



Open letter on behalf of civil society groups regarding the proposal for a Regulation on Terrorist Content Online

Berlin, 09 November, 2020

The undersigned human rights and digital rights organizations call on the participants of the triilogue meeting on the Proposal for a Regulation of the European Parliament and of Council on preventing/addressing the dissemination of terrorist content online to comply with the Charter of Fundamental Rights and discuss further amendments that fully respect freedom of expression, freedom of information and personal data protection of internet users.

I. Definition of terrorist content

1. The definition of terrorist content in the draft regulation is unjustifiably broad. As recent unfortunate attacks and media reporting shows, journalistic, research, or educational content could easily fall under the definition and, therefore, could prevent people from getting access to information.
2. To protect freedom of expression and healthy public debate, it is of utmost importance to exempt content published for journalistic, artistic, educational or scientific purposes, or as criticism of terrorism or political reaction to it.

We suggest to narrow the definition of terrorist content and strictly define material that is unlawful.

II. No mandatory upload filter is acceptable

1. Automated content removal potentially endangers the free flow of lawful information and the freedom to access information. Therefore, any measures taken should be cautious and include proper safeguards. Any solution that is not fully in compliance with the Charter of Fundamental Rights, or the CJEU's case law regarding general monitoring obligations, is unacceptable.
2. In particular, the requirement to filter content in this way would violate the freedom of expression set out in Article 11 of the Charter of Fundamental Rights. Upload filters lack the understanding of linguistic or cultural differences and are unable to assess the context of expressions accurately.
3. Active monitoring of users' content contradicts the 'no general obligation to monitor' rules in the Directive on electronic commerce 2000/31/EC. The requirement to install a system for filtering electronic communications has twice been rejected by the Court of Justice, in the cases Scarlet Extended (C 70/10) and Netlog/Sabam (C 360/10).
4. General monitoring obligations also breach the General Data Protection Regulation. Any algorithm-curated content moderation, such as using upload filters, ultimately requires the processing of personal data. Under Article 22 of the GDPR, users have the right not to be subject to automated decision making without human intervention. This general rule is applicable to upload filters. The right of the users to contest the automated decision-making process entitles them not to give consent to any kind of automated filtering method without human intervention.

We suggest that internet hosting providers should be able to choose measures to implement to avoid access to terrorist content online. Mandatory automated filters are not legal under EU law. Mandatory

upload filters compromise freedom of expression, freedom to access information and personal data protection.

III. Safeguards needed to conduct cross-border removal of online content

1. Any competent authority that is involved in content removal proceedings should be independent, such as courts or independent administrative authorities. The legality of the content is a challenging task that should only be evaluated by independent bodies.
2. Competent authorities vary across the Member States; however, proper evaluation of these designated bodies is important.
3. The ex-ante independent scrutiny of any removal order should be based on judicial cooperation, from all EU Member States involved, in order to ensure legal certainty, to respect the constitutional traditions of Member States, to ensure proper protection of freedom of expression, to respect proportionality requirements, and to ensure access to a redress mechanism on behalf of the owner of the content.

We call on the participants of the triadogue to require that removal orders must only be issued by independent courts or administrative authorities.

IV. One-hour time frame

1. The one-hour time frame is disproportionate and insufficient for the online hosting providers to seek a prior decision from the court, especially because it is combined with severe sanctions for failing to comply with removal orders. Blocking content within an hour is exceptionally burdensome for small companies, such as European startups, which don't have the resources to act expeditiously.

Instead of the strict one-hour time frame, we suggest using the standard of 'acting without undue delay'. This solution would support the initial idea: namely, big companies could act within an hour, while smaller companies should act as soon as they can.

We ask the participants of the triadogue meeting to reevaluate the draft Regulation and modify the text to respect the fundamental rights of users as set out in the Charter of Fundamental Rights.

Sincerely yours,

Dr. Balazs Denes
Executive Director
Civil Liberties Union for Europe

Access Now
Antigone
Article 19
Center for Democracy and Technology
Chaos Computer Club
Copyright 4 Creativity
Digitale Gesellschaft
European Digital Rights
Electronic Frontier Foundation
Homo Digitalis
Mnemonic
Peace Institute
Rights International Spain
Save the Internet
StateWatch