

Combating the dissemination of terrorist content online: authorities, obligations and sanctions

abreuadvogados.com



1. Object and scope of application:

Decree-Law no. 25/2026 ("**DL 25/2026**"), was published on 28 January 2026, which ensures the implementation, in the national legal system, of Regulation (EU) 2021/784, of the European Parliament and of the Council, of 29 April 2021, on combating the dissemination of terrorist content online ("**Regulation 2021/784**").

Regulation (EU) 2021/784 aims to ensure the proper functioning of the Digital Single Market, prevent radicalisation of society and combat the misuse of hosting services for terrorist purposes.

In this context, DL 25/2026 aims, in particular:

- Designate the competent national authorities to issue and review suppression orders, supervise and enforce targeted measures, and impose sanctions;
- Establish the sanctioning regime applicable to non-compliance with the obligations provided for in Regulation 2021/784;
- To make legislative changes to the related diplomas, to ensure the coherence of the regime for combating the dissemination of terrorist content online in the national legal system.

The diploma applies to providers of virtual hosting services that offer their services in the European Union, regardless of their main establishment, as well as to content providers, to the extent of the obligations directly attributable to them under Regulation 2021/784.

2. Competent authorities and their respective competences:

For the purposes of Article 12 of Regulation (EU) 2021/784, DL 25/2026 designates the following entities as competent authorities:

a) Judiciary Police ("PJ")

It is incumbent upon the PJ:

- (c)issue orders to remove or block terrorist content online pursuant to Article 3 of Regulation 2021/784, acting as a national contact point;
- Examine and enforce deletion decisions issued by competent authorities in other Member States.

The suppression or blocking decisions issued by the PJ are subject to judicial validation, through the intervention of the Public Prosecutor's Office at the Central Department of Investigation and Criminal Action ("DCIAP") and a decision of the Criminal Investigation Judge ("JIC"), within a maximum period of 48 hours, under penalty of forfeiture of the suppression or blocking decision.

b) National Communications Authority ("ANACOM")

ANACOM is responsible for:

- Supervise the application of the specific measures adopted by virtual hosting service providers, and the fulfilment of other obligations provided for in the Regulation whose non-compliance constitutes an administrative offence;
- Initiate and instruct administrative offence proceedings, as well as apply the respective fines and sanctions.

Judicial decisions upholding the case can be appealed to the Court of Appeal, while ANACOM's sanctioning decisions may be appealed to the Court of Competition, Regulation and Supervision, both with a purely devolutive effect. In other words, the decision can be enforced during the appeal process, without prejudice to the higher court's ruling if it differs, which can impact actions taken in the meantime under the initial decision.

3. Sanctioning regime:

DL 25/2026 establishes a specific sanctioning regime for non-compliance with the obligations provided for in Regulation 2021/784, qualifying infractions as serious or very serious administrative offences, depending on their nature.

The following constitute administrative offences:

- Failure to comply with the obligation to remove or block terrorist content within one hour;
- Failure to comply with cross-border suppression orders or decisions to restore or unblock content;
- The failure to adopt specific and necessary measures to mitigate the dissemination of terrorist content;
- Failure to comply with obligations to retain content and related data, transparency and cooperation with authorities;
- The lack of designation of contact points and legal representatives in the European Union, where applicable.

Fines vary depending on the seriousness of the infringement and the size of the offender, and may reach, in the case of large companies, amounts of up to € 5,000,500, without prejudice to the fact that, in the event of recurrence of particularly serious infringements, a maximum limit corresponding to 4% of the service provider's annual global turnover is applied.

Attempt and negligence are always punishable, with the minimum and maximum limits of the fine being halved.

4. Relevant legislative changes:

To ensure the effective application of Regulation 2021/784, DL 25/2026 also amends several structuring diplomas, namely:

- Law No. 99/2009, of 4 September 2009 (framework regime for administrative offences in the communications sector), expressly integrating the new sanctioning regime;
- Law No. 62/2013, of 26 August 2013 (Organization of the Judicial System), clarifying jurisdictional competences;
- Regulatory Decree No. 2/2016, of 23 August, on the organization and operation of the Anti-Terrorism Coordination Unit;
- Law no. 68/2019, of 27 August (Statute of the Public Prosecutor's Office), reinforcing the role of the DCIAP in the assessment of suppression or blocking decisions issued by the PJ.

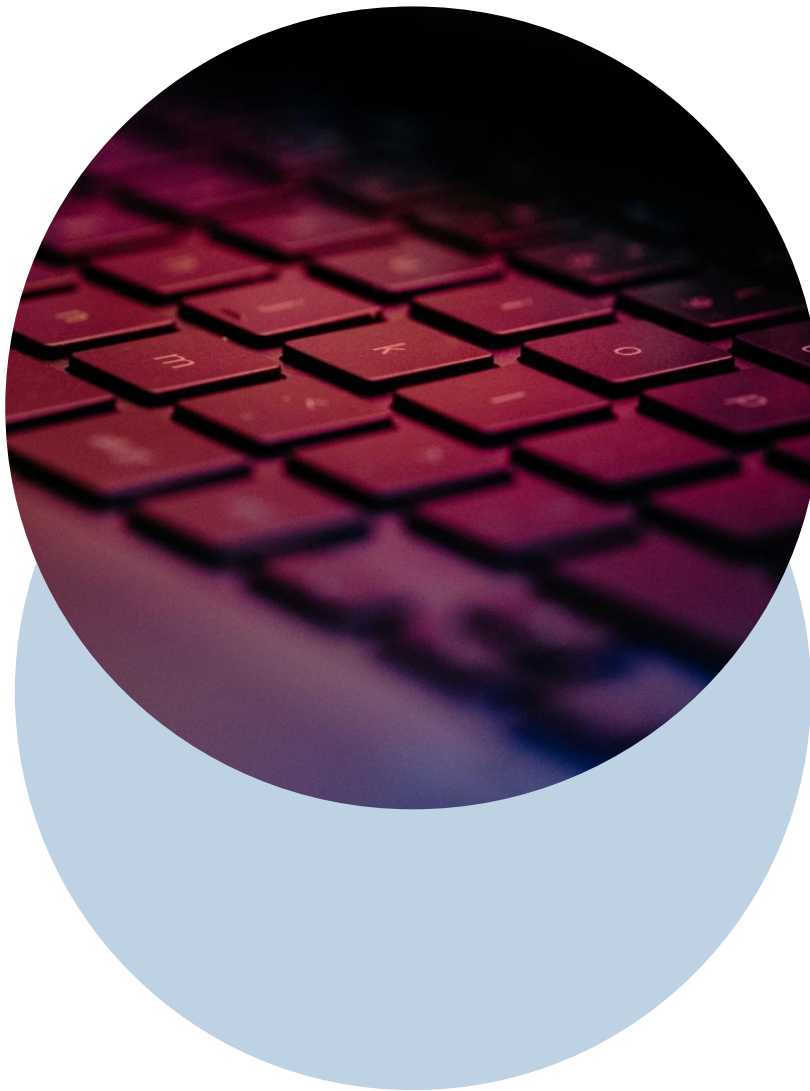
These amendments aim to ensure institutional coherence and coordination between administrative, police and judicial authorities and effectiveness in the national response to the dissemination of terrorist content online.

5. Next steps:

Covered entities must:

- Assess the impact of DL 25/2026 and adapt its internal procedures for responding to decisions to suppress or block content;
- Ensure that there are contact points and, where applicable, legal representatives in the European Union;
- Implement or update specific measures to mitigate the dissemination of terrorist content;
- Promote the training of employees involved in content moderation and the review of internal policies and terms and conditions, to ensure compliance with the Regulation.

DL 25/2026 enters into force on March 29, 2026, 60 days after its publication, thus requiring timely preparation to ensure compliance with the new sanctioning and institutional framework.



Thinking about tomorrow? Let's talk today.

António Andrade – Partner

antonio.andrade@abreuadvogados.com

Manuel Durães Rocha – Partner

manuel.d.rocha@abreuadvogados.com

Ricardo Henriques – Partner

ricardo.henriques@abreuadvogados.com