Eyes Shut, Fingers Crossed: The EU's Governance of Terrorist Content Online under Regulation 2021/784

Valerie Albus

Abstract

This chapter introduces the legislative background, key provisions, and main academic debates surrounding the EU's Terrorist Content Online Regulation (TCO Regulation). The TCO Regulation was the first EU instrument to introduce legally binding rules for hosting service providers regarding the moderation of illegal content, thereby paving the way for subsequent EU Regulations, such as the Digital Services Act. The TCO Regulation establishes a new set of responsibilities for hosting service providers. On the one hand, they must respond to removal orders issued by national competent authorities and take down terrorist content within one hour. On the other, hosting service providers must take preventive measures to ensure that terrorist content remains off their platform, thereby contributing to the prevention of radicalisation and, potentially, terrorist acts. Regrettably, the modalities of the TCO Regulation may undervalue the complex assessments required to determine whether a text, image, or video constitutes terrorist content. Short deadlines and high fines, along with the fact that some Member States do not require a judicial review to issue removal orders, raise concerns regarding the over-removal of content and related risks for fundamental rights. At the same time, the limited transparency obligations for hosting service providers are a missed opportunity to assert public oversight over platforms' (often automated) content moderation practices. While the EU's push for increased responsibility may have prompted hosting service providers to intensify their fight against terrorist content, the TCO Regulation created a system in which the EU Member States choose to remain ignorant as to how this is achieved.

1. Introduction

The spread of terrorist content on online platforms has become a significant security concern over the past decade. Terrorist groups have exploited social media and video-hosting services to disseminate their messages and recruit new followers. Over time, not only the radicalisation of individuals, but also terrorist acts themselves have become more internet-centric. The most recognised example is the 2019 terrorist attack in Christchurch, New Zealand, in which 51 people were murdered and many more injured. Prior to the attack, the perpetrator published a manifesto online and livestreamed the shooting using Facebook Live. This reignited discussions among policymakers about the role of online platforms in the planning and execution of terrorist acts.

Around the same time, over 18,000 kilometres away, the EU institutions in Brussels were negotiating Regulation 2021/784, better known as the Terrorist Content Online Regulation (hereafter, the TCO Regulation). One year earlier, the European Commission tabled its proposal for a Regulation to introduce legally binding rules for hosting service providers on how to deal with terrorist content. The proposal aimed to create so-called removal orders that would allow national competent authorities to compel hosting service providers to remove any such content within one hour. The Regulation's scope aimed to encompass all service providers that enable users to store and disseminate content to the public. This includes social media platforms, such as Facebook, Instagram, and X, as well as video-sharing services like YouTube or Twitch.

After lengthy negotiations, the TCO Regulation was adopted on 29 April, 2021, and became applicable on 7 June, 2022. It now applies to all hosting service providers operating within the EU, irrespective of their place of main establishment (Art. 1(2) TCO Regulation). This includes service providers that are based outside of the EU but provide their services to European users. This approach has allowed the EU to govern the moderation of terrorist content beyond its borders.

The TCO Regulation appeals to the "particular societal responsibilities" of hosting service providers (Recital 5 TCO Regulation). These are expressed in several new duties that such providers must fulfil in order to protect their users from terrorist content. Aside from actualising the aforementioned removal orders, hosting service providers are required to take preventive measures to ensure that their services are not being misused to spread terrorist content. Consequently, hosting service providers

have become the protagonists in the fight against terrorist content: It is primarily *their* responsibility to choose and implement the technological solutions needed to ensure that their platforms stay "clean". Accordingly, their role transcends mere compliance, in that it also involves proactive enforcement, similar to that of public authorities (Tosza, 2021, p. 16). This has prompted scholars to examine the broader shifts in the enforcement landscape brought about by the TCO Regulation, considering that it fosters new modes of EU security integration (Bellanova and De Goede, 2021).

Certainly, even before the TCO Regulation entered into force, many hosting service providers already moderated user-uploaded content, thereby placing limits on freedom of expression and public participation online (Jørgensen and Pedersen, 2017). The novelty of the TCO Regulation is that, for the first time, the EU legislator defined *what* content should be removed and *how*. This has naturally generated discussions on whether the EU has struck the right balance between enlisting hosting service providers in the fight against terrorist content and safeguarding users' fundamental rights to freedom of expression and information.

Being *the first of its kind* makes the TCO Regulation a particularly interesting object of study. The Regulation created path-dependencies, determining the course of EU governance of illegal content more broadly. For example, removal orders were conceived in the Regulation's elaboration and have since inspired similar provisions in the Digital Services Act (DSA)[1] and sectoral legislation. To a certain extent, the TCO Regulation thereby pioneered the growing EU framework that aims to increase accountability of online service providers vis-à-vis European users.

This chapter aims to provide an introduction to the legislative text, covering its legislative history, main innovations, and key provisions. It begins with a broad overview of the background and scope of the Regulation (Section 1), followed by a detailed examination of its most important provisions (Section 2). Throughout the chapter, reference is made to the main scholarly debates surrounding the TCO Regulation, focusing on the role of hosting service providers in law enforcement and related fundamental rights concerns. Additionally, relying on the first transparency reports of

1 For more information on the DSA, see Chapter 4 'The Digital Services Act: Online Risks, Transparency and Data Access' by Marie-Therese Sekwenz and Rita Gsenger. Also, see Chapter 5, 'The Digital Services Act – an appropriate response to online hate speech?' by Pascal Schneiders and Lena Auler.

Facebook and Google, the chapter offers some (limited) empirical insights into the Regulation's first two years of application.

2. Overview

The following overview highlights several milestones in the legislative history of the TCO Regulation (1.1) before contextualising its legal basis in the EU Treaties (1.2), its scope of application (1.3), and the definition of terrorist content (1.4).

2.1 Legislative history

Against the backdrop of a heightened terrorist threat in Europe during the 2010s and concerns over terrorist propaganda acting as a "catalyst" for radicalisation (Recital 5 TCO Regulation), it is somewhat unsurprising that the first EU legislative proposal tackling illegal content focused on the dissemination of terrorist content. It is important to note that the TCO Regulation did not fill a complete legislative vacuum at the time. Several EU instruments regulating specific aspects of illegal content were already in place prior to its proposal and adoption.

Most importantly, Directive 2000/31/EC on electronic commerce ("the e-commerce Directive") had already harmonised the conditions under which intermediaries could be held liable for hosting illegal content, including terrorist content. Article 14 of the e-commerce Directive set out the general principle: Providers of intermediary services were exempt from liability in the EU if they did not have actual knowledge of illegal activity or information on their platforms and, upon obtaining such knowledge, acted expeditiously to remove or disable access to this information.[2]

In addition, sectoral legislation, such as Directive 2018/1808 on audiovisual media services and Directive 2011/93/EU to combat the sexual abuse and exploitation of children and child pornography, had been adopted earlier during the 2010s. However, these Directives did not create legally binding obligations for hosting service providers to act against illegal content, but merely laid down common definitions and minimum standards to be implemented by Member States.

2 This principle is now also enshrined in Art. 6(1) of the DSA. For further reading on the EU's system of intermediary liability, see Frosio (2020) and Wilman (2020).

After initial efforts to enhance voluntary cooperation between EU Member States and hosting service providers, such as through the EU Internet Forum launched by the European Commission in 2015 (see Mitsilegas and Salvi, 2024, p. 192), the idea of a binding EU instrument to counter illegal content began gaining traction in 2017. The European Commission first issued Communication COM/2017/0555 on 28 September, 2017, which outlined guidelines and principles to enhance the responsibility of online platforms for illegal content. This communication placed special emphasis on the business dimension of illegal content and how such content was undermining users' trust in the digital single market. The Commission maintained that, as gatekeepers of content and information, online platforms had a societal responsibility to prevent criminals from exploiting their services to spread illegal content (Communication COM/2017/0555, p. 2).

The idea of a societal responsibility of online service providers was adopted in Commission Recommendation 2018/334 of 1 March, 2018, on measures to effectively tackle illegal content online. In short, the recommendation concluded there to be a need for the EU legislator to harmonise the rules on combatting illegal content online. The Commission thus set the scene for the very broad scope of its future legislative action: The Recommendation defined illegal content as *any* information that does not comply with EU or Member States' law. Recommendation 2018/334 also stressed that online service providers should systematically enhance their cooperation with Member State authorities, such as by establishing effective points of contact and fast-track procedures to remove illegal content upon request (Recommendation 2018/334, 2018, point 22). It should be recalled here that recommendations have no binding force, but merely allow EU institutions to suggest a line of action without imposing any legal obligations.

In parallel with these efforts at the EU level, several Member States had already unilaterally adopted legislation tackling illegal content online. For instance, the German Network Enforcement Act (2017) required online platforms to delete manifestly unlawful content within 24 hours. Likewise, France adopted the Avia Law (2020), which obliged platforms to remove a range of illegal online content, and especially hate speech. However, this law was later declared to be largely unconstitutional by the French Constitutional Council.[3] The principal drawback of these national initiatives was their limited geographical scope. To ensure effective cooperation between

3 See the decision of the French Constitutional Council n° 2020-801 DC of 18 June, 2020.

the law enforcement authorities and online service providers of different countries, it was necessary to agree on an EU-wide solution.

On 12 September, 2018, the European Commission presented its proposed Regulation COM/2018/640 to counter the dissemination of terrorist content online. After lengthy interinstitutional negotiations spanning six trilogues, the TCO Regulation was finally adopted on 29 April, 2021, and became applicable on 7 June, 2022.

2.2 Legal basis

The TCO Regulation was adopted on the basis of Article 114 of the Treaty on the Functioning of the European Union (TFEU), which lays down the procedure under which the European Parliament and the Council may adopt harmonising measures which "have as their object the establishment and functioning of the internal market".

This choice may seem unexpected, especially as the TCO Regulation heavily draws from substantive criminal law and contributes to enforcing corresponding standards in the digital sphere. The legal basis may seem all the more surprising considering that, since the adoption of the Lisbon Treaty, the EU legislator has been empowered to approximate Member States' criminal procedures and harmonise substantive criminal law (Art. 82 and 83 of the TFEU; see Mitsilegas, 2016). So, why did the European Commission put forward a legal basis for the internal market to adopt the TCO Regulation?

The Commission had to make pragmatic choices when drafting the TCO Regulation. Although Art. 82 of the TFEU empowers the EU to adopt minimum rules in the area of criminal procedure, such measures must be based on the principle of mutual recognition of judgments (De Pasquale and Pesce, 2021). Put simply, this principle requires judicial authorities to automatically recognise and execute judicial decisions emanating from other Member States in the same manner as a domestic decision.[4] For example, if a French court issues a European arrest warrant for a person residing in Germany, the German authorities must recognise this decision and surrender the person to France.

As the main purpose of the TCO Regulation was to create duties for *service providers*, the proposal would not have fit in with the mutual recog-

4 For a comprehensive analysis of the principle of mutual recognition in EU law, see Janssens (2013).

nition framework, which relies on cooperation between *judicial authorities* – courts and public prosecutors. In other words, the TCO Regulation would have been an entirely different instrument if it had been adopted under the EU's framework for criminal law.

Aside from these constraints, some additional reasons render the question of the legal basis important from the perspective of the Member States. By virtue of Protocols 21 and 22, Ireland benefits from special opt-out privileges and Denmark is to be automatically excluded from Title V measures, which cover criminal law cooperation (Protocol 21 on the position of the United Kingdom and Ireland in respect of the Area of Freedom Security and Justice; Protocol 22 on the position of Ireland). Thus, by adopting the TCO Regulation on the basis of Art. 114 TFEU, the EU ensured that it would become applicable in all Member States – including Ireland, where many online platforms have their European headquarters.

Consequently, to adopt the Regulation on the legal basis of Art. 114 of the TFEU, the crime prevention goal of the measure was subordinated to the objective of promoting a safe digital single market. Mitsilegas (2016) described this phenomenon as a "functional criminal law spill-over from Title V to other parts of the Treaty" (p.6). This spill-over consists of criminal law measures being adopted under the institutional rules of other policy fields to circumvent the constraints inherent in Title V. The TCO Regulation appears to constitute an example of such a spill-over.

Therefore, when reading the legislative text, one gets the impression that the TCO Regulation awkwardly sits in two chairs. On the one hand, it builds on substantive criminal law and stresses that it should contribute "to achieve the sustained prevention of radicalisation in society" (Recital 2 TCO Regulation). On the other, the Regulation has an internal market rationale, emphasising that a European approach to combatting terrorist content is essential for protecting the functioning of the digital single market.

2.3 Scope of application

Pursuant to Art. 1(2), the TCO Regulation "applies to hosting service providers offering services in the Union, irrespective of their place of main establishment, insofar as they disseminate information to the public". Thus, the Regulation's scope centres around three different notions: "hosting",

"offering services in the Union", and "disseminating information to the public".

According to Art. 2(1) "hosting" consists of the "storage of information provided by and at the request of a content provider". Providers of social media (e.g., Facebook, LinkedIn, X) and video, image, and audio-sharing services (e.g., YouTube, Instagram) are thus covered by the Regulation's scope. In addition, the recitals state that the TCO Regulation should cover file-sharing and other cloud services insofar as these are used to make the stored information available to the public at the direct request of the user (Recital 14 TCO Regulation). The recitals also specify that interpersonal communication services, such as email or private messaging, should fall outside the scope of the Regulation (Recital 14). However, these recitals are not legally binding and only provide interpretative guidance. If the meaning of a provision in the TCO Regulation is unclear, it is ultimately the task of national courts and the Court of Justice of the European Union (CJEU) to rule on its applicability in a given case.

The notion of "offering services in the Union" should be understood as "enabling natural or legal persons in one or more Member States to use the services of a hosting service provider which has a substantial connection to that Member State or those Member States" (Art. 2(4) TCO Regulation). The notion of "substantial connection" refers to the connection of a hosting service provider with one or more Member States resulting either from its place of establishment or from specific factual criteria (Art. 2(5) TCO Regulation). Such factual criteria include having a significant number of users in one or more Member States or the targeting of its activities to one or more Member States.

This results in a very broad geographical scope of application. The Regulation covers not only hosting service providers established in the EU, but also those in third countries. The goal of this broad scope is to ensure that all hosting service providers operating in the EU's digital single market are subject to the same requirements, regardless of their country of main establishment (Recital 15 TCO Regulation). This also allows the EU to govern beyond its borders and set a potentially global regulatory standard.

Finally, "dissemination to the public" refers to "the making available of information, at the request of a content provider, to a potentially unlimited number of persons" (Art. 2(3) TCO Regulation). The Regulation's recitals provide further guidance on this notion. Indeed, they state that this should entail "making the information easily accessible to users in general, without requiring further action by the content provider, irrespective of whether

those persons actually access the information in question" (Recital 14 TCO Regulation).

2.4 Definition of terrorist content

Art. 2(7) establishes what types of material should be considered terrorist content for the purpose of the TCO Regulation. It refers to material which:

(a) incites the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such material, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;
(b) solicits a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;
(c) solicits a person or a group of persons to participate in the activities of a terrorist group, within the meaning of point (b) of Article 4 of Directive (EU) 2017/541;
(d) provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;
(e) constitutes a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541.

The relevant offences to which the TCO Regulation refers are laid down in Directive 2017/541 on combating terrorism ("Terrorism Directive"). This Directive establishes minimum rules regarding the definition of terrorist offences and penalties, and harmonised victims' rights in the EU. Art. 3(1) (a) to (i) of the Directive defines the relevant terrorist offences:

1. Member States shall take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences where committed with one of the aims listed in paragraph 2:

(a) attacks upon a person's life which may cause death;
(b) attacks upon the physical integrity of a person;
(c) kidnapping or hostage-taking;
(d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
(e) seizure of aircraft, ships or other means of public or goods transport;
(f) manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear weapons;
(g) release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life;
(h) interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;
(i) illegal system interference, as referred to in Article 4 of Directive 2013/40/EU of the European Parliament and of the Council [...] in cases where Article 9(3) or point (b) or (c) of Article 9(4) of that Directive applies, and illegal data interference, as referred to in Article 5 of that Directive in cases where point (c) of Article 9(4) of that Directive applies.

For the purpose of Art. 2(7)(c) of the TCO Regulation, which defines as terrorist content any material which "solicits a person or a group of persons to participate in the activities of a terrorist group", a terrorist group's activities are defined in reference to Art. 4(b) of the Directive:

> (b) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group.

Scheinin (2019) was highly critical of the EU legislator's choice to define terrorist content with reference to the Terrorism Directive. He argued that the Directive's definitions were conceived for the evidence-based adversarial process of a criminal trial and cannot serve, at the same time, for administrative decisions ordering the removal of online content. The Directive's definitions contain such elements as "intent" or "aim", or require proof

that a person had "knowledge" of the fact their participation would contribute to the criminal activities of a terrorist group. According to Scheinin (2019), whether these criteria are fulfilled in an individual case cannot be determined by reference to the text, video, or image alone, but requires a careful contextual assessment, including evidence beyond the piece of content itself. The fact that the TCO Regulation completely disregards this complexity creates significant risks for freedom of expression and information.

Similarly, Mitsilegas and Salvi (2024) shed light on the "digital exceptionalism" underlying the TCO Regulation. Their in-depth analysis demonstrates that the EU's regulatory approach to governing terrorist content online has departed from the criminalisation of illegal speech in the offline environment. The authors show that the Regulation over-criminalises online speech through broad definitions of terrorist offences and content, which risks undermining the principles of legality and proportionality. At the same time, this approach results in an increased risk of over-removal and ultimately comes at the expense of freedom of expression and information.

In practice, it is not always straightforward to determine what material falls within the Regulation's scope. Art. 1(3) of the Regulation excludes material disseminated for educational, journalistic, artistic, research, or awareness-raising purposes from its scope. In many cases, intention and context are thus determining factors. In addition, radical, polemic, or controversial views that are expressed in the context of public debate on sensitive political questions should also not be considered terrorist content (Recital 12 TCO Regulation). However, the line between a radical political statement and terrorist content may be very thin. A thorough contextual assessment is, therefore, crucial for distinguishing terrorist content from material covered by freedom of expression.

The recitals to the Regulation specify which factors should be considered when assessing whether material constitutes terrorist content: "the nature and wording of statements, the context in which the statements were made and their potential to lead to harmful consequences in respect of the security and safety of persons" (Recital 11 TCO Regulation). Furthermore, if the material was produced or disseminated by someone on the EU's list of persons, groups, and entities involved in terrorist acts and subject to restrictive measures, this should constitute an important factor in the assessment (Recital 11).

An example can demonstrate the practical difficulty of determining whether content should be removed under the TCO Regulation. As stated above, the Regulation excludes material disseminated for educational purposes from its scope. However, this exception only raises new questions: How does one determine if a text, image, or video has an educational purpose? Does this depend on the identity of the user who uploaded it (i.e., whether they are a teacher or professor)? Or does it depend on their affiliation with an educational or research institution? What about activist groups that aim to educate the public about terrorist activity? And what of anonymously uploaded material?

As this sub-section has shown, determining whether a piece of content should be removed under the TCO Regulation can be highly complex and dependent on many factors that must be established through a nuanced and contextual assessment. However, as the next section shows, the modalities of the TCO Regulation fail to address this complexity. This is especially the case where the removal of content is decided by the hosting service providers themselves using algorithmic content moderation systems.

3. Key provisions

The main innovation of the TCO Regulation is the creation of so-called removal orders (2.1). These can be internal or cross-border, meaning that they can also be addressed to hosting service providers established in different Member States or third countries (2.2). Where it has been established that hosting service providers were exposed to terrorist content, the Regulation requires them to take additional measures to prevent the dissemination of such content on their platforms (2.3). Finally, the Regulation obliges hosting service providers to publish an annual transparency report on how they are dealing with terrorist content (2.4).

3.1 Removal orders

Removal orders provide a basis for competent national authorities to compel hosting service providers to remove or disable access to terrorist content within one hour. Art. 3 of the TCO Regulation lays down the procedure to be followed.

First, the competent authority shall address the removal order to the main establishment of the hosting service provider or to its legal represen-

tative by electronic means capable of producing a written record under conditions that allow the authentication of the sender to be established and the date and time of the order specified (Art. 3(5)).

It is left to the Member States to designate the authorities empowered to issue removal orders.[5] The Regulation does not lay down any conditions that must be met in this regard, meaning that this could potentially be judicial or administrative authorities. The designated authorities range from law enforcement to specialised agencies working on organised crime or counterterrorism. Many Member States have designated multiple authorities, enabling both law enforcement and specialised administrative bodies to issue removal orders. For example, Germany designated both its Federal Criminal Police Office and the Federal Network Agency. Other countries seem to view the fight against terrorist content as a purely administrative matter. Austria, for example, only designated its Communications Authority. Depending on the Member State, the removal order is therefore not subject to any judicial review at the issuing stage.

The deadline to remove or disable access to terrorist content in all Member States is one hour after receipt of the removal order (Art. 3(3) TCO Regulation). This deadline has attracted substantial academic criticism. Following the publication of the proposed Regulation, Coche (2018) warned that the short timeframe, paired with the unclear definition of terrorist content, would "undoubtedly magnify the risks of over-removal of content" (p.12). In a detailed analysis of the origins and framework of removal orders, Rojszczak (2023) concurred, considering that the one-hour time limit "de facto eliminates the possibility of a more detailed legal analysis of a specific case" (p.17).

The hosting service providers' discretion for executing removal orders is minimal. In particular, they are not required to examine the order's admissibility but may only invoke a limited list of technical grounds to justify their non-execution. If they cannot comply with the removal order on grounds of force majeure, de facto impossibility, or if the removal order is incomplete or contains manifest errors, hosting service providers are required to inform the issuing authority of this (Art. 3(7) and (8) TCO Regulation). This information, however, only suspends the deadline, mean-

5 For an overview of the authorities that have been designated by the Member States, see the list of national competent authorities and contact points published by the European Commission (2025).

ing that the one-hour time limit begins once the grounds for non-execution have ceased to exist.

Certainly, hosting service providers that have received a removal order shall have the right to challenge it before the courts of the Member State of the issuing authority (Art. 9(1)). The Member States had to implement effective procedures for exercising this right. Nevertheless, even if a hosting service provider intends to take legal action, this does not entail a suspension of their obligation to execute the removal order.

The TCO Regulation lays down serious penalties for non-compliance (Art. 18). To this end, Member States had to adopt rules on penalties, which can be of an administrative or criminal nature. The type and level of penalty are decided on a case-by-case basis, depending on the nature, gravity, and duration of the infringement, whether the infringement was intentional or negligent, as well as the financial strength and size of the hosting service provider. If a hosting service provider systemically and persistently fails to comply with removal orders, penalties as high as 4% of their global turnover of the preceding business year can be imposed. Thus, further to the one-hour deadline, the high penalties create another incentive for hosting service providers to refrain from conducting more detailed assessments of removal orders.

Finally, hosting service providers shall make information on the removal order available to the user who uploaded the content (Art. 11). This duty entails either informing the individual of the reasons behind the removal and their rights to challenge it or providing them with a copy of the order. This obligation may be suspended when the public interest requires this information to be withheld, such as if this could threaten an ongoing criminal investigation.

3.2 Cross-border removal orders

Removal orders can be internal or cross-border in character. In other words, the issuing authority can address removal orders to hosting service providers established in their own or another Member State, or even outside the EU. As a reminder, the TCO Regulation also applies to hosting service providers that are established in third countries but offer their services in the EU. Generally speaking, the same procedure, duties, deadlines, and penalties apply as in internal cases. This subsection therefore only

highlights some differences between cross-border and internal removal orders.

For cross-border removal orders, there is an additional requirement to notify competent authorities in the Member State where the hosting service provider is established (Art. 4(1) TCO Regulation). For example, if the German Federal Network Agency wants to order the removal of terrorist content published on Instagram, which is owned by Meta Platforms Ireland, they must send a copy of the order to the Irish authorities.

This notification requirement is important because the Member State of establishment may scrutinise the validity of the removal order against the TCO Regulation and EU fundamental rights law (Art. 4(3)). In the above example, this would mean that the Irish authorities assess whether the cross-border removal order fulfilled the Regulation's conditions and respected the EU Charter of Fundamental Rights, and especially freedom of expression. This allows the authorities in the Member State of establishment to protect users from abusive removal orders. An example of such an order would be one that is not targeted at specific items of content, but aims to remove all content uploaded by a specific user. Another example could be an order that is abused to prevent activists or political dissidents from communicating with the public. If the authorities in the Member State of establishment find that the removal order infringes the Regulation or the Charter, they should adopt a reasoned opinion to that effect within 72 hours of receipt. This will cause the removal order to cease having legal effect, and the hosting service provider will have to reinstate the content and access thereto (Art. 4(7)).

For cross-border removal orders, the Regulation also foresees a more active role for hosting service providers: They may send a reasoned request to the competent national authority in their Member State to scrutinise the order as described in the previous paragraph (Article 4(4)). To return to the German example, this would mean that Instagram could contact the competent authorities in Ireland and ask them to assess the removal order received from the German Federal Network Agency. This gives hosting service providers an important role in preserving legality and respect for fundamental rights: If they suspect that a cross-border removal order raises problems, they can alert the competent authorities in their Member State, who will have to issue a reasoned decision.

This provision may become important in practice. It is to be expected that the Member States that are home to many bigger hosting service providers receive a higher number of notifications regarding such removal

orders. Ireland, for example, is the Member State of establishment of Meta and Google, two companies offering a range of services that fall into the TCO Regulation's scope. We can thus expect that the Irish authorities receive a comparatively high number of notifications. In such a scenario, hosting service providers can act as important filters. They can flag problematic orders and thereby draw the competent authority's attention to those which require further scrutiny. Nevertheless, the same concerns as for internal removal orders apply here as well: Due to the one-hour deadline and high fines that hosting service providers face for non-execution, they may not have the time or incentive to do this in practice. Ultimately, it is always safer for the service provider to immediately comply with a removal order, and thus avoid hefty fines.

3.3 Specific measures to address the dissemination of terrorist content

Beyond dealing with removal orders, the TCO Regulation requires hosting service providers that have been exposed to terrorist content to take additional measures to protect their users against such content.

This procedure is laid down in Art. 5 of the TCO Regulation and applies to hosting providers who have a history of such exposure. This is the case where a provider has received two or more removal orders in the previous 12 months. Where this is established, they shall take additional measures to address the misuse of their services (Art. 5(4)). In case of non-compliance, the same provisions regarding penalties apply as for (cross-border) removal orders (Art. 18).

Hosting service providers have broad discretion to determine the type of measures they choose to achieve this goal. As suggested by the Regulation, these measures may include appropriate technical and operational measures or capacities, but also mechanisms for users to report terrorist content or those for user moderation (Art. 5(2)). The hosting service provider may, for example, decide to hire specialised staff or invest in developing technological tools to better detect and remove terrorist content. This may include upload filters, which allow for the automatic recognition and blocking of content – a highly controversial practice that is also being debated in the context of other types of illegal content, such as child sexual abuse material or copyright infringements (see Romero Moreno, 2020).

Scholars have warned that the broad discretion afforded to hosting service providers under Art. 5 significantly enhances their role in "policing"

online content. Carrera et al (2022, p. 11) considered that the TCO Regulation thereby "assigns service providers with 'law enforcement duties' to remove, disable access to, or assess nature of online content in ways that are both reactive [...] and proactive".

The proactive measures required under Art. 5 have also prompted the question of whether the Regulation impacts the EU's system of intermediary liability. As a reminder, providers of intermediary services – including hosting services – are exempt from liability in the EU if they do not have actual knowledge of illegal activity or information on their platforms and, upon obtaining such knowledge, act expeditiously to remove or disable access to it (see Section 1.1). In this regard, Kuczerawy (2019, p. 1) observed a general shift "from liability to responsibility". She maintained that the EU is moving away from its traditional, negligence-based liability system towards proactive measures, such as those required under the TCO Regulation.

Another aspect that has been raised in this connection is the prohibition of general monitoring. As a rule, Member States may not impose a general obligation for hosting service providers to monitor the information they transmit or store, nor a general fact-finding obligation regarding illegal activity (Art. 15 e-commerce Directive; Art. 8 DSA). However, crucially, the prohibition of general monitoring is addressed to the Member States, not the service providers themselves. Hence, this does not prevent hosting service providers from undertaking such far-reaching monitoring activities voluntarily. According to Carrera et al (2022), the TCO Regulation does not exclude the use of automated tools, and thus legitimises automated filtering and content blocking as a way for hosting service providers to comply with their obligations under Art. 5. Connected to this, Frosio (2018) maintained that the introduction of proactive measures leads to a de facto delegation of enforcement duties to private actors and the algorithmic tools they use. This is particularly problematic where such tools are used to block images and videos that have been previously labelled as terrorist content without any administrative or judicial oversight.

Art. 5(1) of the TCO Regulation states that the proactive measures taken by hosting service providers should not unduly encroach on users' freedom of expression and information by over-removing material that does not constitute terrorist content. The Regulation further stresses that these measures should be applied in a diligent and non-discriminatory manner (Art. 5(3)). However, the Regulation only provides for very limited public oversight in this regard. Pursuant to Art. 5(5) of the Regulation, hosting service providers shall report to the competent authority on the specific

measures they have taken to comply with the Regulation within three months of receiving the decision and on an annual basis thereafter. Several considerations raise doubts as to the potential of these reports to provide meaningful public oversight regarding the hosting service providers' content moderation practices.

First of all, so far, the transparency reports published by hosting service providers (see Section 2.4) go into little detail as to how terrorist content is detected, removed, and blocked.[6] Of course, it should be noted that these reports are publicly accessible, while those addressed solely to the competent authorities could go into greater detail in this respect. However, it is unlikely that hosting service providers will voluntarily report more than what is strictly required by Article 5.

In addition, if hosting service providers rely on algorithmic moderation systems to fight the spread of terrorist content, they may be bound by contractual secrecy or trade secrets, which limits what they can disclose about the technology used. Curtin and Fia (forthcoming) outlined this problem regarding public authorities' use of AI systems. Secrecy may limit access to training data, algorithms, and technical documentation, which impinges on transparency and the possibility of exercising public oversight. The same concerns apply in the context of the TCO Regulation: Without comprehensive access to technical components and documentation, hosting service providers can use secrecy to shield themselves from public scrutiny regarding their content moderation practices and whether these are applied in a non-discriminatory manner.

Furthermore, competent national authorities have no vested interest in conducting thorough reviews of the preventive measures taken under Article 5. The TCO Regulation ultimately relies on the rationale that hosting service providers should internally develop and implement solutions to address the spread of terrorist content. As long as platforms remain "clean", public authorities may limit themselves to a superficial review and avoid closely examining how this is achieved.

6 In the early years of the German Network Enforcement Act, transparency reports did not meet lawmakers' expectations either, raising doubts about their effectiveness in clarifying content moderation practices. For more information, see Heldt (2019).

3.4 Transparency obligations

Finally, the TCO Regulation outlines a number of transparency obligations, which should contribute to holding hosting service providers accountable for their content moderation practices vis-à-vis their users.

First of all, hosting service providers must clearly outline their policy for addressing terrorist content in their terms and conditions (Art. 7(1) TCO Regulation). This may include an explanation of how specific measures function, as well as the potential use of automated tools.

Moreover, hosting service providers are required to publish transparency reports detailing the actions they have taken to address the dissemination of terrorist content (Art. 7(2)). These reports should include, amongst other things, information about the measures taken in relation to the identification and removal of terrorist content, as well as measures to prevent the reappearance of this material, the number of items of terrorist content removed following removal orders, and specific measures undertaken (Art. 7(3)). The reports should also specify whether the removal orders were complied with and, if not, the grounds for non-compliance. In addition, the reports should detail the number and outcome of complaints handled by the hosting service provider, decisions imposing penalties, as well as the number and outcome of administrative or judicial review proceedings brought by the hosting service provider.

As of June 2024, hosting service providers have had to publish two transparency reports: The first of which covering the period following the entry into force of the TCO Regulation in 2022, and the second covering the full year of 2023. These reports provide initial insights into the TCO Regulation's practical application.

Transparency reports from Meta and Google have indicated that the number of removal orders is still relatively low. For 2023, Meta reported 143 requests for removal orders for Facebook (Facebook Transparency Report, 2023, p. 8). Notable, in addition to the low number, is that the majority of orders were deemed not compliant with the conditions for their issuing. The report has specified that, for Facebook, only 15 requests were, in fact, valid orders issued by competent authorities. Among these, only 10 led to content being removed or access thereto being restricted in the EU. Google's transparency report paints a similar picture, stating that they received no removal orders from competent authorities under the TCO Regulation in 2023 (Google Transparency Report, 2023, p. 2).

For now, terrorist content is removed almost exclusively following the platforms' internal policy. Meta cited 6.1 million items of content removed for violating Facebook's policies on "Dangerous Organizations and Individuals", "Violence and Incitement", and "Coordinating Harm and Promoting Crime" (Facebook Transparency Report, 2023, p. 9). According to Meta, these policies are "congruent with the Regulation's definition of 'terrorist content'" (Facebook Transparency Report, 2023, p. 5). Google cited over 16.3 million items of terrorist content that were removed in 2023 (Google Transparency Report, 2023, p. 2). However, the report failed to specify how many of these would have been covered by the TCO Regulation.

Nevertheless, it would be premature to conclude that the relative underuse of removal orders suggests that the Regulation is not being applied. National authorities may require time to integrate removal orders into their practices, potentially causing delays in the implementation of the Regulation. In addition, the removal of the vast majority of content according to internal policies demonstrates the effectiveness of preventive tools used by the platforms to combat the spread of terrorist content. In this regard, both providers have stated that their content moderation relies on a combination of automated systems, human review, and user reports (Facebook Transparency Report, 2023, p. 2; Google Transparency Report, 2023, p. 1).

One might argue that, if terrorist content is removed directly by the platforms, and national authorities have no need to intervene, the TCO Regulation has achieved its goal. However, in the absence of more detailed information on what content is removed following the platforms' internal policies, and how these overlap with the Regulation's definitions, it is hard to discern whether the platforms are complying with EU rules or simply over-removing content.

4. Conclusion

By introducing legal obligations regarding how to deal with terrorist content, the TCO Regulation marked the beginning of the EU's efforts to enhance the responsibility of online platforms for the content they host and disseminate. The Regulation establishes a new set of responsibilities for hosting service providers. On the one hand, they must respond to removal orders issued by national competent authorities by taking down terrorist content within a one-hour deadline. On the other, hosting service

providers must also take preventive action. If they have been exposed to terrorist content, they must adopt specific measures to ensure that their platforms remain free of such content. The Regulation thereby fundamentally changes the enforcement landscape: Hosting service providers do not merely have to comply with legal requirements, but actively contribute to the prevention of radicalisation and, potentially, terrorist acts.

Determining whether a text, image, or video constitutes terrorist content can be highly context-dependent and technical. Traditionally, courts establish this through an evidence-based procedure, considering not only the content itself, but also contextual factors. Regrettably, the modalities of the TCO Regulation do not do justice to this complexity and create significant risks for abuse. The short deadlines and high fines, along with the fact that some Member States do not require judicial review to issue removal orders, have raised concerns regarding the over-removal of content and the associated risks to freedom of expression and information.

Moreover, the TCO Regulation legitimises, and even incentivises, the use of algorithmic moderation systems to detect and remove terrorist content. Hosting service providers are thus likely to rely on algorithmic tools and AI to comply with the Regulation's requirement to take preventive measures to stop the spread of terrorist content. In this regard, the Regulation would have provided an opportunity to assert public oversight by requiring hosting service providers to publish detailed reports on what content is removed under the Regulation and how this content was detected. Instead, the Regulation only requires them to provide minimal information on their content moderation practices, and the first transparency reports show that platforms are typically unwilling to share more than what is required in this regard. The TCO Regulation thus created a system where hosting service providers are responsible for the removal of terrorist content, but the EU Member States cannot know – or, indeed, prefer not to know – how this is done.

Even if the TCO Regulation led to hosting service providers intensifying their fight against terrorist content, whether its implementation can be termed a success would remain in doubt. While the EU's push for preventative action may have helped keep terrorist content off social media and video-sharing platforms, we seem to have gained no clarity on how this is achieved.

References

Bellanova, R. and de Goede, M. (2021) 'Co-producing security: platform content moderation and European security integration', *Journal of Common Market Law Studies,* 60(5), pp. 1–19.

Carrera, S., Mitsilegas, V., Stefan, M. and Vavoula, N. (2022) *Towards a principled level playing field for an open and secure online environment. Regulation, enforcement and oversight of online content moderation in the EU and the United Kingdom*. CEPS Task Force Report [Online]. Available at: https://cdn.ceps.eu/wp-content/uploads/2022/10/CEPS-Task-Force-Report_Online-Content-Regulation.pdf (Accessed: 27 January 2025).

'Charter of Fundamental Rights of the European Union' (2012) *Official Journal* C 326, 26 October, pp. 391-407 [Online]. Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.C_.2012.326.01.0391.01.ENG (Accessed: 27 January 2025).

Coche, E. (2018) 'Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online', *Internet Policy Review,* 7(4), pp. 1–17.

'Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online' (2018) *Official Journal* L 63, pp. 50-61, [Online]. Available at: http://data.europa.eu/eli/reco/2018/334/oj (Accessed: 27 January 2025).

'Consolidated version of the Treaty on the Functioning of the European Union' (2012) *Official Journal* C 326, 26 October, pp. 47-390 [Online]. Available at: http://data.europa.eu/eli/treaty/tfeu_2012/oj (Accessed: 27 January 2025).

'Consolidated version of the Treaty on the Functioning of the European Union Protocol (No 22) on the position of Denmark' (2012) *Official Journal* C 326, 26 October, pp. 299-303 [Online]. Available at: http://data.europa.eu/eli/treaty/tfeu_2012/pro_22/oj (Accessed: 27 January 2025).

'Consolidated version of the Treaty on the Functioning of the European Union Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice' (2016) *Official Journal* 202, 7 June, pp. 295-297, [Online]. Available at: http://data.europa.eu/eli/treaty/tfeu_2016/pro_21/oj (Accessed: 27 January 2025).

Curtin, D. and Fia, T. (forthcoming) 'Cracking Secrecy Dominance in European AI Regulation'.

De Pasquale, P. and Pesce, C. (2021) 'Article 82 (principle of mutual recognition)' in Blanke, H. and Mangiameli, S. (eds.) *Treaty on the Functioning of the European Union – a commentary: volume I: preamble, Articles 1–89*. Cham: Springer International Publishing, pp. 1559–1580.

'Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market' (2000) *Official Journal* L 178, 17 July, pp. 1-16 [Online]. Available at: http://data.europa.eu/eli/dir/2000/31/oj (Accessed: 27 January 2025).

'Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA' (2011) *Official Journal* L 335, 17 December, pp. 1-14 [Online]. Available at: http://data.europa.eu/eli/dir/2011/93/oj (Accessed: 27 January 2025).

'Directive (EU) 2017/541 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA' (2017) *Official Journal* L 88, 31 March, pp. 6-21 [Online]. Available at: http://data.europa.eu/eli/dir/2017/541/oj (Accessed: 27 January 2025).

'Directive (EU) 2018/1808 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities' (2018) *Official Journal* L 303, 28 November, pp. 69-92 [Online]. Available at: http://data.europa.eu/eli/dir/2018/1808/oj (Accessed: 27 January 2025).

European Commission (2017) Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, tackling illegal content online. Towards an enhanced responsibility of online platforms COM/2017/0555 final [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0555 (Accessed: 27 January 2025).

European Commission (2025) *List of national competent authority (authorities) and contact points*. European Commission [Online]. Available at: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en (Accessed: 31 January 2025).

Facebook (2024) *European Union terrorist content online transparency report*. Facebook [Online]. Available at: https://transparency.meta.com/sr/eu-online-report-fb-feb29-24 (Accessed: 27 January 2025).

French Constitutional Council, 'Décision n° 2020-801 DC of 18 June, 2020' (2020) *Journal Officiel de la République Française* n°0156, 25 June [Online]. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031998/ (Accessed: 27 January 2025).

Frosio, G. (2018) 'Why keep a dog and bark yourself? From intermediary liability to responsibility', *Oxford International Journal of Law and Information Technology,* 26(1), pp. 1–38.

Frosio, G. (ed.) (2020) *The Oxford handbook of online intermediary liability*. Oxford: Oxford University Press.

'Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)' BGBl. I 2017, p. 3351 [Online]. Available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html (Accessed on: 27 January 2025).

Google (2024) *Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online transparency report*. Google [Online]. Available at: https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-26_2023-1-1_2023-12-31_en_v1.pdf (Accessed: 27 January 2025).

Heldt, A., (2019) 'Reading between the lines and the numbers: an analysis of the first NetzDG reports', *Internet Policy Review*, 8(2), pp. 1–18.

Janssens, C. (2013) *The principle of mutual recognition in EU law*. Oxford: Oxford University Press.

Jørgensen, R.F. and Pedersen, A.M. (2017) 'Online service providers as human rights arbiters' in Taddeo, M. and Floridi, L. (eds.) *The responsibilities of online service providers*. Cham: Springer International Publishing, pp. 179–199.

Kuczerawy, A. (2019) 'General monitoring obligations: a new cornerstone of internet regulation in the EU?' in Centre for IT & IP Law (ed.) *Rethinking IT and IP law – celebrating 30 years CiTiP*. Antwerp: Intersentia, pp. 141–148.

'LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet (Avia Law)' (2020). *Journal Officiel de la République Française*, n°0156, p.11, 25 June [Online]. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970 (Accessed: 27 January 2025).

Mitsilegas, V. (2016) *EU criminal law after Lisbon: rights, trust and the transformation of justice in Europe*. Oxford: Hart Publishing.

Mitsilegas, V. and Salvi, C. (2024) 'Digital exceptionalism, freedom of expression and the rule of law: the case of targeting terrorist content online', *Rivista Eurojoust,* 2(2024), pp.181–205.

'Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online' (2021) *Official Journal* L 172, 17 May, pp. 79-109. [Online]. Available at: http://data.europa.eu/eli/reg/2021/784/oj (Accessed: 27 January 2025).

'Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act)' (2022) *Official Journal* L 277, 27 October, pp. 1-102, [Online]. Available at: http://data.europa.eu/eli/reg/2022/2065/oj (Accessed: 27 January 2025).

Rojszczak, M. (2023) 'Gone in 60 minutes: distribution of terrorist content and free speech in the European Union', *Democracy and Security*, 20(2), pp. 179–209.

Romero Moreno, F. (2020) 'Upload filters and human rights: implementing Article 17 of the directive on copyright in the digital single market', *International Review of Law, Computers & Technology,* 34(2), pp. 153–182.

Scheinin, M. (2019) 'The EU regulation on terrorist content: an emperor without clothes', *Verfassungsblog*. 30 January 2019 [Online]. Available at: https://verfassungsblog.de/the-eu-regulation-on-terrorist-content-an-emperor-without-clothes/ (Accessed: 27 January 2025).

Tosza, S. (2021) 'Internet service providers as law enforcers and adjudicators. A public role of private actors', *Computer Law & Security Review,* 43, pp. 1–17.

Wilman, F. (2020) *The responsibility of online intermediaries for illegal user content in the EU and the US*. Cheltenham: Edward Elgar Publishing.