tech against terrorism

Tech Against Terrorism response to the EU's terrorist content online regulation

Support mechanisms, legal certainty, and safeguards needed to avoid negative impact

June 2021

INTRODUCTION

On 28 April the EU Parliament announced that the regulation on preventing the dissemination of terrorist content online had been approved. On 7 June, the law, which was initially introduced by the Commission and has gone through several iterations, entered into force and will start applying on 7 June 2022.

The law compels tech companies to remove terrorist content within one hour following removal orders from so-called competent authorities. These bodies, which each Member State will appoint, are also entitled to instruct companies to introduce "specific measures" to tackle terrorist content and to issue financial penalties if companies cannot comply with the regulation. Companies that are not based in the EU will need to appoint a legal representative based in the region. Companies, and competent authorities, will have to issue transparency reports on their efforts to comply with the regulation. Failure to comply with the obligations could make companies liable for financial penalties, and failure to comply with the one-hour removal deadline might lead to a penalty of four percent of a company's global turnover.

Unfortunately, as Tech Against Terrorism has cautioned during the proposal stage, the regulation does not recognise the threat of terrorist exploitation of smaller platforms, and offers little clarity on how smaller platforms will be supported in tackling this threat and in complying with the regulation. Without support, we fear that the regulation will do little to achieve its intended purpose and risks harming innovation and competition in the process. Furthermore, the EU should consider the incentives the law creates and what this means for the objectives the EU has set out in its overall tech strategy and the Digital Services Act.

Several matters that are key to understand how the law will function in practice remain vague. With about a year until the regulation starts applying, we call on the EU to provide clarity on three key issues:

1. What support will the EU provide for smaller tech companies that are likely to struggle to comply with the regulation and for initiatives that support smaller companies in building capacity against terrorist exploitation of their platforms?
2. How will the EU provide legal certainty for platforms working to comply with the regulation?
3. What safeguards will be introduced to ensure that competent authorities do not abuse their status or are instrumentalised for political objectives?

RECOMMENDATIONS

Recommendations regarding legal certainty and support for smaller tech platforms

We recommend that the EU:

1. Clarifies what support will be given to smaller platforms to help them comply with the regulation
2. Ensures that smaller platforms will only need to notify competent authorities once if they are likely to struggle to act on removal orders within one hour, instead of having to report this every time they receive an order. This could be assessed on a regular basis in line with existing frameworks, such as the Commission Recommendation 2003/361/EC on micro and smaller enterprises
3. Provides legal certainty to tech platforms by clarifying exactly how their activity will be measured, for example by clarifying what "systematic and consistent failure" to comply with removal orders (Article 3) means and what platforms need to do to be seen to comply with the specific measures outlined in Article 5
4. Confirms whether platform size and financial capacity will be considered when issuing penalties for platforms
5. Clarifies under what exact circumstances a company's legal representative may be held liable for infringements of the regulation

Recommendations regarding competent authorities

We recommend that the EU clarifies what safeguards it will implement to ensure that competent authorities:

1. Have sufficient understanding of risks to human rights and freedom of expression associated with the measures they implement, for example removal orders and specific measures
2. Are uniform in their judgement and do not politicise removal orders or impose national speech standards on the rest of the EU
3. Have a clear and uniform understanding of the accuracy threshold of removal orders as specified by the regulation
4. Do not exploit their right to prevent user notice in case of content removal
5. Are consistent and accurate in issuing penalties to companies
6. Are disincentivised from instructing over-zealous content removal
7. Are held accountable for assessments and judgements made in implementing this regulation

Furthermore, we encourage the EU to:

8. Clarifies what framework competent authorities will use to assess company compliance with the "specific measures" obligations in Article 5
9. Clarifies how it will monitor and ensure that removal orders receive sufficient scrutiny
10. Expands the transparency requirements for competent authorities in line with the Tech Against Terrorism Guidelines (forthcoming) to cover processes and systems used to identify terrorist content online, breakdown of issued removal orders by platform, and appeals made under Article 9 and the outcome of each case

OUR CONCERNS

The human rights and freedom of expression concerns associated with the regulation are well documented and have been eloquently articulated by several civil society organisations and UN Special Rapporteurs, the Council of Europe, and the EU's Fundamental Rights Agency. The concerns centre around the potential negative implications of a short removal deadline and the risk of competent authorities becoming politicised and de facto contributing to extra-territorial enforcement of national speech standards. At Tech Against Terrorism, we have noted several concerns about the impact on smaller platforms and are doubtful whether the law will be effective in achieving its intended purpose. Whilst it is disappointing that these criticisms have not been taken into account, in this piece we look forward and focus on how the EU can provide clarity on several key challenges.

Lack of legal certainty and consideration for smaller tech company capacity

The regulation does in our view not account for the fact that smaller tech companies constitute one of most important strategic threats with regards to terrorist use of the internet. Therefore, any online counterterrorism effort needs to focus on supporting small platforms in improving their response. There is sufficient evidence for this, but the EU seems to have introduced legislation that is primarily aiming to make a political point against larger tech companies. This will probably lead to impressive takedown statistics from the companies that are able to comply with the regulation – the Facebooks of the world – but it does not acknowledge the wider reality of terrorist content dissemination and the role smaller tech platforms play within it. We fear that this is a potential misjudgement, and that as a result the regulation will likely not improve the overall threat picture. Instead, it risks overburdening smaller platforms and make them less effective at addressing terrorist content online. Therefore, we call on the EU to clarify how it will support platforms in complying with the regulation.

Further, the law does little to provide legal certainty for platforms. Firstly, there is lack of legal certainty as to what exactly is expected of platforms across several key provisions. One is around smaller tech platforms' obligations. The EU has partially incorporated our feedback around smaller platform capacity, where we cautioned that a platform run by just one person (the type of platform that terrorists prefer to exploit) will not be able to comply with the one-hour removal deadline (Article 3). The regulation will now excuse platforms if they can showcase "objectively justifiable technical or operational reasons […] without undue delay" that caused them to miss the one-hour deadline. Whilst this is reasonable, less so is that platforms will seemingly need to notify competent authorities every time they cannot comply (which does little to ease operational burden on smaller platforms) and that it is at the discretion of the competent authority whether such justifications are acceptable (no information on how this will be assessed is provided).

Based on an assessment made on data collected by the Terrorist Content Analytics Platform (TCAP), some smaller platforms will likely need to spend up to an hour per day and five hours per week asking for a deferral on the removal orders. In reality, it is likely that that this will translate into almost twice as much time per day and week given that the content in scope for this regulation is far more expansive than the TCAP, which in its more narrow scope collects official content from designated terrorist groups. Despite this considerable time commitment, platforms will have no legal certainty whether they are excused from penalisation. The EU should therefore reconsider compelling smaller companies to report on inability to remove content for every removal order to avoid overburdening them.

Secondly, some companies will on the order of competent authorities have to introduce "specific measures" (for example technical solutions and user flagging mechanisms) to tackle terrorist content (Article 5). Platforms need to ensure that these measures are proportionate and account for fundamental rights. However, there is no guidance about platforms' liability if any such measures, and especially if incentivised by the one-hour removal deadline, lead to adverse impact on fundamental rights. As it stands, platforms might be excused for thinking that they risk getting punished for complying with the regulation.

Thirdly, there is little clarity regarding potential penalties (Article 18). The regulation states that "systematic and consistent failure" to comply with the removal orders will lead to financial punishment of up to four percent of the company's global turnover, but the regulation does not define what "systematic and consistent" means. Even less clarity is provided with regards to other infringements, including complying with the "specific measures" in Article 5. There is mention of potential exemption from financial penalties for smaller platforms. However, there is little certainty provided as to when exactly platforms can expect such penalties to be imposed, and there is no assurance that platform size and financial strength will be taken into account. Instead, this seems to be entirely at the discretion of the competent authority and Member States. It is therefore very difficult for smaller companies to know exactly what they are required to do to avoid penalisation. Moreover, in a move that resembles regulation in less democratic jurisdictions, company legal representatives may also be held legally liable for breach of this regulation, although it is not clear what threshold will need to be met for this to apply.

Lack of safeguards regarding competent authorities

Given the important role played by competent authorities, we encourage the EU to clarify what safeguards it will put in place to ensure that competent authorities do not undermine the rule of law, human rights, and freedom of speech. We note that, whilst the regulation states that such authorities "shall not seek or take instructions" from any other body (Article 13), there is no clear explanation of how this will be prevented or monitored. Further, no clear expectations on competent authorities' expertise on terrorism and human rights considerations are found in the regulation. Much criticism against the regulation concerns the fact that competent authorities can issue removal orders across borders, which critics assess can lead to extra-territorial enforcement of national speech codes, or removal orders being abused to remove legitimate content. Such concerns are partly due to there being no formalised threshold for what type of bodies are eligible for competent authority status. Whilst competent authorities may scrutinise each other's removal orders[1], it is unclear by what standards such scrutiny should be carried out and who will monitor that competent authorities do not abuse or mistakenly place "specific measures" duties on tech platforms. Lastly, it is currently unclear how the EU will ensure that competent authorities are consistent in their decisions to penalise companies under Article 18.

The EU should therefore seek to confirm what safeguards will be put in place to prevent abuse of removal orders and other responsibilities placed with the competent authorities. Furthermore, the EU should clarify how it aims to ensure competent authorities are consistent in their decisions to penalise platforms to provide legal certainty for platforms.

[1] If a competent authority in Country A issues a removal order to a platform with this base in Country B, the latter's competent authority will have the right to scrutinise the removal order.

Incentives and smaller tech company support mechanisms

We have concerns about the incentives the law creates and what the effect of those will be. The incentive is clear: tech companies should remove more terrorist content, and preferably swiftly, to avoid punishment. Whilst the aim of the regulation is not misguided (much of Tech Against Terrorism's work revolves around supporting tech platforms in tackling terrorist content swiftly) there are obvious concerns with an intergovernmental entity like the EU mandating by law the swift removal of a particularly hard to define content category, including how such an arrangement will impact the free, transparent, and competitive internet that the EU seeks to encourage.

Much of this due to the fact that smaller platforms will not be able to comply with the regulation, including the one-hour removal deadline, the transparency requirements (Article 7), and the six-month preservation requirement (Article 6).[2] Worryingly, platforms are also being asked to inform users when their content has been removed as a result of a removal order (Article 11)[3], which seems to outsource a key part of the remedy process to private platforms rather than the authority which ordered the content to be removed.

At Tech Against Terrorism, our key focus is on supporting smaller platforms in tackling terrorist use of the internet. To date we have worked closely with 25 companies to improve their counterterrorism practices as part of our mentorship programme. Furthermore, we have alerted more than 4,000 URLs to 50 different tech companies via the Terrorist Content Analytics Platform, which has been funded by the Government of Canada. In our global workshops, we have engaged with more than 150 tech companies around the world. We are ready to help further, and are already adapting our support mechanism to ensure we can help smaller platforms to comply with this regulation. However, scaling this work – which will be required to help tech companies comply with the regulation and avoid harming competition and innovation in the European tech space – will require time and resources. Without this being provided, the regulation could incentivise smaller tech companies to subscribe to protocols, technology, and coalitions developed by larger tech platforms that are unaligned with EU priorities and the objectives set out in the Digital Services Act.

[2] Companies that remove terrorist content will need to preserve it for six months.
[3] Article 11 states that tech companies will need to inform users when their content has been deleted for counterterrorism purposes, although competent authorities can request that companies refrain from doing so.