



Council of the
European Union

058316/EU XXVI. GP
Eingelangt am 18/03/19

Brussels, 18 March 2019
(OR. en)

15729/18

Interinstitutional File:
2018/0331(COD)

CT 206
ENFOPOL 631
COTER 194
JAI 1327
CYBER 333
TELECOM 495
FREMP 245
AUDIO 136
DROIPEN 222
COHOM 184
CODEC 2400

COVER NOTE

From: General Secretariat of the Council
date of receipt: 18 December 2018
To: Delegations

Subject: Proposal for a Regulation of the European Parliament and of the Council
on preventing the dissemination of terrorist content online
= Opinion of the European Economic and Social Committee

Delegations will find attached the opinion of the European Economic and Social Committee on the above-mentioned subject.

Please note that other language versions should be available at:

<https://dm.eesc.europa.eu/EESCDocumentSearch/Pages/opinionssearch.aspx>

15729/18

AC/mr

JAI.1

EN



European Economic and Social Committee

SOC/609

Preventing the dissemination of terrorist content online

OPINION

European Economic and Social Committee

Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online

A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018

[COM(2018) 640 final - 2018-0331 (COD)]

Rapporteur: **José Antonio MORENO DÍAZ**

Referral	European Council, 24/10/2018 European Parliament, 22/10/2018
Legal basis	Articles 114(1) and 304 of the Treaty on the Functioning of the European Union
Section responsible	Section for Employment, Social Affairs and Citizenship
Bureau decision	11/12/2018
Adopted at plenary	12/12/2018
Plenary session No	539
Outcome of vote (for/against/abstentions)	126/0/3

1. Conclusions and proposals

- 1.1 The EESC welcomes the initiative, which seeks greater security for the inhabitants of the EU: however, in the debate between security and freedom the Committee has always upheld the need to defend the freedoms, including freedom of expression, freedom of access to information and communication, and the confidentiality of communications. Ultimately, this means access to effective legal protection and to fair and prompt proceedings.
- 1.2 The recent terrorist attacks on EU soil have demonstrated how terrorists misuse social networks to recruit and groom supporters. Terrorists use encrypted communications to prepare and facilitate terrorist activity, and the web to glorify their atrocities, urge others to follow suit and instil fear in the general public.
- 1.3 The EESC calls for the clearest possible criteria to be devised to define vague legal concepts such as "terrorist information", "terrorist acts", "terrorist groups" or "glorifying terrorism".
- 1.4 Terrorist content shared online for such purposes is disseminated through hosting service providers that allow the upload of third party content. Terrorist content online has proven instrumental in radicalising and inspiring attacks from so-called 'lone wolves' in several recent terrorist attacks within Europe.
- 1.5 Technological means of prevention (automated parameters, algorithms, search engines, etc.) are very useful, but the intervention of a human as mediator and intermediary is crucial in accurately assessing this content.
- 1.6 The EESC highlights the need to combat the dissemination of terrorist information and digital recruitment on social networks. At the same time, censorship or forced self-censorship on the internet should be opposed. The Committee recalls that, where the internet is concerned, it is essential to guarantee the effective right to information and freedom of expression for everyone living in the EU.
- 1.7 Protecting the internet and combating radical groups should help to boost trust in the internet and thus ensure the economic development of this economic sector.
- 1.8 The EESC emphasises the need to assess the impact that applying this proposal would have on small- and medium-sized enterprises, together with the possibility of temporary application which would make it easier for them to adapt and would not distort free competition to the benefit of large-scale operators.

- 1.9 The regulatory measures proposed to protect the internet and safeguard the population in general, and young people in particular, must be strictly governed by law and guarantee everyone the right to information and to appeal against administrative decisions.
- 1.10 The EESC also emphasises the need to assess access providers, and for social network managers to take proactive measures to promote reporting and direct action by associations, NGOs and users against such content: these "counter-arguments" must be effectively deployed if they are to have a preventive effect.
- 1.11 The large number of digital platforms at European level and the different sizes of these businesses must be reflected in the way the terms of the proposal are adapted for small businesses of this kind.
- 1.12 The EESC emphasises that users must be clearly reminded of the national rules on the production of terrorist content. It also calls for the right to appeal against an administrative decision to be guaranteed with a clear explanation of this right and online tools for its exercise.

2. **Context of the proposal**

- 2.1 The ubiquity of the internet allows its users to communicate, work, socialise, create, obtain and share information and content with hundreds of millions of individuals across the globe: in consequence, the Commission proposes to introduce mechanisms to prevent the communication and dissemination of terrorist content¹.
- 2.2 It is important to distinguish between concepts, and the term "internet" is thus too broad. Internet simultaneously refers to the web, to social networks and to the darknet. It also includes the internet of things, which constitute clear security loopholes in electronic warfare. ISIS recruiters, for example, currently communicate more easily via online game consoles than through the web. The expression "to prepare and facilitate terrorist activity" does not apply to internet or the social networks, but to the darknet. The major GAFAM online companies are not active on the darknet or encrypted networks.
- 2.3 However, the ability to reach such a large audience at minimal cost also attracts criminals who want to misuse the internet for illegal purposes. Recent terrorist attacks on EU soil have demonstrated how terrorists misuse the internet to groom and recruit supporters, to prepare and facilitate terrorist activity, to glorify in their atrocities and urge others to follow suit and instil fear in the general public.

¹ [COM\(2018\) 640 final](#).

- 2.4 While the EU Internet Forum brought together a number of actors, not all hosting service providers have engaged in it and, moreover, the scale and pace of progress among hosting service providers as a whole is not sufficient to adequately address this problem. A specific effort must be made in favour of proper training for social network moderators.
- 2.5 Terrorist content shared online for such purposes is disseminated through hosting service providers that allow the upload of third party content. Terrorist content online has proven instrumental in radicalising and inspiring attacks from so-called "lone wolves" in several terrorist attacks within Europe. The strongest influence has been detected among the younger sectors of the population.

3. **Summary of the proposed Regulation and general comments**

- 3.1 The EESC has already set out its position on illegal online content²: this new Commission initiative specifically concerns online terrorist content.
- 3.2 The personal scope of the proposal includes hosting service providers who offer their services within the EU, regardless of their place of establishment or their size.
- 3.3 We consider that providers of information, search engines, and hosting sites or networks should also be included.
- 3.4 Small- and medium-sized internet companies do not have the technical, human or financial capacity to act effectively against terrorist content. The EESC considers that timeframes and procedures need to be adapted for this type of business. SMEs could be allowed a certain amount of time to implement the Regulation.
- 3.5 Preventive and proactive measures taken by NGOs, trade unions and civil society in general must also be highlighted.
- 3.6 To ensure the removal of terrorist content, the Regulation introduces a removal order which can be issued as an administrative or judicial decision by a competent authority in a Member State. In such cases, the hosting service provider is obliged to remove the content or disable access to it within one hour.
- 3.7 The definition of terrorist content may vary from country to country, and it is important to make this clear in order to avoid arbitrary decisions and legal uncertainty.

² [OJ C 237, 6.7.2018, pp. 19-25.](#)

- 3.8 The one-hour timeframe is unrealistic. In France, for example, the current time-lag between a source being reported and being removed is 16 hours for paedophile sites and 21 hours for terrorist sites, as classifying sites is very time-consuming. The EESC considers that a more realistic and effective timeframe should be introduced.
- 3.9 The Regulation requires hosting service providers, where appropriate, to take proactive measures proportionate to the level of risk and to remove terrorist material from their services, including by deploying automated detection tools. This is crucial and we must call for and support technological innovation in order to create technological tools.
- 3.10 The Commission proposes the use of instruments such as automated detection, and urges companies to step up efforts to support research geared to the production of appropriate technological tools.
- 3.11 As part of the measures to protect content which is not terrorist content from erroneous removal, the proposal sets out obligations to put in place remedies and complaint mechanisms to ensure that users can challenge the removal of their content. In addition, the Regulation introduces obligations on transparency for the measures taken against terrorist content by hosting service providers, thereby ensuring accountability towards users, citizens and public authorities.
- 3.12 Emphasis must be placed not only on the scrutiny and review of content, but also on human and technological mediation. The issue of censorship by human mediators may give rise to serious concern in terms of respect for workers' rights, as well as compliance with the rules on the right to information and respect for the private life of everyone living in the EU.
- 3.13 The EESC considers that the provider should notify the owner of the site or information to be censored. It must be borne in mind that people have a right to be informed of an administrative decision.
- 3.14 In order to guarantee people's rights regarding administrative decisions, the EESC calls on access providers to indicate, in their content policies, clients' rights and obligations, such as how information producers are to be informed of removal decisions and the legal arrangements available to clients.

4. Explanation of the provisions of the proposal

4.1 Terrorists' online propaganda seeks to incite individuals to carry out terrorist attacks, including by equipping them with detailed instructions on how to inflict maximum harm. Further propaganda is commonly released after such atrocities, whereby they glorify in these acts, and encourage others to follow suit. This Regulation contributes to the protection of public security, by reducing the accessibility of terrorist content that promotes and encourages the violation of fundamental rights.

4.2 For the purposes of the Regulation, the proposal lays down the following definitions:

"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 parties³;

"content provider" means a user who has provided information that is, or that has been, stored at the request of the user by a hosting service provider⁴;

the EESC proposes that a new point be added including the following:

- "information providers": search engines that enable identification of and access to content.

4.3 Regarding the definition of "terrorist content" as one or more of the following items of 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 offences⁵;

the EESC proposes that a new point be added including the following:

- recruitment and training of persons with the aim of committing or supporting terrorist acts.

³ [COM\(2018\) 640 final – Article 2\(1\).](#)

⁴ [COM\(2018\) 640 final – Article 2\(2\).](#)

⁵ [COM\(2018\) 640 final – Article 2\(5\).](#)

- 4.4 The definition of the content to be censored is very brief as there are many texts, images, videos and other content and formats that do not glorify terrorism - because they do not incite to specific acts - but facilitate and highlight extremist theories that lead to violence.
- 4.5 The Regulation also helps to tackle companies which, through their activities, facilitate and highlight extremist theories that lead to violence. It must also contribute to combating recruitment via social networks.
- 4.6 Article 1 sets out the subject matter, indicating that the Regulation lays down rules to prevent the misuse of hosting services for the dissemination of terrorist content online, including duties of care on hosting service providers and measures to be put in place by Member States.
- 4.7 The expression concerning the misuse of hosting services to disseminate terrorist content online should be replaced, by adding the dissemination of propaganda content, messages or media and including an indication of URLs and information for access to terrorist content or messages, as this would also cover search engines.
- 4.8 Article 5 lays down a requirement for hosting service providers to put in place measures to expeditiously assess content referred through a referral from either a competent authority in a Member State or an EU body without however imposing a requirement to remove the content referred nor does it set specific deadlines for action.
- 4.9 The EESC considers that in order to be effective, work should begin on a list of a set number of criteria for defining types of content and messages that are either terrorist in nature or glorify terrorism, with the aim of providing legal certainty so as to avoid arbitrary decisions on removal of content and also to safeguard the rights to information and freedom of opinion. The Regulation should also add the criteria needed to make it possible, at European level, to describe content such as information on terrorist groups, information that glorifies or justifies terrorism, technical or methodological information facilitating the manufacture of weapons that can be used in attacks, or appeals for recruitment.
- 4.10 Article 14 provides for the establishment of points of contact by both hosting service providers and Member States to facilitate communication between them, particularly in relation to referrals and removal orders. In order to safeguard the relevant human rights, the EESC considers that these points of contact must include specialist judges who can identify problems and are trained not only to identify attitudes, behaviour or actions of a terrorist nature, but also in technological skills. These abilities should also be required of both hosting service providers and Member State appointees, to facilitate communication between them, particularly in relation to referrals and removal orders.

- 4.11 The Regulation should stipulate that hosting service providers must supply information accessible to all so that the points of contact can function properly, as well as defining the content and form of communication with the members of these contact points.
- 4.12 Article 16 requires hosting service providers which do not have an establishment within any Member State but which do offer services within the EU, to designate a legal representative in the EU: in the Committee's view, this requirement should be extended to access providers and internet industries so as include search engines, social networks, internet phone applications and the gaming industry.
- 4.13 Hosting service providers active on the internet play an essential role in the digital economy by connecting business and citizens and by facilitating public debate and the distribution and receipt of information, opinions and ideas, contributing significantly to innovation, economic growth and job creation in the EU. The EESC considers that it should also be extended to internet service providers, content hosting services, digital social networks and digital telephony companies.
- 4.14 The proposal for a Regulation introduces 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 EU bodies. The EESC considers the purpose of this to be to limit terrorism-related content, enable it to be swiftly deleted by hosting service providers and reduce terrorist propaganda and recruitment via the internet.

Brussels, 12 December 2018

Luca Jahier

The president of the European Economic and Social Committee
