EDiMA

EDiMA position on the draft Regulation on preventing the dissemination of terrorist content online

EDiMA[1] supports the Commission's goal to fight against the dissemination of terrorist content and propaganda, being that online or offline. EDiMA members already include provisions in their terms of services against the use of their services for terrorist related activities, and we furthermore welcome the intention to clarify the processes and improve the cooperation between private companies, law enforcement and other competent authorities.

Our membership has fully engaged with the EU institutions and law enforcement bodies to address this serious concern and enacted voluntary[2] measures at the company level to do so. The EU and Global Internet Forums[3] are concrete examples of the useful cooperative framework our companies have created to tackle terrorist content online.

Despite the effectiveness of existing industry-led efforts[4], our understanding is that the proposed Regulation has been drafted with an intention of expediting results. However, the text as it stands fails to provide the necessary clarity and legal certainty needed to achieve the stated goal.

The proposal needs clarification and definition

Definitions are missing or not specific enough to ensure a consistent implementation across the EU. The definition of what constitutes a terrorist organisation is broad and vague. Article 2.3 of Directive (EU) 2017/541 defines a terrorist group as a "structure group of more than two persons, established for a period of time and acting in concert to commit terrorist offences". While such a flexible definition may be useful for expert law enforcement, it is amorphous and difficult for private companies to interpret. It is thereby inappropriate to ask companies to use proactive measures to detect such content.

Furthermore, the definition of terrorist offence is too broad in the context of this Regulation and it is not necessarily linked to a terrorist organisation. EDiMA would welcome specific wording adapted to this proposal, including language that appropriately refers to the terrorist organisations designated on the EU terrorism list. Similarly, the definition of what constitutes a competent authority or how many can coexist is lacking in the proposal.

Due to certain content being more at risk of abuse by terrorists, the Regulation should also be made more specific as to in what circumstances hosting service providers should take proactive action, by

[1] EDiMA is the European trade association representing online platforms and other innovative businesses. It is an alliance of new media and Internet companies whose members include Airbnb, Allegro, Amazon EU, Apple, eBay, Expedia, Facebook, Google, King, Microsoft, Mozilla, Oath, OLX, TripAdvisor, Twitter, Veon Digital and Yelp.

[2] In December 2016, the founding member companies of the GIFCT (Facebook, Microsoft, Twitter, and YouTube), committed to creating a shared industry database of "hashes" — unique digital "fingerprints" — for violent terrorist imagery or terrorist recruitment videos that were removed from their services. By sharing these hashes with one another, they can identify potential terrorist images and videos on their respective hosted consumer platforms. This collaboration is resulting in increased efficiency as they continue to enforce their policies to help curb the pressing global issue of terrorist content online.

[3] https://gifct.org/

[4] The European Commission's Impact Assessment recognises that online platforms' efforts are producing results. See page 11.

removing the ambiguous terms such as 'appropriate' and 'reasonable' actions (articles 3 and 6) and adding in clearer instructions.

The scope of the proposal is too broad and needs to better support the online ecosystem

EDiMA has strong concerns on the impact of this text on the online ecosystem. The goal of this Regulation is to cover all hosting service providers and content providers online, regardless of the nature of their service or their ability to comply with its requirements. Estimates from the European Commission Impact Assessment[5] point to a basis of over 10500 hosting service providers (HSPs) established in Europe, and almost 20000 HSPs[6] established both in Europe and in the US and Canada, all of which would be covered by the regulation. This would make small providers the most vulnerable if terrorist groups decide to host and share terrorist content on their platform. But the response of the European Commission, a focus on imposing penalties on platforms via article 18, is inappropriate. The text should not only seek to ask those players that are too small to set-up expensive reviewing teams but should adequately support them, financially and in terms of technical and legal assistance. Furthermore, implementing this Regulation within six months as foreseen by the Commission will be impossible for most of the HSPs.

The definition of hosting service providers also raises concerns as it is extremely broad, not consistent with the terminology adopted in the e-Commerce Directive and goes beyond the purposes offered in the explanatory memorandum[7]. It is possible, for example, that companies would need to breach confidentiality or encryption agreements with their corporate customers to comply if the scope is not limited to consumer-facing services.

This definition is inconsistent with the e-Commerce Directive, targeting the content provider rather than recipient of the service. In addition, it focuses on communication to third parties rather than communication to the public, de facto also covering business-to-business communications. It puts cloud service providers into an untenable position to monitor their clients' communications.
Concretely, cloud infrastructure providers offer as a service the IT infrastructure, enabling customers to build on top of cloud infrastructure services. Such customers are the ones controlling the data and having the ability remove content. In most instances cloud infrastructure providers are technically unable to block individual illegal content and they would be forced to take down – or simply 'turn off' - entire public services that rely on their infrastructure.

Here, we recommend a definition of 'hosting service provider' that 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 disseminating the information stored to the public.'*

---

[5] See page 6 of the Impact Assessment.

[6] The EU IRU has identified over 70 platforms used by terrorist groups to spread their propaganda materials and has been referring Internet content across over 31 online platforms. This is a voluntary arrangement and it is ultimately for the companies to decide whether to remove the material. Nevertheless, in 91.4% of the EU IRU referrals, the material has been swiftly removed. Additionally, the EU IRU is in constant dialogue and engagement with new platforms that are being used by terrorist propagandists, in order to help them increase their resilience against terrorist related propaganda.
(Data taken from the Europol report on the EU Internet referral unit:
https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights)

[7] That memorandum makes clear that the target of regulation is for "[t]errorist content shared online for such purposes is disseminated through hosting service providers that allow the upload of third-party content."

The risk of an increased fragmentation of the DSM

The Regulation, as it stands, risks to increase the fragmentation of the Digital Single Market. There is no definition of what could constitute a competent authority in the text, nor a maximum number set by Article 17. It will be up to the Member States to decide individually. These authorities will also be responsible for laying down the rules on penalties according to Article 18, with no indications as to the framework of those sanctions and no mechanism to ensure a harmonised approach across the EU. This Regulation needs to clearly state that competent authorities should act in full conformity with the Charter of Fundamental rights while providing meaningful safeguards to prevent any abuse.

The flexibility granted to Member States will further complicate the work of the hosting and content providers, who will have to deal with more than 27 different national authorities in the absence of a single European framework.

EDiMA calls for a more unified approach in this proposal. This Regulation needs to provide a strong and efficient European framework to tackle the spread of terrorist content online.

A one-hour turnaround time that lacks proper technical assessment

EDiMA questions the one-hour turnaround time for platforms to remove content following a removal order, as set in Article 4.2. A fixed turnaround time is disproportionately burdensome and would be ineffective. While our members have shown their commitment in removing terrorist content as expeditiously as possible, this limit will be unworkable for most of the intermediaries targeted. The requirement will force platforms, large and small, to set-up dedicated teams operating 24/7 to deal with the removal orders coming from a proliferation of competent authorities all over the EU. Smaller platforms will be particularly disadvantaged, as they do not have the resources to comply with the Regulation, especially given the absence of support in this text. The risk of the potential penalties will force them to cease their operations in the EU.

The one-hour turnaround time for taking down terrorist content prescribed by article 4 is impractical for most online intermediaries. The threat of penalties applied as prescribed in article 18 could force many platforms to cease their operations in the EU. The combination of short turnaround time and high penalties also provides a perverse incentive for companies to over-remove content without conducting the necessary and appropriate human oversight. This Regulation needs to be applicable across the online ecosystem to ensure an efficient fight against the spread of terrorist content, while preserving fundamental rights.

A concerning focus on proactive measures

Giving Member States an option to introduce their own unlimited proactive measures raises several concerns for EDiMA. First, such a monitoring is often impossible as many hosting services provide for encrypted storage of data, which prevents the service itself from accessing its customers' data. This Regulation would potentially render those services illegal in the EU.

Second, monitoring tools are costly – introducing another disadvantage to smaller market players and are not always reliable[8]. Automated filters cannot distinguish between an image used for propaganda, information or parody purposes. Such systems need to be trained, meaning that they cannot recognise

[8] The Impact Assessment mentions page 13: « *Costs can vary, from the use of simple (and not particularly reliable) hashing software, to 100 million EUR reported by one major video sharing platform."*

new pictures, videos or speeches, and in terms of terrorist content risk impacting the work of journalists and organisations monitoring human rights abuses for example. The safeguards proposed in Article 9 will not be sufficient as human oversight in itself cannot be applied systematically[9].
Finally, different hosting providers host very different types of content. The imposition of proactive measures across the board, to all HSPs will be burdensome and inefficient. It should be very explicit what HSPs, what kind of content, and under which circumstances proactive measures are required.

The potential penalties, combined with the lack of appeal mechanism for online platforms would mean that hosting and content providers would have to remove content injudiciously to avoid any legal risk, which will certainly be detrimental to fundamental rights. Moreover, as the definition of terrorist content is very broad, hosting services providers will need to assess themselves what content can be considered terrorist content[10]. They will design their proactive measures consequently, without any proper safeguards[11]. This could have very serious implications on the free circulation of information and freedom of expression as many small providers will not have access to proper legal advice.
Different proactive measures could also have to be implemented depending on the Member State and its own definition of what is terrorist and what is not, and what each individual Member State considers to be "effective and proportionate" measures.

EDiMA strongly cautions the institutions against such risks and recommends proactive measures to be encouraged, wherever possible, but not imposed across the board.

The worrying introduction of a general monitoring obligation
The general monitoring obligation in the Regulation contradicts fundamental rights afforded under EU law. Recital 19 undermines the cornerstone principles of the 2000 e-commerce Directive that are so crucial for the preservation of fundamental rights[12]. In practice, Member States will have the possibility to impose a general monitoring obligation to certain providers if they consider it proportionate to fulfil the goals of this Regulation. The lack of a precise definition of "terrorist content" makes this provision even more problematic. EDiMA considers this provision as disproportionate and in direct contradiction with several articles of the EU Charter of Fundamental Rights.

The need for more clarity on data-sharing and retention requirements
EDiMA finds the Regulation's provisions on data-sharing and retention requirements ambiguous and contradictory to other laws and pieces of EU legislation.
The requirement of notification to competent authorities upon becoming aware of "any evidence of terrorist offences" as described in Article 13.4 inappropriately shifts the function of law enforcement investigation from government to private actors. Law enforcement powers belong to the government, and not to industry.

[9] Furthermore, the text of the Regulation does not take into consideration the severe psychological consequences of being exposed to disturbing content for the reviewers. Human review is necessary but should be applied in targeting cases. As such it cannot constitute a safeguard in itself.
[10] It is particularly the case for referrals (Article 5) and in Article 6.1.
[11] The Regulation is very broad here as Article 6.1 states that HSPs shall take proactive measures "where appropriate". This nuance will be interpreted differently depending on Member States and competent authorities.
[12] "*A decision to impose such proactive measures should not in principle lead to the imposition of a general monitoring obligation.*"

It is also too broad and not proportionate. The line between a terrorist offence, hate speech or incitement to hatred is thin. Our members are committed in fighting against all those behaviours but the question of what should be shared with competent authorities remains. To make sure they comply fully with the Regulation, providers will potentially over-report such content, at the risk of transmitting sensitive, personal information to law enforcement authorities.

EDiMA recommends a more specific definition that limits disclosures to law enforcement authorities where there is an imminent threat to life. This is needed to avoid conflicts of law and uphold users' fundamental rights. Similarly, the provision on data retention requirements details in Article 7 needs to be strengthened by aligning and harmonising such requirements with the e-evidence proposal.

A single judicial authority

To the extent that content is required to be removed by law, each Member State should have a single judicial authority that notifies the HSP through a completed legal removal request that the content must be removed.

We believe a judicial authority is better placed to assess these kinds of requests, rather than an administrative or law enforcement bodies due to the importance of fundamental rights that are stake.

Penalties

The sanctions provisions in Article 18 are ill-defined and will lead to varying penalties across Member States. This could lead to disproportionate outcomes. We recommend a sole competent authority acting on behalf of the EU27 be named to impose commensurate penalties, removing penalties associated with Article 13(4), and to specify the sanctions in Article 18(1), like those in Article 18(4), are financial in nature. Additionally, the definition of systematic failures in Article 18(4) is ambiguous, and likely to lead to unharmonized assessments across Member States.

Fines with up to 4% of global turnover for systematic failures to comply with a fixed one-hour turn-around time are disproportionate and unreasonably high. This proposal does not include the gradation of sanctions ranges provided by Article 83 of the GDPR, where the 4% threshold is limited to the most serious, intentional infringement of the GDPR principles. Global turnover, rather than EU-specific revenue, is also disproportionate. The scope of revenues should be limited to the jurisdiction of the regulation.

We recommend removing the disproportionate up to 4% penalty rate for systematic violations and reserving the regulation's highest fines only for the most egregious violations where a provider acts intentionally or with gross negligence.

Conclusion

While EDiMA firmly shares the European Commission's objectives of improving and streamlining the fight against the spread of terrorist content, this proposal as it stands will not provide the robust framework that is needed in a proposal of its kind. In order to be impactful and efficient, this Regulation should seek to help hosting and content service providers instead of only focusing on penalties.

Definitions needs to be tightened up, and it needs to be explicit when it is required for HSPs to implement proactive measures. The number of national competent authorities needs to be limited and the legal certainty of the proposal improved to provide for a strong, robust and consistent regulatory framework across the EU. Safeguards to protect fundamental rights should be strengthened to make sure citizens fully benefit in the fight against terrorist content online.