FRISCO
Fighting Terrorist Content Online

FRISCO Closed-Door Workshop Report

"The TCO Regulation from the Perspective of National Stakeholders: Bridging Policy and Practice"

DEMOKRITOS · TREMAU · INACH · MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER · CIVIPOL · learn · Violence Prevention Network · IVSZ

Funded by the European Union

On the second day of the FRISCO project's final conference (18 October 2024), a closed-door workshop entitled The TCO Regulation from the perspective of national stakeholders: bridging policy and practice was held for a selected group of regulators and law enforcement experts from across the EU. Participants were invited to discuss and share national experiences and practical lessons from the implementation of the TCO regulation, as well as to brainstorm solutions to ongoing common challenges.

A presentation of EUROPOL's PERCI platform demonstrated the support the tool can offer to EU Member States (MSs), which might further increase in the future, including as a result from the ongoing evaluation and revision processes related to the TCO regulation. The main functions of PERCI are to enable centralised transmission of removal orders, but also referrals, which allows for de-confliction and coordination between Member States and scrutiny of cross-border referral orders. Since July 2023, over 1000 removal orders have been transmitted via PERCI, as well as over 37,000 referral notifications, which demonstrates that the tool is in use by most Member States. There are over 600 HSPs already that have access to the tool, although the information on points of contact of HSPs for the receipt of removal orders is still scarce. Participants suggested to allow national regulators to access and use PERCI who are not competent authorities for the TCO, but for the DSA, which might be an option in the future.

State of Implementation

The workshop demonstrated that Member States are at various stages of adopting the TCO stipulations into national workflows, depending on the degree to which national legislation covering illegal online content and processes existed before the TCO regulation entering into force and the duration of and hurdles to the process of designation of national competent authorities.

- Since many national agencies acquired new competencies, **new structures had to be created** accordingly in some Member States. Sometimes even entirely new agencies.

- Where **competencies are shared between multiple agencies**, communication channels and workflows had to be established. In some cases, national legislation had to be created to govern these new relationships and to implement the TCO Regulation at national level. This process is still pending in some Member States.

- **Yet approaches differ considerably**. Some MSs are not using referrals at all but only removal orders, while in others, referrals are a well-established pre-existing mechanism that leads to high levels of compliance by HSPs affected and which has a lower legal threshold compared to removal orders, for which a court order is required in some countries.

- In cases of **imminent threat to life**, referrals are not as effective due to the urgency, and removal orders are the preferred approach.

- Some Member States already had **well-developed systems and processes** to handle terrorist content online, including well-established referral and removal approaches (e.g. France). For them the **TCO Regulation is used complementary** to the national framework and the same authorities implementing it are also in charge of TCO implementation. The TCO was also found helpful for **streamlines processes in cross-border cases** particularly.

Funded by
the European Union

- Participants stressed that in some instances **national law is broader than the TCO Regulation**. For example, some categories of online services are not covered by the TCO but are important as they are affected by terrorist content (such as internet service providers and search engines). In some countries they are covered by national law. In France, the bulk of the content is dealt with via removal request under national law, which are sent to both the content provider and the HSP and allow for delisting and access blocking measures, not only removal. At the same time the TCO is complementary and is used when there is a need to escalate or send a stronger message to uncooperative platforms, due to the **deterrence effect of potential penalties**.

- Many MSs have already developed **country-specific guidelines for HSPs** on the TCO and held information and awareness raising events. Most MSs reported that they are using PERCI to transmit referrals and removal orders and find it useful to centralise procedures and deconfliction.

Challenges and Recommendations

Participants pointed out a persistent **lack of resources** by many authorities that makes it necessary to prioritise crime areas other than terrorist content online. Assessing content is not always already within the competencies of the competent authorities and is an area in which additional capacities are required for many MSs.

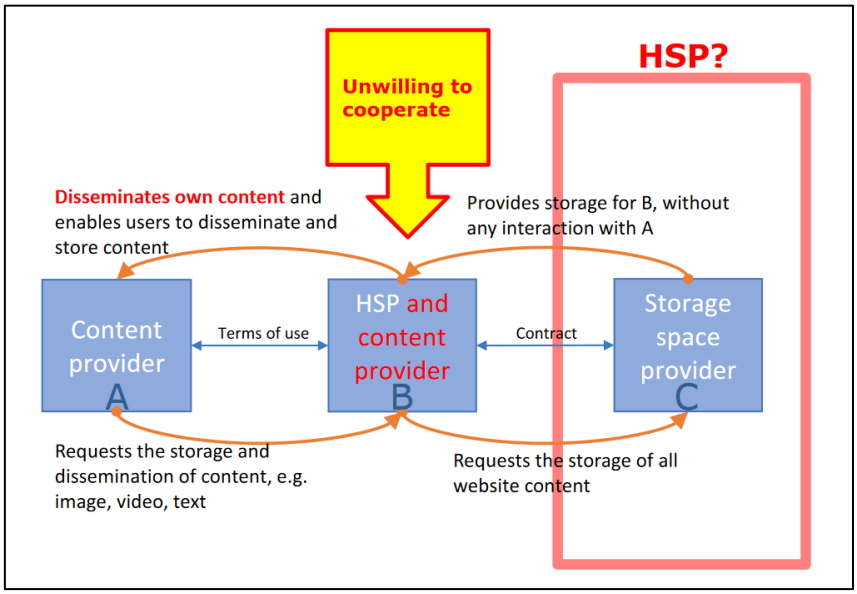
The **detection of content** is another area where authorities would benefit from additional resources. While some structures for the active detection of terrorist content exist, until now these are predominantly geared towards Islamist content. **Assessing hybrid threats, hate speech and borderline content** was mentioned as a particular challenge for security actors.

In many Member States, **no exhaustive list of Hosting Service Providers** (HSPs) exist that the competent authorities could use to get in contact with HSPs and inform them of their obligations. Depending on the size of the MS and the number of HSPs registered nationally, some have proactively gathered this information, while for others this task will still require considerable resources.

One specific challenge was highlighted regarding access to and **willingness to cooperate of intermediary services**. In cases where HSPs cannot be reached themselves or via intermediaries, some competent authorities have standing cooperations with internet service providers, who, as a last resort, can be asked to take down entire websites. This is also the procedure that many MSs apply to hostile or terrorist websites, in some instances via subpoenas.

A specific challenge was highlighted by the German authorities, relating to determining liability in the case of uncooperative HSPs who act as intermediaries and are both a Hosting Service Provider for a content provider, as well as a content provider whose content is stored by a storage space provider. Such cases pose the question which entity is ultimately disseminating the content to the public – and hence is liable. This requires further assessing the type of services each of the entities involved provides and how the content is managed (and who can modify the content as per TCO Recital 14), to determine liability and scope of application of the TCO Regulation.

Funded by
the European Union



Generally, responses to removal orders by HSPs have been accommodating and only one case was mentioned in which an HSP did not comply. Since this case is still ongoing, it could not be discussed in detail.

Representatives of some MSs pointed to persisting difficulties **in localising HSPs** (e.g. in the case of websites) as well as in working with **HSPs located outside the EU** and that focus should be put on this target group in a revised TCO. A possible solution can be for HSPs to automate blocking/removal of content via geofencing, but this solution requires further discussion at EU level and an amendment of the TCO Regulation.

Participants agreed that **more effort and resources need to be invested to reach out to HSPs,** inform them of their obligations and support them with implementation. Projects like FRISCO are contributing greatly to raise awareness among the target group and are supporting efforts by the national competent authorities.

Another recommendation was **to harmonise language across the DSA and TCO** as well as other complementary regulations, especially because the type of services affected by both overlap, yet the DSA has a broader scope by also covering intermediary service providers, not only Hosting Service Providers.

Specific measures required from HSPs that have been exposed to terrorist content (by receiving two or more removal orders within the past 12 months) have not been discussed, since authorities are not confronted with many such cases yet.

Funded by the European Union

About FRISCO

FRISCO ("*Fighting Terrorist Content Online*") is an EU-funded project implemented by a team of 8 partners across Europe. Our main objective is to raise awareness among small tech companies and online platforms and to help them comply with the EU Regulation on Terrorist Content Online (TCO Regulation). By supporting the fight against terrorist content in Europe, we are helping to prevent and counter violent extremism online and to create a safer online environment.

Follow us

friscoproject.eu
frisco-eu-project
FRISCOproject

Funded by the European Union

Disclaimer: This report is part of the EU-funded project FRISCO (https://friscoproject.eu/). Views and opinions expressed are however those of the speaker(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.