tech against terrorism europe

Digital Services Act & Terrorist Content Online Regulation

Analysis and comparison

Funded by the European Union

Executive Summary

The Digital Services Act (DSA) and the Regulation on Terrorist Content Online (TCO) are both legislative measures enacted by the European Union (EU) which are aimed at regulating digital services and combating the spread of harmful content online.

While both measures are concerned with reducing online harm in the EU, they differ in the nature and extent of: the harm they purport to mitigate; the burden of compliance imposed on platforms undertaking relevant activities; and on the activities which bring platforms in scope.

In its concern with a more specific and egregious form of online harm, the TCO generally imposes more stringent requirements on tech platforms and is expressed in more mandatory terms. However, this is not uniformly the case across all the areas which are common to both the DSA and the TCO. In the matter of crisis response in particular, the DSA's requirements are more exacting and potentially more onerous than those provided by the TCO.

Funded by the European Union

Introduction

The DSA, which is envisaged to come fully into force in February 2024, aims to revamp the regulations governing digital services within the EU and foster a safer online environment for users. Its primary goal is to modernise and harmonise the digital service regulations across the EU, and to establish clear responsibilities and accounting mechanisms for digital service providers.

The TCO, which came into force on June 7 2023, contributes to the EU's effort to combat terrorist content online, prevent radicalization, enhance international cooperation to ensure rapid content removal, and protect online platforms and trust users.

This analysis aims to provide an extensive comparison of the two regulations by analysing their similarities and differences in the following key areas:

1. Definitions
2. Platforms in scope
3. Removal orders and specific measures
4. Content moderation
5. Complaint mechanisms
6. Transparency report
7. Crisis response mechanism

To become more acquainted with global online regulation related to counterterrorism and violent extremist content, check out Tech Against Terrorism's (TAT) Online Regulation Series[1] which examines over 100 pieces of legislation from 30 jurisdictions around the world. Tech Against Terrorism Europe[2] (TATE) has also created a guide[3] which both discusses the obligations on hosting service providers (HSPs) to counter the dissemination of terrorist content online and provides practical advice on how to fulfil these obligations.

Definitions

The TCO defines *terrorist content* as content that:

- *Incites the commission of one of the offences referred in (a) to (I) of EU Directive 2017/541, where glorifying terrorist material or advocating of terrorist offences (directly or indirectly), thus causing a danger of the offences being committed.*
- *Solicits a person to commit or contribute to a terrorist offence*
- *Solicits a person or a group to participate in activities of a terrorist group, as defined by Art.4 (b) of EU Directive 2017/541*
- *Provides instructions on the making of weapons for the purposes or committing or contributing to the committing of a terrorist offence.*

Funded by the European Union

- *Constitutes a threat to committing a terrorist offence*[4]

Although the DSA does not include an explicit definition of terrorist content, it offers a detailed description of the term i*llegal content*, which encompasses terrorist content, and is defined as*:*

> *"Any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law."*[5]

TCO	DSA
The TCO defines terrorist content as any content that promotes, encourages, or instructs the commission of terrorist offences.	The DSA defines illegal content as any information that does not comply with EU legislation, or the law of a member state concerned.
Examples: • Terrorist propaganda • Incitement • Instructional material	Examples: • Hate speech • Child sexual abuse material • Hate crimes • Incitement to violence • Copyright infringement • Counterfeit goods

Platforms in Scope

Definitional and Territorial Scope

The Digital Services Act covers three types of intermediary services: **mere conduit services, caching services, and hosting services**. The latter is defined as a service "consisting of the storage of information provided by, and at the request of, a recipient of the service."[6] The DSA applies to various digital intermediaries and encompass all services provided through the internet. This affects hosting providers in particular, and includes platforms that store user-generated content and make it available on demand. Even third-party traders selling on online marketplaces are impacted because the marketplaces must obtain specific information from these traders. However, there is an exception: if the storage and distribution of user-generated content is only an insignificant part of the service, then the regulation does not apply.

DCU GHENT UNIVERSITY JOS LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN SAHER EUROPE Swansea University Prifysgol Abertawe tech against terrorism Funded by the European Union

By its territorial scope, the DSA aims to establish a secure digital environment across the EU. The law applies when relevant intermediaries:

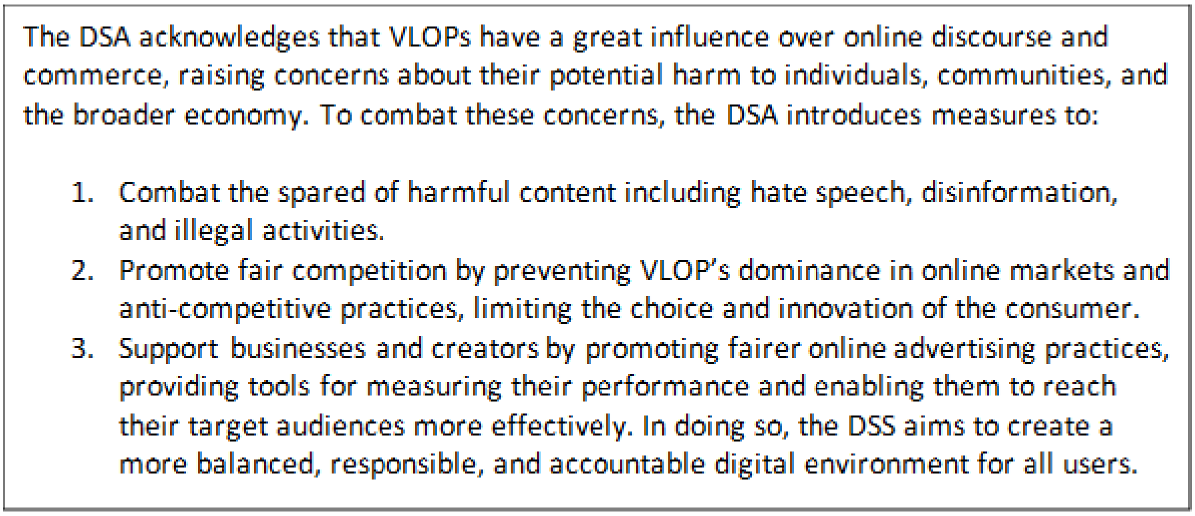
- *Have an establishment in the EU; or*
- *Have a significant number of users in the EU; or*
- *Target its activities towards one or more EU member states.*[7]

The TCO has a different scope and focuses on Hosting Service Providers (HSPs). As defined in point (b) of Article 1 of Directive (EU) 2015/1535 of the European Parliament and of the Council, the TCO refers to "any service normally provided for remuneration, at a distance, by electronic means and at individual request of a recipient of service."[8] As per Article 2 of the TCO, the regulation applies to HSPs that:

- *Have a significant number of users of its services in one or more Member States; or*
- *Target their activities to one or more Member States.* [9]

Platform Size

The Digital Service Act encompasses a broad spectrum of online intermediaries, including internet service providers, cloud services, messaging platforms, marketplaces, and social media networks. Specific due diligence obligations apply to hosting services, in particular very large online platforms (VLOPs) which have a significant societal and economic impact, reaching at least 45 million users in the EU, which represents 10% of the EU population.



The DSA acknowledges that VLOPs have a great influence over online discourse and commerce, raising concerns about their potential harm to individuals, communities, and the broader economy. To combat these concerns, the DSA introduces measures to:

1. Combat the spared of harmful content including hate speech, disinformation, and illegal activities.
2. Promote fair competition by preventing VLOP's dominance in online markets and anti-competitive practices, limiting the choice and innovation of the consumer.
3. Support businesses and creators by promoting fairer online advertising practices, providing tools for measuring their performance and enabling them to reach their target audiences more effectively. In doing so, the DSS aims to create a more balanced, responsible, and accountable digital environment for all users.

Similarly, very large online search engines with more than 10% of the 450 million consumers acquire a greater responsibility for tackling illegal content online.[10] Very large enterprises are additionally responsible for:

- Carrying out evaluations of potential risks that may affect the EU, including threats to civic narratives, fundamental rights, and the dissemination of illegal content through their services.
- Taking appropriate measures to address identified risks by implementing strategies to mitigate them.
- Conducting an independent annual audit to ensure compliance and effectiveness of risk mitigation efforts.
- Establishing a user complain mechanism that remains available for users for at least 6 months.

By contrast, the TCO does not contemplate any additional responsibilities according to the size and the reach of the platforms.

Removal orders and Specific Measures

Under the DSA, platforms are required to comply with removal orders issued by Member States for illegal content *without undue delay.*[11] Although there is no specific timeframe mentioned, the DSA makes a reference to the 24-hour removal suggested by the 2016 Code of Conduct on Countering Illegal Hate Speech Online.[12] The DSA specifically states in Article 8 that platforms are not subject to a broad monitoring responsibility but are required instead to respond to individual instances of illicit content without engaging in constant proactive surveillance.

In the case of the TCO, EU Member States have a designated Competent Authority empowered to issue removal orders to HSPs requiring them to take down content or disable access to it in the EU. The TCO establishes stricter guidelines that require the removal of terrorist content online ordered by these Member State Competent Authorities within an hour of receipt. The Competent Authority should provide the HSP with applicable procedures and deadlines at least 12 hours prior to issuing the first order. If an HSP cannot comply because of *force majeure*, including technical and operational reasons, the HSP should inform the Competent Authority without undue delay.

The TCO introduces specific measures for HSPs that are "exposed to terrorist content". These platforms are those that have been found to host terrorist content more than twice in a year. As part of the additional responsibilities, platforms are expected to:

- Establish a team dedicated to identifying and removing terrorist content (as well as developing and implementing preventive measures).

- Conduct a risk assessment to identify the specific threat posed by terrorist content on their platform.
- Implement preventive measures to reduce the risk of terrorist content being shared on the platform.
- Conduct regular audits of content moderation practices.

Content Moderation

One of the main objectives of the TCO is to eradicate terrorist content from the online sphere. To reach this objective, platforms need to take proactive measures to remove terrorist content and implement detection techniques to deter users from accessing it. Well-defined procedures are provided in the TCO which give clear guidelines for reporting and removing such content. Content screening and detection technologies may be used to ensure efficient identification and prevention of online terrorist content.

By contrast, Article 27 of the DSA establishes broader responsibilities and highlights the active participation of moderators in preventing the propagation of illegal content. In addition to making their terms and conditions transparent, platforms must provide a clear and specific statement of reasons when imposing restrictions on content uploaded by the users. HSPs must explain the facts and circumstances relied on when taking the decision, including whether the content is considered illegal or violates the platform’s terms and conditions (with reference to concrete legal or contractual agreements).

Moderators are further encouraged by the DSA to detect and remove potentially harmful content. However, while the legislation exempts micro and small firms from this activity due to their reduced capability, and as much as they are not required to report, such platforms must still follow the principles of responsible content moderation. This method aims ensure balanced treatment by aligning regulatory requirements with the differing capabilities and resources of the entities.

Complaint Mechanism

Both the DSA and the TCO require platforms to have complaint mechanisms that prioritise consideration of the user's perspective when resolving concerns relating to a piece of content uploaded by that user.

The DSA lays out several procedures that users affected by content moderation can rely on to complain against and challenge decisions taken by a provider. Under the DSA, users have the option to directly complain to the platform provider using internal complaint mechanisms or seek redress before national courts. The DSA obliges online platform providers to establish internal complaint-handling mechanisms, enabling users to file a complaint electronically and free of charge.

The platform providers must handle complaints in a "timely, non-discriminatory, diligent and non-arbitrary manner and under the control of appropriately qualified staff, not solely on the basis of automated means."[13] When the user complaint contains enough evidence for the platform provider to consider that its decision is not justified, the provider shall reverse its decision without undue delay.

Under the TCO, HSPs are also required to create user-friendly complaint mechanisms and ensure that all complaints are dealt with rapidly and transparently. When content is taken down, platforms need to provide a message in lieu of the content which explains why the content was removed and mentions that the action has been taken in line with the TCO. Article 10 also establishes that if the content removal is found to be unjustified, the HSP must reinstate the content and notify the complaint within two weeks of receipt of the original complaint. If the HSP decides to reject the appeal, it must provide the user with an explanation.

Transparency Reports

The DSA requires platforms to provide annual transparency reports that allow assessment of the platforms' content moderation efforts, the removal orders received and actioned, user complaints, and actions taken. Transparency reports should be easily accessible to the general public.

The TCO imposes similar obligations since it requires platforms engaging in content moderation to prepare an annual report. However, compared with the DSA, the TCO report needs to include more information, notwithstanding its greater focus on the removal of terrorist content. To follow the established guidelines, TCO-mandated reports should include information on measures taken both to identify and remove content and to address the reappearance of content, especially when using automated tools, as well as statistics relating to:

- Pieces of terrorist content removed or disabled following removal orders, or specific measures, as well as the pieces of content not removed.
- Complaints handled by the HSP.
- Administrative or judicial reviews requested by the HSP.
- Cases in which the HSP was required to reinstate content following review.
- Cases in which the content was reinstated following a complaint from a suer.

Some platforms opt to combine the DSA's Yearly Report with the TCO's Transparency Report. When doing so, they must clearly indicate their adherence to the reporting rules and make sure they include all the information required under both reporting obligations. Tech Against Terrorism offers a number of resources to upskill platforms in transparency reporting, including transparency reporting guidelines[14] and a TCO transparency report template.

Funded by the European Union

Crisis Response Mechanism

Article 36 of the DSA requires platforms to take specific measures when a crisis is declared, defined as a serious threat to public security or public health in the Union, which includes acts of terrorism or emerging acts of terrorism. The DSA crisis response mechanism empowers the European Commission to require very large online platforms (VLOPs) and very large online search engines (VLOSEs) to make specific risk assessments and take specific risk mitigation measures tailored to the crisis at hand. As a result, VLOPs and VLOSEs will need to assess how they function during times of crisis and how they might use their services to contribute to mitigating the crisis. The DSA recommends that VLOPs initiate voluntary crisis protocols.

In this case, the TCO has a more limited role since HSPs must promptly inform the relevant authorities of the Member State concerned, or the Competent Authority of the Member State they are established in, of imminent threats to life or suspected terrorist offences.

The European Union has created the EU Crisis Protocol (EUCP), a voluntary mechanism to help coordinate rapid cross/border responses to the viral spread of terrorist and violent extremist content online in response to real world incidents[15]. This protocol clarifies the relationship between the voluntary EUCP and the TCO, on Article 14(5) providing for an imminent threat to life situation. The EUCP also outlines the specific procedures, roles, and responsibilities of key actors and identifies tools for monitoring and exchanging critical information.

Focusing on removing harmful content, the Global Internet Forum to Counter Terrorism (GIFCT) leverages the Content Incident Protocol (CIP). This protocol enables the swift takedown of content linked to terrorist or violent extremist events, including live streams of murders or attempts directly preceded by the perpetrator or accomplice.[16]. Following a declared Content Incident Protocol (CIP) by the GIFCT Operating Board, hashes of an attacker's video and related content are distributed within the GIFCT hash database. This empowers member platforms to identify and remove this content from their platforms. Tech Against Terrorism can activate its own response based on GIFCT CIP that is verified against its own criteria[17].

DCU GHENT UNIVERSITY LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN SAHER EUROPE Swansea University Prifysgol Abertawe tech against terrorism Funded by the European Union