

# **Comments on leaked draft Terrorist Content Regulation**

### March 2020

#### Introduction

- 1. ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19) is an independent human rights organisation that works around the world to protect and promote the rights to freedom of expression and freedom of information. ARTICLE 19 has significant experience working on the impact of terrorism legislation on freedom of expression. For instance, we have analysed Spain's implementation of the Terrorism Directive,<sup>1</sup> the UK Counter Terrorism and Border Security Bill<sup>2</sup> and Russia Extremism legislation,<sup>3</sup> among others. We are closely following the work of the Global Internet Forum on Countering Terrorism (GIFCT) and are a member of the Christchurch Call to eliminate terrorist and violent extremist content online.
- 2. In this briefing, ARTICLE 19 outlines our key concerns with the proposed draft Terrorist Content Regulation (Draft Regulation), as leaked on 06 March 2020.<sup>4</sup> In our view, it is an extremely regressive piece of legislation that fails to protect human rights, in particular the rights to freedom of expression and privacy and data protection. We are particularly concerned about proposals for mandatory filters, obligations to remove broadly defined terrorist content within one hour and insufficient procedural safeguards for the protection of freedom of expression and privacy online. As the end of the trialogue negotiations draws near, ARTICLE 19 urges the European Commission and the European Council to follow the lead of the European Parliament to protect users' rights to freedom of expression and data protection and amend the draft Regulation.

# Subject matter and scope

- 3. The European Commission and European Council propose that the Draft Regulation should apply to the dissemination of "terrorist content online" rather than the *public* dissemination of such content.<sup>5</sup>
- 4. ARTICLE 19 notes that this broad wording means that in practice the obligations set out in the Regulation would be applicable not only to social media platforms but also to a range of information society providers such as cloud infrastructure providers and providers of private

<sup>&</sup>lt;sup>1</sup> ARTICLE 19, Spain: Speech related offences of the Penal Code, March 2020.

<sup>&</sup>lt;sup>2</sup> ARTICLE 19, <u>House of Commons Public Bill Committee – Counter-Terrorism and Border Security Bill 2018</u>, Written Evidence, June 2018.

<sup>&</sup>lt;sup>3</sup> ARTICLE 19, Rights in extremis: Russia's anti-extremism practices from an international perspective, September 2019.

<sup>&</sup>lt;sup>4</sup> Politico, <u>Leaked Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online</u>, March 2020.

<sup>&</sup>lt;sup>5</sup> See Article 1 of the Draft Regulation.

messaging services. Put it differently, private conversations on Messenger, WhatsApp, Signal and other messaging apps would fall within its scope. So would any conversations or materials stored in the Cloud. If adopted, this would be a serious – and in our view disproportionate - interference with the right to privacy, particularly given the other measures proposed by the European Commission and the Council (see further below).

- 5. By contrast, the European Parliament has been trying to limit the scope of the Regulation to the public dissemination of terrorist content and exclude private communications and cloud infrastructure providers. In addition, the European Parliament is proposing to make explicit that the Regulation should not apply to "content disseminated for educational, artistic, journalistic or research purposes, nor to content which represents an expression of polemic or controversial views in the course of public debate."
- 6. In our view, the European Parliament's approach is much more proportionate than the Commission's or the Council's. It is also more consistent with existing EU legislation in this area, namely Article 5 of the Terrorism Directive 2017 (2017 Directive). While the Terrorism Directive itself raises human rights and freedom of expression concerns, the European Parliament should be encouraged to hold its ground on these two issues for the purposes of the Regulation.

#### Recommendation:

- The scope of the Terrorist Content Regulation should be limited to the *public* dissemination of 'terrorist' content, which ought to be defined in line with international standards on freedom of expression;
- The Terrorist Content Regulation should make clear in the recitals and the main body of the text that freedom of expression must be protected when determining whether content ought to be removed as 'terrorist.' This could be achieved, *inter alia*, in the way suggested by the European Parliament in its latest proposal.

### **Definitions**

- 7. Under the Draft Regulation, 'terrorist content' is defined primarily by reference to Article 3(1) of the 2017 Directive as well as by language largely borrowed from Article 5 of the 2017 Directive. Whilst Article 3(1) of the 2017 Directive requires Member States to prohibit a number of terrorist acts such as attacks on a person's life or kidnapping, Article 5 requires Member States to prohibit the public provocation to commit terrorist offences.
- 8. The proposal from the Commission uses broader language such as 'encouraging the contribution to terrorist offences', 'promoting the activities of a terrorist group by encouraging the participation or support to a terrorist group' or 'instructing on methods or techniques for the purpose of committing terrorist offences'.
- 9. For its part, the European Parliament (EP) had originally introduced a subclause whereby terrorist content would have included the depiction of the commission of terrorist offences 'thereby causing a danger that one or more such offences may be committed intentionally." However, the latest European Parliament's proposals suggest replacing this subclause with a recital clarifying that terrorist material includes 'live transmissions of terrorist offences thereby causing a danger that further such offences may be committed.'
- 10. ARTICLE 19 is concerned by the various proposed definitions of 'terrorist content' in the Draft Regulation:

- Use of overbroad terms: in our view, the definitions contained in the Draft Regulation are generally inconsistent with international standards on freedom of expression that recommend avoiding the use of vague terms such as 'glorifying' or 'promoting' terrorism. Part of the problem stems from the fact that the underlying offence of 'public provocation to commit terrorism' under Article 5 of the 2017 Directive is itself drafted in overly broad language in a number of places. In particular, it requires Member States to prohibit the dissemination of messages to the public that indirectly advocate the commission of terrorist acts, thereby causing a danger that one or more such offences may be committed" (our emphasis). None of these terms are defined. It is entirely unclear, for example, what level of actual risk of the terrorist acts occurring is necessary for the offence to be committed. We note that in English, the word that would tend to suggest that there is a high probability or about 51% risk that a terrorist act will be committed, is 'likely.' By contrast, the word 'may' indicate a much lower threshold.
- Undue inclusion of live transmissions of terrorist offences: we are also concerned that the live transmission of terrorist offences could be treated as 'terrorist' content under the current European Parliament's proposal. We note that nobody suggested that for instance, during the live broadcast of the terrorist attacks on the World Trade Centre in New York city that such content should be treated as terrorist material likely to induce similar attacks, though it may well have been. We also observe that in some countries, such as Turkey, the government has sought to ban coverage of terrorist attacks on both traditional and social media, often in order to prevent scrutiny of its own actions.<sup>6</sup> There is also a very real concern that these kinds of provisions could be misused in the context of protests that turn violent such as the Gilet jaunes or Catalan independence movements. Whilst we understand concerns with some live videos (such as those in the wake of the Christchurch terrorist attacks), it is important to distinguish videos that are published by terrorist themselves with a clear intent to incite similar actions or discrimination from footage posted by victims, bystanders or journalists with a view to reporting on live events.
- 11. ARTICLE 19 suggests that in order for offences of incitement to commit acts of terrorism to be compatible with international standards on human rights, they, at least, (a) must be defined strictly, avoiding vague terms such as 'glorifying', 'encouraging', 'promoting', 'advocating' 'supporting' or 'contributing'; (b) must include an actual (objective) risk that the act incited will be committed; and (c) should include a requirement of *intent* to communicate a message and intent that the message at issue incites the commission of a terrorist;<sup>7</sup>

## **Recommendation:**

- The offences of incitement to commit acts of terrorism in the Draft Regulation must be revised, including by ensuring that they are defined more strictly, include a requirement of intent and an actual (objective) risk that the act incited will be committed;
- The definition of terrorist content should clearly and explicitly exclude content published for journalistic, educational, research, artistic or other lawful purposes;
- References to live transmissions of terrorist should be removed. In the alternative, a new recital should clarify that any removal of such material should be consistent with the protection of freedom of expression and media freedom.

# **Duties of care**

<sup>&</sup>lt;sup>6</sup> ARTICLE 19, <u>Turkey: Government must protect Protest and Debate after Ankara Attack</u>, 15 October 2015

<sup>&</sup>lt;sup>7</sup> See for more details UN Special Rapporteur on Counter Terrorism, A/HRC/31/65, 2016, para 24.

- 12. ARTICLE 19 is concerned that the Draft Regulation makes reference to 'duties of care' without making any serious attempt at defining what this means, save for the European Parliament's proposal that it should not amount to a general monitoring obligation. Indeed, in our experience, 'duties of care' often imply 'proactive measures' or 'general monitoring obligations', which is a source of grave concern for reasons we outline further below. In our view, it is also vital that the relationship between the Terrorist Content Regulation and the E-Commerce Directive (ECD) is clarified in the text of the Regulation as proposed by the European Parliament.<sup>8</sup> In particular, the liability exemptions under Articles 12-14 ECD and the prohibition on general monitoring under Article 15 ECD should remain applicable, lest information society providers are incentivised to remove greater volumes of content at the expense of freedom of expression.
- 13. We also note with concern that the European Parliament is proposing that hosting providers who obtain 'knowledge' or 'awareness' of terrorist content on their services should have a duty to report such content to the authorities and remove it expeditiously. In our view, this language is problematic for two reasons.
  - First, it suggests that hosting providers would be required to inform the authorities every time their own systems detect 'terrorist' content since mere 'knowledge' rather than 'actual' knowledge is required. Given that platforms now identify millions of pieces of content automatically, this means that companies would have to devote considerable resources to report those pieces of content, potentially at the expense of other measures. It would also likely overwhelm the authorities who would then have to sort through this content to decide which one should lead to prosecutions.
  - Second, we find that the proposed language in Article 3(2)(b) of the Draft Regulation fails to clarify the relationship between knowledge obtained by hosting providers as a result of their own systems, the reporting duty and what this means for the purposes of the liability exemption under Article 14 of the ECD. In other words, this proposal could well undermine the EP's own proposed text at Article 1 (2) (c).

# Recommendation:

- The text of the Terrorist Content Regulation should make clear that it is without prejudice to the application of the ECD and other relevant EU legislation, such as the Audio-Visual Media Services Directive (AVMSD);
- Reference to 'duties of care' should be avoided altogether; in the alternative, we support the EP's proposal to clarify that this should not amount to a general monitoring obligation;
- The Terrorism Regulation should make clear the relationship between any reporting duty and immunity from liability under Article 14 ECD.

#### Removal orders

14. Article 4 of the Draft Regulation provides for removal orders. Under the Commission's proposal, removal orders would be issued by a 'competent authority.' To be valid, removal orders would have to contain certain elements, including the identification of the competent authority and authentication of the removal order, a statement of reasons as to why the content is considered 'terrorist', a URL, a reference to the Draft Regulation as the appropriate legal basis for the order, date and time stamp, information about redress available to the hosting provider and content

<sup>&</sup>lt;sup>8</sup> At proposed Article 1 (2) (c).

provider, and where appropriate a decision not to disclose information about the removal order. Upon receipt of the order, the hosting provider would have to remove the content or disable access to it within one hour. Hosting providers would be able to ask for more detailed reasons for the removal where appropriate. They would have to acknowledge receipt and inform the competent authority about the removal, including the time at which action was taken. If compliance with the order is impossible in practice for reasons 'not attributable to it' or because of force majeure, hosting providers would have to inform the competent authority without delay. Finally, the competent authority issuing the order would have to inform the competent authority that oversees the implementation of proactive measures when an order has become final.

- 15. The European Parliament's proposal replicates many of the steps set out in the Commission's proposal, albeit with generally stricter requirements for valid notices. Under its proposal, removal orders would be issued by the competent authority of the Member State of main establishment of the hosting service provider (main competent authority). Such orders would be applicable in all Member States. Meanwhile, the competent authorities of other Member States could order access to be disabled to terrorist content within their own territory. Notified content would have to be removed 'as soon as possible and within one hour' from receipt of the order. To be valid, removal orders would have to contain information similar, though generally more detailed and specific, than the information required under the Commission's proposal. Redress would have to be available both with the competent authority and the courts. The European Parliament's proposal further makes clear that a hosting provider could refuse to execute an order when it contains manifest errors or does not contain sufficient information.
- 16. The defining feature of the European Parliament's proposal however is that it creates both a consultation procedure and a cooperation procedure for issuing additional removal orders between Member States. Under the consultation procedure, the main competent authority can raise concerns about the impact of an order made by the competent authority of another Member State on the fundamental interests of that Member State. Under the cooperation procedure, the competent authority that only has authority to enforce an order within its territory can request the main competent authority to issue the same order but applicable in all the Member States. The main competent authority has one hour to accept or refuse the request. If it needs more time, it can ask the hosting provider to disable access to the content at issue for 24 hours, after which time it must notify it of its decision to grant or refuse the request.

### 17. ARTICLE 19 has a number of serious concerns with the removal procedure:

• Lack of guaranteed independence of the competent authority: we note that the Draft Regulation fails to guarantee the independence of the competent authority issuing removal orders. In our view, such orders should be made by the courts, whose role is to determine the legality of content. As such, the Draft Regulation should either replace 'competent authority' with 'judicial authority' or at least make clear that the competent authority must be independent. The removal of content is a serious interference with the right to freedom of expression. It is nothing less than censorship. For this reason, we believe that, like data protection rights, it should only be authorised by a court or independent authority (see, mutatis mutandis, Digital Rights Ireland). We further note that in some countries such as Spain, for instance, terrorist removal orders are made by the courts. In our view, the Regulation should under no circumstances be used to lower due process standards across the EU by encouraging removal orders to be made by law enforcement authorities.

•

<sup>&</sup>lt;sup>9</sup> See e.g. ARTICLE 19's analysis of the Spain Penal Code, op.cit.

- Unduly short removal timeframes: we are dismayed that the European institutions continue to believe that a balanced assessment of terrorist content can be made within one hour. Such short timeframes only demonstrate that the EU is not serious about protecting freedom of expression. In particular, it is well-known that whether or not content amounts to incitement to terrorism is a typically context-specific assessment. As noted by Facebook, such a blunt time-to-action approach is also likely to be counter-productive since it implies that companies will have to examine all requests immediately rather than prioritise the most serious ones.<sup>10</sup>
- Cross-border due process and geographical scope: we are concerned that the proposed consultation and cross-border cooperation mechanisms enable the removal of content across the EU in circumstances where there is no guarantee that a court would be examining the proportionality of such a measure. Moreover, it is unclear how users would be able to challenge or otherwise be involved in the consultation or cooperation procedures. In any event, we believe that users should be able to challenge decisions to remove content across the EU in the Member State where the hosting provider has its legal establishment. In our view, this is necessary to guarantee the rights to an effective remedy and freedom of expression since the legality of terrorist content may vary from country to country. Further, or in the alternative, we note that in France, the authorities are currently required to inform a competent qualified person sitting within the data protection authority CNIL whenever a removal order is issued. 11 The qualified person makes a recommendation in relation to the decision at issue and if the police refuse to follow it, the qualified person can take matters to court. Therefore, ARTICLE 19 believes that the EU institutions should at the very least explore putting in place a similar safeguard, akin to a public interest advocate, that would enable fundamental rights issues to be aired in proceedings. This would be particularly important in the absence of any other way for users to challenge removal orders.
- 18. ARTICLE 19 further notes that under proposed Article 5 (Referrals), the Draft Regulation would codify existing practice whereby law enforcement file removal requests with tech companies, who are not under any obligation to comply with them. In our view, removal requests of this kind are problematic since they allow law enforcement authorities to bypass the normal legal process for the removal of content and make it harder to challenge those removals. Moreover, there is currently little to no transparency on the use of such requests by law enforcement authorities. Whether or not Article 4 is adopted, law enforcement authorities should at least be required to publish detailed data about their requests to tech companies to remove content.

# **Recommendations:**

- Removal orders should be made by a court or independent adjudicatory body;
- Compliance with removal orders should take place within a reasonable timeframe, e.g. 7 days. If, however, the situation is urgent, e.g. someone's life is at risk, law enforcement should be given statutory powers to order the immediate removal or blocking of access to the content at issue. Any such order should be confirmed by a court within a specified period of time, e.g. 48 hours;
- Any cross-border consultation or cooperation mechanism should allow users to challenge removal decisions in order to protect the rights to an effective remedy and freedom of expression. Further or in the alternative, the European institutions should explore the possibility for a public interest advocate or defender of fundamental rights to be informed of removal decisions so as to raise their compatibility with fundamental rights and take the matter to court, where appropriate.

<sup>&</sup>lt;sup>10</sup> See Facebook, <u>Charting a Way Forward: Online Content Regulation</u>, February 2020.

<sup>&</sup>lt;sup>11</sup> For an outline of this procedure, see the 2018 annual report of the CNIL qualified person, available from here.

# Proactive and/or specific measures

- 19. Under Article 6 of the Draft Regulation, the Commission and Council propose imposing proactive measures on hosting appropriate, 'where appropriate.' Such measures should be "effective and proportionate, taking in to account the risk and level of exposure to terrorist content, the fundamental rights of the users, and the fundamental importance of the freedom of expression and information in an open and democratic society." The competent authority would be able to request regular reports from the hosting service provider setting out the specific proactive measures they have taken to prevent the re-upload of content previously identified as terrorist as well as detecting, identifying and removing terrorist content. The competent authority would then assess whether the measures are effective and proportionate and if not, would request the hosting provider to implement additional measures. The competent authority and the hosting provider would cooperate to determine what those measures should be, including key objectives and benchmarks as well as timelines for their implementation. In the absence of an agreement, the authority would have the power to order additional specific measures, taking into account the impact of such measures on fundamental rights and the economic capacity of the hosting provider. The hosting provider would be able to request a review or revocation of the decisions made by the authority and the authority would have to provide a reasoned decision within a reasonable period of time.
- 20. By contrast, the European Parliament proposes that hosting service providers may take specific measures that should be effective, targeted and proportionate, taking into account the risk and level of exposure of terrorist content, the fundamental rights of users and the particular importance of freedom of expression. Such measures could not entail the use of automated tools nor a general monitoring obligation. The competent authority overseeing the implementation of specific measures could issue a request for necessary, proportionate and effective additional specific measures to be adopted when a hosting service provider has received a substantial number of removal requests. The request would have to take into account a number of factors, including technical feasibility, size and economic capacity of the provider and fundamental freedoms, particularly freedom of expression. The hosting provider would be able to request a review or revocation of such a request.
- 21. The latest text under discussion in the leaked draft (comment section) suggests that the European institutions have largely followed the European Parliament's approach and agreed to the adoption of *specific* measures. A hosting provider is deemed to have been exposed to terrorist content and therefore required to adopt specific measures if it has received two or more uncontested removal requests. The text further makes clear that any requirement to take measures must not involve general monitoring obligations nor an obligation to use automated tools.
- 22. ARTICLE 19 generally welcomes the European Parliament's proposal. We have long opposed mandatory monitoring obligations. We have also long advocated for appropriate safeguards when hosting providers use automated tools (such as human in the loop and meaningful transparency). At the same time, we are somewhat sceptical that the adoption of specific measures will not lead to general monitoring obligations in practice. Furthermore, the text still makes reference to 'mechanisms' and 'automated tools' to identify and expeditiously remove terrorist content. Reference is also made to the need to adopt appropriate safeguards in order to avoid the removal of non-terrorist content, especially through human oversight and verification. We suggest that specific measures must be commensurate with the technical and operational capabilities of the hosting service provider. While these safeguards are welcome, this

<sup>12</sup> See ARTICLE 19, CJEU judgment in Facebook Ireland case is threat to online free speech, 3 October 2019.

still seems to suggest that specific measures will almost inevitably entail the widespread use of filters in practice.

- 23. Furthermore, we are concerned that in the absence of a clear definition guaranteeing the independence of the competent authority in the Draft Regulation, specific measures may currently be ordered by law enforcement agencies. This is especially problematic given that the 'competent authority' appears to be tasked with ordering content removals, overseeing the implementation of specific measures and in the case of the main competent authority, cross-border requests. Specific measures are deeply intrusive and significantly interfere with the right to freedom of expression. As such, we believe that they should only be ordered by a court. This is especially the case if the jurisprudence of the Court of Justice of the European Union (CJEU) on 'equivalent content'<sup>13</sup> is applied to 'terrorist' content.
- 24. Finally, we note that the Draft Regulation provides that where hosting providers obtain "knowledge or awareness of terrorist content," they must inform the competent authorities of such content and remove it expeditiously. We are concerned that the proposed text fails to make reference to 'actual' knowledge, consistent with the ECD. Nor does it specify that the content to be removed must be 'illegal' terrorist content. In our view, these are important additions, particularly given that there is currently no agreement over what amounts to a 'competent authority' under the Regulation.

# Recommendations:

- There should be no general obligation to monitor or mandatory proactive measures;
- Specific measures should only be ordered by a court;
- Specific measures should only apply to content that is identical to content that has been declared unlawful by a court; if specific measures were to be applied to 'equivalent' content, what amounts to 'equivalent' content should be determined by the court who declared the original content unlawful;
- Insofar as hosting providers use automated tools, they should at a minimum be transparent about them, including by providing meaningful information allowing the public to understand how algorithms are used to moderate 'terrorist' content; they should also ensure that automated tools are only used to identify or detect content rather than to remove content, which should involve human decision-making and verification.

# Safeguards and accountability

- 25. ARTICLE 19 welcomes the Commission and Council proposal to put in place transparency obligations for competent authorities. Equally, we welcome proposals to include a human in the loop and verifications in relation to the implementation of specific or proactive measures (if the latter are adopted contrary to our recommendations). ARTICLE 19 further supports the European Parliament's proposal that Member States should put in place effective procedures in order to enable both content providers and hosting service providers to challenge removal orders. The complaint mechanism under Article 10 that would enable content providers to complain about the implementation of proactive or specific measures is also positive. So is the latest negotiated text concerning information provided to content providers.
- 26. While all these measures are generally positive, we emphasise that they are the *bare minimum* for the protection of freedom of expression, particularly in circumstances where the 'competent

<sup>&</sup>lt;sup>13</sup> See C-18/18 Glawischnig-Piesczek v. Facebook Ireland.

authority' may be a law enforcement agency. Indeed, the Draft Regulation currently puts forward a model whereby content must be removed in exceedingly short time frames by an undefined competent authority or through the use of filters. In other words, the only way freedom of expression is protected is largely after the fact if individuals are willing to put in the time and effort to complain rather than accept a decision to remove. This inevitably introduces friction. Moreover, remedies will be meaningless unless European institutions insist on both companies investing in and Member States providing sufficient financial support for these measures to be implemented.

# Recommendation

• Legal remedies and complaint mechanisms must be appropriately resourced to be effective.

# Compatibility with GDPR and privacy

27. ARTICLE 19 notes that the Draft Regulation does not appear to make reference to the compatibility between proactive or specific measures with the GDPR or the right to privacy under the European Charter of fundamental rights. This is surprising since the CJEU has previously held that the kinds of filters at issue in the *Scarlet Extended SA*<sup>14</sup> and *Netlog*<sup>15</sup> cases raised privacy issues. In our view, this question should be addressed and at the very least compatibility with the GDPR ensured in the Terrorist Content Online Regulation.

### <u>Recommendation</u>

• Ensure the compatibility of the proposed measures under the Terrorist Content Regulation with the GDPR.

<sup>&</sup>lt;sup>14</sup> See <u>Case C-70/10,</u> 24 November 2011

<sup>&</sup>lt;sup>15</sup> See <u>C-360/10</u>, 16 February 2012