DIGITALEUROPE

29 OCTOBER 2019

DIGITALEUROPE's views on the Terrorist Content Online Regulation

Executive Summary

DIGITALEUROPE's membership fully supports the efforts of the EU institutions to fight terrorism and incitement to violence with the proposed Terrorist Content Online Regulation. We believe this is an important policy area that, if done right, will help reduce the dissemination of terrorist content online.

DIGITALEUROPE's member companies have undertaken extensive work to fight terrorism and incitement to violence, including expanding their cooperation with law enforcement authorities and increasing available measures to tackle extremist content on a voluntary basis.

In light of the trialogue negotiations on the proposed Regulation, DIGITALEUROPE encourages the institutions to find a balance that is both pragmatic as well as effective. The Regulation should ensure appropriate safeguards regarding rule of law, fundamental rights, and the feasibility of implementation for hosting service providers.

We recommend:

- A targeted scope, both regarding the definition of terrorist content itself as well as focusing on hosting service providers that disseminate content to the general public. Enterprise and cloud infrastructure providers should not be included.
- The deadline for content removal must be pragmatic and flexible enough to ensure that hosting service providers can comply with (cross-border) orders from the competent authorities.
- The Regulation should not prescribe mandatory proactive measures and referrals, but instead facilitate existing best practices and cooperation between service providers and law enforcement.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

A clear scope that is fit for purpose

The scope of the Regulation as formulated in the Commission's original proposal potentially sweeps in many services on which terrorist content is rarely a problem. The proposed broad definition risks capturing a significantly larger than intended group of information society services.

It is important to differentiate between services whose primary purpose is to make content widely available to the public by default and those that are used primarily for personal storage of private content and are not designed to facilitate broad dissemination of content. The scope should focus on providers that enable its users to make content available to the general public. This gives better legal certainty and prevents services from being needlessly affected, while also avoiding over-removal of lawful user content.

In contrast, enterprise and cloud services which allow users to share content with selected users (but not with the general public) should not fall under the Regulation. Such services are used primarily for sharing content or collaboration between colleagues or small groups of friends and family.

Cloud infrastructure service providers in particular act as an initial layer of foundational infrastructure and enable customers to build and run their own cloud-based IT systems which the latter then design, control and manage. The cloud infrastructure service providers cannot access or control specific pieces of content, only the customer has this technical ability. If a cloud infrastructure service provider were ordered to remove a specific terrorist content, it would have to remove all the customer's data on that service, meaning that lawful content from other users would also be removed. For instance, if a comment made in a blog were considered terrorist content, cloud infrastructure service providers would often only be able to take down the entire website or blog.

A focused scope also brings the Regulation more in tune with estimates from Europol that only around 150 companies[1] were identified as hosting terrorist content, a large part of them being established outside of Europe and offering their services across the Single Market. Further, orienting the Regulation towards dissemination to the general public also aligns with the same terminology used in the Directive on Combating Terrorism.[2]

For these above reasons, we urge the co-legislators to clarify that the Regulation does not apply to enterprise or cloud services that purely provide the backend infrastructure and do not share content to the general public.

---

1 Impact assessment: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf

2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017L0541

A workable deadline for hosting service providers

The one-hour deadline for content removal does not take into account several practical difficulties such as the need to translate the request, the need to identify whether the request came from a valid competent authority, the technical operations to remove the content, the international dimension of the internal organization of several hosting companies, and even time zone differences.

The tight deadline, in combination with the broad definition of terrorist content, the very broad interpretation of competent authorities and the absence of any redress option for users (aside from going to the national competent authority issuing the request) creates a worrying situation that could be open to abuse and provides insufficient protection for fundamental rights.

Therefore, DIGITALEUROPE instead recommends that the timeline for hosting service providers to comply should be 'without undue delay' from receipt of the order, allowing hosting service providers sufficient time to address each request.

The Regulation itself (article 4.6) already refers to the notion of 'without undue delay' in other instances, which is a common practice in EU legislation[3] and is present in several Member states' national law.[4] Companies of all sizes need the time and opportunity to take appropriate and balanced action against their end-user and minimize collateral impact.

A clearer definition of terrorist content

The recitals to the Regulation rightly identify that terrorist content can be legally disseminated for many valid reasons including educational, journalistic or research purposes and that radical, polemic or controversial views should not be considered terrorist content. For material hosted on cloud service providers, where broader context is unavailable, it is frequently impossible for providers or authorities to make such distinctions.

Some types of content can be easily identified as illegal, while other content such as speeches require nuanced judgment. Moreover, there needs to be more certainty around the definition of terrorist organizations. Greater clarity is possible by limiting the definition of terrorist organization to those on the EU or UN designated terrorist organizations lists.

---

[3] General Data Protection Regulation (art 33.2)

[4] For example, under French criminal code, the Prosecutor or police officers may request the communication of any piece of evidence related to an investigation that is stored in the companies or public administrations' the IT systems. The said companies or administrations must provide the requested evidence without undue delay (art. 60-1 CPP).

The definition of 'terrorist content' should be clarified and linked to a designated list of terrorist organisations in order for companies to be able to create a more manageable process. We also recommend that the Recital 9 setting out various legitimate forms of expression be included in the main text of the definition.

Proactive monitoring obligations jeopardizing fundamental rights

DIGITALEUROPE's member companies have invested in developing technology to combat and counter terrorist propaganda. We would call for this voluntary regime to be maintained alongside the Regulation since it has been working well. Legal protection is needed for platforms and providers who take proactive measures to take down harmful content, and it should be clarified that by doing so they would not lose liability protections in line with the 'Good Samaritan' principle proposed in Recital 5.

Further, the Regulation should not include mandatory proactive filtering measures. This would be a far departure from the principles of limited liability as established in the e-Commerce Directive and could have far-reaching consequences for start-up businesses in Europe, for users and for fundamental freedoms such as privacy and freedom of speech. Such an obligation would also be against established case law against a general monitoring obligation.

In addition to these legal and fundamental rights concerns, even practically a general monitoring obligation and proactive removal of content could be technically impossible at times depending on the service provided. Many hosting service providers do not have access to their customers' data and may therefore not be able to scan or filter all the content that is being processed since they do not control or have access to the data, which in often is encrypted. This applies to enterprise services as well as cloud infrastructure service providers.

A single judicial authority per Member State

The Regulation states that a removal order can be issued as an administrative, judicial or law enforcement decision by a national competent authority. The process to identify such competent authorities is not detailed in the proposal. Since the measures pronounced by the 'competent authority' have to strike the right balance between several potentially conflicting rights, the intervention of a judge is necessary and represents an additional safeguard. This would also ensure that proper expertise is there and would help avoid erroneous removal of legal content.

Therefore, it is crucial that each Member State should have a single judicial authority to notify the hosting service provider for content removal. A single point

of contact system has proven to work very well in Member States that have put it in place for law enforcement data access requests. It makes the system far more efficient, as it decreases the turnaround times to process requests, facilitates cooperation with service providers and provides more legal certainty.

Removing referrals to ensure a regulatory framework that works in practice

The envisaged referral system raises a number of concerns. Whilst service providers will enforce their own terms and conditions, the Regulation essentially privatises the assessment of terrorist content. Since the Regulation already sets out a procedure for issuing removal orders, this mechanism should be the one used by the competent authority for all terrorist content. This would ensure that the decision is made by those with expertise rather than individual companies. This would create a more efficient and streamlined process and reduce error.

FOR MORE INFORMATION, PLEASE CONTACT:

Jochen Mistiaen

Senior Policy Manager

jochen.mistiaen@digitaleurope.org / +32 496 20 54 11

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK