

Regulation Addressing the Dissemination of Terrorist Content Passed

News

Thomas Wahl

After approval by the European Parliament and the Council (→ [eucrim 1/2021, 25](#)), Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online was published in the [Official Journal L 172 of 17 May 2021](#). Eucrim has informed of the negotiations of this controversial piece of legislation (last → [eucrim 1/2021, 25-26](#); [eucrim 4/2020, 284-285](#) with further references). The Commission tabled the proposal on 12 September 2018 (→ [eucrim 3/2018, 97-98](#)). The dossier sparked fierce criticism by civil stakeholders (see also the analysis of the Commission proposal by [G. Robinsion, eucrim 4/2018, 234-240](#)). The Regulation aims to curb the dissemination of contents by terrorists who intend to spread their messages, radicalise and recruit followers, and facilitate and direct terrorist activities.

The Regulation lays down uniform rules to address the misuse of hosting services for the dissemination to the public of terrorist content online. Particularly, it regulates the duties of care to be applied by hosting service providers (HSPs) as well as the measures to be in place on the part of Member States' authorities in order to identify and ensure the quick removal of terrorist content online and to facilitate cooperation with each other and Europol. The key elements of the new legislation are as follows:

Material scope ("terrorist content")

- The Regulation takes up the definitions of terrorist offences set out in Directive 2017/541 on combating terrorism and makes use of them for preventive purposes. The definition of terrorist content online applies to material that:
 - Solicits someone to commit or to contribute to terrorist offences or to participate in activities of a terrorist group;
 - Incites or advocates terrorist offences, such as by glorification of terrorist acts;
 - Provides instruction on how to conduct attacks.
- Such material includes text, images, sound recordings, videos, and live transmissions of terrorist offences, which cause a danger of further such offences being committed.
- *Exception:* Material disseminated for educational, journalistic, artistic or research purposes or for awareness-raising purposes will not be considered "terrorist content".

AUTHOR

Thomas Wahl

Senior Researcher
Max Planck Institute for the
Study of Crime, Security and
Law

Published in
2021, Vol. 16(2) *eucrim* pp 95 –
97

ISSN: 1862-6947
<https://eucrim.eu>



Personal scope

- The Regulation applies to all hosting service providers offering services in the EU. HSPs in this sense are providers of information services which store and disseminate to the public information and material provided by user of the service on request, irrespective of whether the storing and dissemination to the public of such material is of a mere technical, automatic and passive nature. Such platforms can be social media, video image and audio-sharing services;
- Interpersonal communication services, such as emails or private messaging services as well as services providing cloud infrastructures do, in principle, not fall under the Regulation.

Temporal scope

- The obligations set out in the Regulation will apply as of 7 June 2022.

One-hour rule

- The Regulation considers that terrorist content is most harmful in the first hours after its appearance. Hence, HSPs will be obliged to stop the dissemination of such content as early as possible and in any event within one hour.

EU-wide removal orders

- The competent authority of each EU Member State has the power to issue a removal order directly requiring HSPs to remove or disable access to terrorist content in all Member States;
- HSPs must designate or establish a contact point for the receipt of removal orders by electronic means and ensure their expeditious processing.
- *Form and contents*: The Regulation established templates in which the authorities must fill in all the necessary information for HSPs;
- Removal orders must contain justifications as to why the material is considered to be terrorist content, including detailed information on how to challenge the removal order.

Cross-border removal orders

- Where the HSP's main establishment is or its legal representative resides in a Member State other than that of the issuing authority, a copy of the removal order must be submitted simultaneously to the competent authority of that Member State;
- The competent authority of the Member State where the HSP has its main establishment or where its legal representative resides can scrutinise the removal order issued by competent authorities of another Member State to determine whether it seriously or manifestly infringes the Regulation or the fundamental rights enshrined in the CFR;
- Both the content provider (user) and the HSP have the right to request such scrutiny by the competent authority in the Member State where the HSP has its main establishment or where its legal representative resides;
- The scrutiny must be carried out swiftly and a decision of whether an infringement is found must be taken within 72 hours of receiving the copy of the removal order/the request, so that it is ensured that erroneously removed or disabled content is reinstated as soon as possible;
- Where the decision finds an infringement, the removal order will cease to have legal effects.

Proactive measures

- The Regulation sets out several specific measures that HSPs exposed to terrorist content online must implement to address the misuse of its services;
- It is for the HSPs to determine which specific measures should be put in place. Such measures may include:
 - Appropriate technical or operational measures or capacities, such as staffing or technical means to identify and expeditiously remove or disable access to terrorist content;
 - Mechanisms for users to report or flag alleged terrorist content;
 - Any other measures the HSP considers appropriate and effective to address the availability of terrorist content on its services or to increase awareness of terrorist content;
- HSPs are obliged to apply specific measures with effective safeguards to protect fundamental rights, in particular freedom of speech;
- There is no obligation for HSPs to use automated tools to identify or remove content. If they choose to use such tools, they need to ensure human oversight and publicly report on their functioning.

Safeguards

- The Regulation installs several safeguards that are to solve conflicts with fundamental rights, in particular the freedom of speech.
- *Transparency*: Both Member States and HSPs will be obliged to issue annual transparency reports on the measures taken and on any erroneous removals of legitimate speech online;
- *Notification duty*: If content is removed, the user will be informed and provided with information to contest the removal;
- *Complaints*: HSPs must establish user-friendly complaint mechanisms and ensure that complaints are dealt with expeditiously towards the content provider. The mechanisms must ensure that erroneously removed content can be reinstated as soon as possible;
- *Legal remedies*: Content providers and HSPs must not only have the rights to let review the removal orders by the relevant authorities but can also seek judicial redress in courts in the respective Member States.

Sanctions

- Member States must adopt rules on penalties for non-compliance of the Regulation on the part of HSPs;
- Penalties can be of an administrative or criminal nature and can take different forms (e.g. formal warnings or fines);
- Member States must ensure that penalties imposed for the infringement of this Regulation do not encourage the removal of material which is not terrorist content;
- In order to ensure legal certainty, the Regulation sets out which circumstances are relevant for assessing the type and level of penalties. When determining whether to impose financial penalties, due account should be taken, for instance, of the financial resources as well as the nature and size of the HSP;
- Member States must provide that a systematic or persistent failure to comply with the “one-hour rule” following a removal order is subject to financial penalties of up to 4 % of the HSP’s global turnover of the preceding business year.

The Regulation also lays down the modalities how the new rules are monitored by the Member States and evaluated by the Commission. The Commission is requested to submit an implementation report by 7 June

2023. By 7 June 2024, the Commission shall carry out an evaluation of the Regulation and submit a report to the European Parliament and to the Council on its application.

Statements:

Commission Vice-President *Margaritis Schinas* **told journalists**: “With these landmark new rules, we are cracking down on the proliferation of terrorist content online and making the EU's Security Union a reality. From now on, online platforms will have one hour to get terrorist content off the web, ensuring attacks like the one in Christchurch cannot be used to pollute screens and minds. This is a huge milestone in Europe's counter-terrorism and anti-radicalization response.”

MEP *Patryk Jaki* (ECL, PL) who was the main rapporteur on the Regulation for the EP **said**: “I strongly believe that what we achieved is a good outcome, which balances security and freedom of speech and expression on the internet, protects legal content and access to information for every citizen in the EU, while fighting terrorism through cooperation and trust between states.”

Other MEPs commented more critically. EP Vice-President *Marcel Kolaja*, who was rapporteur in the IMCO committee, **criticised**: “This regulation can indeed strengthen the position of authoritarians. European Pirates as well as dozens of NGOs were pointing out the issue for a long time, but most political groups ignored our warnings. We are likely to see Europe undermine its fundamental values.”

Several **non-governmental organisations continue to see** the new Regulation as a significant threat to freedom of expression, which has not been remedied by the compromise text between the EP and the Council. In particular, the broad understanding of “terrorist content” poses the risk that orders for political purposes will be abusively issued under the guise of combating terrorism. In addition, **critics predict** that giving HSPs such a short deadline for removing contents would encourage them to use algorithms for their moderation, which is problematic.

It remains to be seen whether the new EU Regulation addressing the dissemination of terrorist content online can withstand a possible judicial review.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and “criministrative” law.

All news items are freely accessible at: <https://eucrim.eu/news/>

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.

The project is co-financed by the **Union Anti-Fraud Programme (UAFP)**, managed by the **European Anti-Fraud Office (OLAF)**.



**Co-funded by
the European Union**