Coimisiún na Meán

Terrorist Content Online Regulation Q&A

13 June 2024

General

1. What is the Terrorist Content Online Regulation?
   The Terrorist Content Online Regulation (TCOR) is an EU law which creates mechanisms to counteract the dissemination of terrorist content online and to require the speedy removal of terrorist content by hosting service providers.

2. What is terrorist content?
   Terrorist content is content that incites, solicits, threatens or provides instruction on the commission of terrorist offences. TCOR defines illegal terrorist content as information which is used to incite and glorify the commission of terrorist offences, encouraging the contribution to and providing instructions for committing terrorist offences as well as promoting participation in terrorist groups.

3. What is a hosting service provider under the Terrorist Content Online Regulation?
   Under the Regulation, a hosting service provider (HSP) is a service which allow users to store and share publicly available information online. Examples of hosting service providers include social media platforms, web hosting services and cloud services.

4. Who is responsible for enforcing the Terrorist Content Online Regulation in Ireland?
   An Garda Síochána is the body responsible for issuing removal orders to hosting service providers when content appears on their services. Coimisiún na Meán was designated as a competent authority under TCOR by Minister for Justice Helen McEntee to oversee the measures taken by HSPs based in Ireland when they are exposed to terrorist content, this role took effect on 30 November 2023.

5. What is Coimisiún na Meán's role regarding services exposed to Terrorist Content?
   Coimisiún na Meán determines when hosting services providers are exposed to terrorist content and oversees how they implement ''specific measures" to prevent the further dissemination of terrorist content, pursuant to Article 5 of TCOR.

   Coimisiún na Meán will assess the mitigating steps hosting service providers take, supervise their response to removal orders and look at issues relating to reporting, remedy and further mitigation.

Decision Framework

1. What is the Decision Framework for the Terrorist Content Online Regulation?

Coimisiún na Meán has published a Decision Framework for TCOR. This Decision Framework represents the decision-making process Coimisiún na Meán will follow to determine if a hosting service provider in Ireland is exposed to terrorist content.

2. Under the Decision Framework, what is the criteria for a hosting service provider to be deemed as exposed to terrorist content?
   Once Coimisiún na Meán has been notified of two or more final removal orders for terrorist content in the previous 12 months, Coimisiún na Meán will then consider whether to apply the provisions of the Terrorist Content Online Regulation, following the Decision Framework.

3. What steps will Coimisiún na Meán take when they are informed that a hosting service provider in Ireland has received two or more final removal orders for terrorist content?
   The Decision Framework follows a two-stage process:

   Stage 1: Preliminary Decision and Engagement with the Provider
   When Coimisiún na Meán is notified that a hosting service provider in its jurisdiction has received two or more final removal orders in the previous 12 months, it will consider the matter and make a preliminary decision on whether the provider is exposed to terrorist content. Before taking a decision that a provider is exposed to terrorist content, Coimisiún na Meán will engage with the HSP setting out the reasons informing the preliminary decision taken by the Commission and inviting the provider to respond. The provider may respond to Coimisiún na Meán within a period of three weeks. A provider's failure to respond or engage with Coimisiún na Meán within this stage will not preclude Coimisiún na Meán from taking a decision based on the existing evidence available to it.

   Stage 2: Decision
   This stage of the Coimisiún na Meán's decision-making process involves taking a Decision, having regard to the information available to it, and representations received following engagement with the relevant hosting service provider under Stage 1. Coimisiún na Meán will take a decision finding that the provider is or is not exposed to terrorist content. The decision will take effect upon Coimisiún na Meán issuing the provider with written notice of the Decision.

4. How will the public know that Coimisiún na Meán has decided that a hosting service provider is exposed to terrorist content?
   If Coimisiún na Meán decides that a hosting service provider is exposed to terrorist content, this decision, and the name of the provider to which it relates, will be published on the Coimisiún na Meán website.

Obligations on Hosting Service Providers

1. What actions are hosting service providers required to take if the Commission decides the provider is exposed to terrorist content?
   Following a decision that it is exposed to terrorist content, a hosting service provider's key obligations are to:
   - *Where applicable, include in its terms and conditions and apply provisions to address the misuse of its services for the dissemination to the public of terrorist content;*
   - *Take specific measures to protect its services against the dissemination to the public of terrorist content;*
   - *Report to Coimisiún na Meán, within three months of receipt of the Decision and on an annual basis thereafter, on the specific measures that it has taken and that it intends to take in order to comply with the obligations set out above.*

2. What are the specific measures that hosting service providers are required to take?
   It is for the hosting service provider to decide which specific measures it will take, and Coimisiún na Meán has an evaluation function. TCOR indicates that measures may include one or more of the following:
   - *appropriate technical and operational measures or capacities, such as appropriate staffing or technical means to identify and expeditiously remove or disable access to terrorist content;*
   - *easily accessible and user-friendly mechanisms for users to report or flag to the HSP alleged terrorist content;*
   - *any other mechanisms to increase the awareness of terrorist content on its services, such as mechanisms for user moderation; and*
   - *any other measure that the HSP considers to be appropriate to address the availability of terrorist content on its services.*

3. Will the specific measures taken by hosting service providers be effective to deal with the dissemination of terrorist content?
   The measures which are taken by the hosting service provider must be effective in mitigating the level of exposure of the services of the provider to terrorist content. They must also be targeted and proportionate.

   The measures must be applied in a manner which takes full account of the rights and legitimate interests of users, including fundamental rights concerning freedom of expression and information, respect for private life and the protection of personal data.

   The specific measures must also be applied in a diligent and non-discriminatory manner.

4. How can it be guaranteed that hosting service providers will implement the required specific measures?
   A hosting service provider must report to Coimisiún na Meán on the specific measures that it has taken and intends to take. If, based on the reports provided by the hosting service provider or, where relevant, any other objective factors, Coimisiún na Meán considers that the specific measures do not meet the provider's obligations under TCOR, Coimisiún na Meán will address a decision to the provider requiring the necessary measures be taken to ensure that the obligations are complied with.

5. Can a hosting service provider appeal a decision taken by Coimisiún na Meán that it is exposed to terrorist content?
   Following a Decision that a hosting service provider is exposed to terrorist content, the provider may, at any time, request Coimisiún na Meán to review and, where appropriate, amend or revoke a Decision.

   In reviewing the Decision, Coimisiún na Meán will consider any additional information provided by the hosting service provider as part of the request for review. Coimisiún na Meán may also invite the provider to provide any further information which it may require as part of the review.

   If Coimisiún na Meán decides to revoke a Decision, the hosting service provider's reporting obligations cease. However, if the Decision is upheld, the provider will be obliged to continue reporting until such time as Coimisiún na Meán deems that the provider is no longer exposed to terrorist content.

Users

1. What should users do if they come across terrorist content on an online platform?
   Users should in the first instance report the content to the platform where they saw it. If a user believes that the content represents an immediate threat or risk to life or property, they should immediately inform An Garda Síochána. Users may also report terrorist content to Coimisiún na Meán via the Contact Centre.

The public can contact the Contact Centre by emailing usersupport@cnam.ie or calling 01 963 7755 from Monday-Friday, 8am-6pm.

2. How does the Terrorist Content Online Regulation help to keep users safe online?
   TCOR outlines the responsibilities of hosting service providers to take appropriate, reasonable and proportionate actions to ensure the safety of their services and to swiftly and efficiently detect and remove terrorist content online, considering the fundamental importance of freedom of expression and information in an open and democratic society.

Online Safety Framework

1. What is the Online Safety Framework?
   The Online Safety Framework is composed of the Digital Services Act, the Online Safety Code and the Terrorist Content Online Regulation (TCOR). When taken together, the Online Safety Framework will encompass all of the powers of Coimisiún na Meán to regulate online platforms at a systemic level, and to improve online safety for all users.

2. How is terrorist content addressed in the Digital Services Act and the Online Safety Code?
   Under the Digital Services Act, online platforms are required to act quickly to remove or disable access to illegal content when the platform becomes aware of it. Terrorist content is regarded as illegal content under the Digital Services Act.

   The Online Safety Code places an obligation on Video-Sharing Service Providers (VSPSs) to take appropriate measures to protect the public from programmes, user-generated videos and audiovisual commercial communications containing content the dissemination of which constitutes an activity which is a criminal offence under EU law.

Sanctions

1. What sanctions can be applied to hosting service providers under TCOR?
   Infringement by hosting service providers of the Terrorist Content Online Regulation can lead to the imposition of administrative fines, including financial penalties of up to four percent of global turnover.