. The determination as to whether a service provider offers services in the Union requires an assessment whether it enables legal or natural persons in one or more Member States to use its services and has a substantial connection to that Member State or Member States, in particular an establishment that is relevant to the provision of those services or, in the absence thereof, other specific factual criteria pointing to such a substantial connection. However, the mere accessibility of a service provider's website or of an email address or of other contact details in one or more Member States, taken in isolation, should not be a sufficient condition for the application of this Regulation.

Specific measures *(new article merging Articles 3, 6 and 9)*

We are satisfied with the new proposed wording (distributed at the meeting of 31 January 2020) on specific measures. We commend the Presidency on its drafting work, which enshrines the obligatory nature of these measures whilst striking a balance with respect for fundamental rights. We can therefore issue a positive opinion on this compromise proposal, subject to the following points being taken into account.

- point 2 of the attached document: we suggest replacing the sentence '*it shall take specific measures to protect their services against the dissemination of terrorist content*' with '*It shall take specific measures to make sure their services are not used to disseminate terrorist content*'. We also propose replacing '*Those measures **may** include, in particular, one or more of the following*' with '***must***' or '***shall***'.

- point 4: we wonder why no reference is made to Europol's Internet Referral Unit (IRU), which is playing an increasingly significant role in the fight against unlawful online content at the European level.

- point 5: we would point out that meeting the 'golden hour' objective will not be possible with a time limit of 'three months'. A time limit of one month maximum would be more suitable.

- point 7: we suggest replacing '*within a reasonable time period*' with '*within a month*', to reflect point 5.

Transparency obligations of the competent authorities *(Article 8a)*

We support the proposed wording of Article 8a on the transparency obligations of the competent authorities.

Definition of terrorist content *(Article 2)*

We support the compromises proposed by the Presidency, with the exception of line 93. This definition adds a condition to the Council definition ('*where such material, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences*'), making it more restrictive.

Moreover, in the Parliament proposal on the '*depiction*' of terrorist offences (line 97), the words '*thereby causing a danger that further such offences be committed*' should be deleted. Based on the wording, and given its placement in recital 9, this phrase would apply not only to content inciting terrorist offences, but also to instructions for making explosives and, more generally, to all terrorist

content (recruitment, threats, etc.). Yet the condition of a 'danger that [...] offences be committed' only makes sense for incitement.

Finally, we support the proposal to move the exclusion of journalistic, educational, scientific or artistic content to Article 2(5). In substance, however, the Parliament's wording remains unacceptable, in that theoretically there is nothing preventing content published for journalistic purposes, for example, from also being published for terrorist purposes. The Commission proposal, which suggests 'taking into account' fundamental freedoms when assessing whether content constitutes terrorist content seems more balanced and could be an appropriate compromise.

]