FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

REGULATING ONLINE TERRORIST CONTENT

BALANCING PUBLIC SAFETY AND FUNDAMENTAL RIGHTS

REPORT

Contents

Foreword

List of promising practices

Key findings and FRA opinions

Ensure clarity of the definition of terrorist content and the foreseeability of its application

FRA opinion 1

FRA opinion 2

FRA opinion 3

Avoid incentivising HSPs to over-remove content

FRA opinion 4

FRA opinion 5

Avoid discriminatory impact on particular groups

FRA opinion 6

Enhance the transparency of the use of the regulation

FRA opinion 7

Strengthen the effectiveness of the regulation in line with the proportionality principle

FRA opinion 8

FRA opinion 9

Increase the effectiveness of safeguards and remedies

FRA opinion 10

FRA opinion 11

Support the application of the regulation in line with fundamental rights through further guidance, training and awareness-raising

FRA opinion 12

Introduction

Legislative and policy context of addressing terrorist content online

International and regional law and standards

European Union law and policy

Addressing terrorist content online and fundamental rights

Methodology and scope

1. Defining terrorist content online

1.1 Suitability and legal clarity of the definition of online terrorist content

1.2 Bodies interpreting the definition: independence, expertise and oversight

1.3 Content disseminated for recognised legitimate purposes

2. Removal orders and referrals

2.1 Impact of removal orders on content providers and HSPs

2.1.1 Mandatory prompt removal of content

2.1.2 Risk of erroneous assessment of content

2.1.3 Uneven use of removal orders for different types of terrorism

2.1.4 Impact of removal orders on HSPs, including small enterprises and microenterprises, and their freedom to conduct a business

2.2. Referrals and their interplay with removal orders

2.2.1 Lack of clarity, foreseeability and transparency in the use of referrals and removal orders

2.2.2 Impact of removal orders on the voluntary nature of referrals

2.2.3 The differential treatment of HSPs

3. The regulation and HSP content moderation

3.1 Fundamental rights impact of HSP content moderation policies

3.1.1 Risk of over-blocking due to reliance on automated tools

3.1.2 Limitations of HSP human moderation

3.1.3 Disproportionate impact of HSP content moderation on certain types of content and particular groups

3.1.4 HSP transparency reporting as a missed opportunity

3.2 Challenges related to specific measures

3.2.1 Lack of clarity when an HSP is exposed to terrorist content

3.2.2 Specific measures as an incentive to use intrusive tools

3.2.3 Effectiveness of internal complaint mechanisms of HSPs

4. Selected safeguards and remedies

4.1 Effective scrutiny of cross-border removal orders

4.2 Practical obstacles to accessing remedies

4.3 Limited incentives to seek a remedy

Conclusion

Annex: Methodology

Acronyms and Abbreviations

Endnotes

Foreword

Terrorist content online presents a key threat to fundamental rights, democracy and the rule of law. The EU's legislative and other efforts to address such content and prevent terrorism, therefore, also serve to protect rights.

At the same time, such measures and their practical application to counter online terrorism must avoid overreaching with respect to legitimate content that is not terrorist in nature. This is important for the protection of a range of rights, from freedom of expression to prohibition of discrimination, which serves to ensure the legitimacy of these important efforts.

This report examines the EU's key legal instrument in this field, Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. It looks at how the regulation and its application in practice impacts fundamental rights, drawing on the experience of over 60 experts. These include practitioners from law enforcement, counterterrorism, regulatory and other authorities working with the regulation, staff of companies providing online hosting services that the regulation addresses, and civil-society and academic experts with technical knowledge on the topic.

The results provide valuable insights into how these practitioners and experts experience the practical application of the regulation and where – based on their knowledge and expertise – they see particular challenges with regard to fundamental rights. At the same time, the report identifies specific practices that support the application of the regulation – and which address the proliferation of terrorist content online more broadly – in a manner that helps overcome some of these issues and better safeguards fundamental rights.

As the regulation became applicable in 2022, its application is necessarily still evolving. In this regard, the evidence contained in this report can be used to address the identified challenges, foster a common interpretation of the regulation, its obligations and applicable safeguards, and promote an effective framework for addressing the proliferation of online terrorist content in full respect of fundamental rights.

Sirpa Rautio
Director

List of promising practices

- Aligning the interpretation of the regulation among competent authorities through regular workshops, Section 1.1
- Implementing external oversight when issuing removal orders, Section 1.2
- Additional measures to safeguard media independence, Section 1.3
- Supporting HSPs through terrorist content online capacity-building projects, Section 2.1.4
- Supporting transparency through enhanced reporting, Section 2.2.1
- Systematically monitoring the impact of own content moderation policies on removals and complaints, Section 3.1.4
- Providing additional information on specific measures to HSPs at the national level, Section 3.2.1
- Integrating information on remedies into PERCI, Section 4.2

Key findings and FRA opinions

Terrorist content online presents a key threat to fundamental rights, democracy and the rule of law. The EU's legislative and other efforts to address such content can serve to underpin fundamental rights and the prevention of terrorism.

This report presents the findings of the European Union Agency for Fundamental Rights (FRA) on the impact on fundamental rights of the application of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, as the key EU instrument in this field.

Terrorist content proliferates in the online environment alongside hybrid threats, disinformation and other security threats. It can manifest itself in a variety of ways, ranging, for example, from propaganda materials published directly by terrorist organisations on their websites, to footage of terrorist attacks disseminated on online platforms, to social media posts inciting the commission of terrorist offences. The dissemination of such content poses significant security risks and can impact fundamental rights, including the right to life and human dignity – to name just two.

In an effort to support the fight against terrorism, the findings in this report – based on the experiences of practitioners and other experts working with the regulation – can be used to enhance the regulation's application, where needed.

While the analysis contained in the report focuses specifically on the application of the regulation in practice, its findings also contribute to discussions on the broader challenges of regulating freedom of expression online beyond the context of terrorist content.

The regulation provides national competent authorities, such as law enforcement agencies and media regulatory bodies, with the possibility to order social media platforms and other hosting service providers (HSPs) anywhere in the EU – including HSPs located outside the EU but providing services within its territory – to promptly remove content disseminated to the public on their platforms, which authorities consider to amount to terrorist content. Furthermore, HSPs considered to be exposed to terrorist content can be ordered to adopt specific measures to counter this exposure. In doing so, it complements existing voluntary cooperation between authorities and HSPs, such as the EU Internet Forum and the Code of Conduct on Countering Illegal Hate Speech Online, with a set of enforceable tools. The EU Platform on Illicit Content Online (PERCI), established by the European Union Agency for Law Enforcement Cooperation (Europol), supports EU Member States in applying the regulation.

The regulation recognises the need to respect fundamental rights when implementing its provisions. Specifically, Article 23 requires the European Commission to assess the regulation's impact on fundamental rights. The Commission requested FRA carry out research in connection with this assessment.

A broader EU legislative framework for dealing with online terrorist content

The EU has a broad legal framework in place dealing with online content, some of which is of direct relevance to terrorist content and the application of the regulation. Notably, the Digital Services Act (DSA) establishes harmonised rules preventing illegal and harmful activities online, also encompassing terrorist content. The Audiovisual Media Services Directive requires Member States to ensure that video-sharing platforms do not disseminate content inciting terrorism. The main EU criminal law instrument in the field of counterterrorism, Directive (EU) 2017/541 on combating terrorism, criminalises a variety of activities that can be committed both online and offline, notably public provocation to commit a terrorist offence, and requires Member States to ensure the prompt removal of content constituting this offence. FRA issued a report on the fundamental rights implications of Directive (EU) 2017/541 in 2021.

This report presents the main findings from FRA's research, which can serve to support the evaluation of the regulation, and offers FRA's own independent assessment and conclusions. It provides insights into the experiences of practitioners and other experts with in-depth knowledge in this field, with the practical application of the provisions of the regulation at the national level. These empirical findings confirm that while the regulation serves an important and legitimate goal, it also affects a wide range of fundamental rights and freedoms that the European Union Charter of Fundamental Rights (the Charter) and international human rights instruments safeguard. In this respect, it speaks to some of the concerns expressed by national and EU stakeholders, international human rights bodies, civil-society organisations, professional associations, academics and HSPs in relation to the draft regulation when it was proposed in 2018.

Rights of the Charter that it most directly affects include freedom of expression and information (Article 11), the right to respect for private and family life (Article 7), protection of personal data (Article 8), freedom of thought, conscience and religion (Article 10), freedom of assembly and of association (Article 12), freedom of the arts and sciences (Article 13), freedom to conduct a business (Article 16), non-discrimination, including on the grounds of ethnic origin, religion or belief (Article 21) and the right to an effective remedy and to a fair trial (Article 47).

This set of findings draws from interviews with 62 experts, including practitioners from selected competent authorities who are involved in applying the regulation, ranging from law enforcement and counterterrorism agencies to regulatory bodies, and experts from HSPs affected by the regulation and civil-society and academic experts focusing on the topic. Limited desk research in 27 Member States supported the fieldwork, collecting basic information about the legal and institutional framework supporting the application of the regulation at the national level.

Combating terrorist content while respecting fundamental rights is a complex and challenging task. Findings from FRA's research show that competent authorities applying the regulation are generally aware of the potential fundamental rights impact of their work and undertake efforts to target only content that is clearly terrorist content in its nature.

Still, a number of challenges emerge as regards the impact that applying the regulation has on

fundamental rights, as the findings show. The report brings the findings to the attention of the EU institutions and Member States and can help them assess the need for further steps to ensure that the application of the regulation complies fully with fundamental rights.

As the fieldwork interviews covered authorities in a limited number of Member States, alongside selected HSPs and other experts, the findings do not claim to be representative of the situation in the EU or for HSPs as a whole. In addition, with the regulation applicable since July 2022, the degree of its use varies across the EU, which limits practical experience with some of its key elements. Nevertheless, the results provide a valuable insight into how experts who apply the regulation in their work, or are directly affected by its application, experience its impact on fundamental rights.

Ensure clarity of the definition of terrorist content and the foreseeability of its application

Article 2(7) of the regulation defines terrorist content by means of its relationship with one of the terrorist offences established under Directive (EU) 2017/541 on combating terrorism, such as content soliciting, inciting or threatening to commit one of these offences. Article 1(4) states that the regulation shall apply without prejudice to freedom of expression and information, including freedom and pluralism of the media, under Article 11 of the Charter. In addition, Article 1(3) in conjunction with Recital 12 stipulates that content disseminated for educational, journalistic, artistic, research or counterterrorism purposes, and material expressing polemic or controversial views in the public debate, will not be considered terrorist content.

Interviewees express concern that the definition of terrorist content provided by the regulation, which determines the scope of application of the instrument as a whole, does not offer sufficient clarity as to what content can be considered terrorist content and liable to removal. This can hamper the uniform application of the regulation across the EU and, in relation to different types of terrorist content (see FRA opinion 8), reduce foreseeability and result in risks for the freedom of expression and information and a variety of other rights, as content that is not terrorist content in its nature could be removed. This is further compounded by the diversity of authorities across the EU that use the definition when applying the different provisions of the regulation. While these authorities play a key role in ensuring a fundamental-rights-compliant application of the regulation, they are seldom judicial bodies and are equipped with a different degree of fundamental rights expertise and resources.

Findings show that the inclusion of ‘glorification’ in the definition of material inciting a terrorist offence, one of the types of terrorist content, poses a particular challenge for competent authorities to establish a clear line between terrorist content and permissible forms of expression, which may in some cases include expressing radical or controversial views. Although competent authorities focus their efforts on capturing content that is clearly terrorist content in nature, encompassing the concept of glorification – rather than focusing on direct incitement to commit a terrorist offence – increases the risk of overreaching to legitimate content, including political

opinions.

There is still limited experience with cases of educational, journalistic, artistic or research-related content, and specific safeguards have been implemented in some Member States to avoid such content being subject to removal. However, interviewees express concerns that reporting or research on particular conflicts or events that involve terrorist groups or trigger polarised public debate might be impacted.

FRA opinion 1

The Commission should consider reviewing the definition of terrorist content, such as the reference to 'glorification', and providing further clarity. This would facilitate its use by competent authorities, strengthen the foreseeability of the application of the regulation for HSPs and users of their services and help provide for a comparable level of fundamental rights safeguards across the EU.

FRA opinion 2

The Commission and Europol should, within their respective mandates, continue to facilitate discussions, promote exchange of experience and provide technical support to Member State authorities to support uniform application of the regulation, including a common, fundamental-rights-compliant interpretation of the definition of terrorist content.

FRA opinion 3

Member States should ensure that competent authorities are well-equipped to interpret the definition of terrorist content when applying the different provisions of the regulation in a manner that safeguards fundamental rights and they have sufficient resources for their tasks, including by making available guidance and training where needed.

Avoid incentivising HSPs to over-remove content

Removal of online content affects freedom of expression and information (Article 11 of the Charter) and can affect a broader range of other fundamental rights, including freedom of thought, conscience and religion (Article 10 of the Charter), freedom of assembly and of association (Article 12 of the Charter), freedom of the arts and sciences (Article 13 of the Charter) and non-discrimination (Article 21 of the Charter).

According to Article 3 of the regulation, competent authorities can issue removal orders which require HSPs to remove, or disable access to, terrorist content in all Member States within one hour. When receiving a removal order, the regulation does not envisage HSPs reviewing whether

the content indeed constitutes terrorist content or granting them a possibility to contest the removal order prior to its execution. Together with a risk of penalties for non-compliance, this may incentivise HSPs to take down content even if they consider the assessment of the competent authority to be erroneous. FRA's findings show that particularly smaller HSPs or those without particular fundamental rights expertise are likely to fully defer to the expertise of the authorities. While interviewees across all professional groups acknowledge the need for speedy takedowns of content posing a particular risk, some question whether the same urgency applies to all types of content falling within the scope of the regulation and the impact this may have on the rights of HSPs and users whose content may be subject to removal (content providers).

In addition, many competent authorities continue to prefer the use of referrals. The regulation (Recital 40) does not preclude the Member States from using referrals as a tool for voluntary cooperation by which national law enforcement or counterterrorism authorities (and Europol) inform HSPs about potential terrorist content detected on their platforms, allowing HSPs to review it based on their terms and conditions. Findings show that competent authorities often consider referrals more practical and agile than removal orders. However, interviewees express concerns over the interplay between the use of removal orders and referrals, stating that the regulation does not sufficiently clarify the relationship between the two tools and differentiate as to when removal orders and referrals, respectively, should be used. Namely, interviewees note that the prospect of receiving a removal order might incentivise some HSPs to remove content based on a referral without a meaningful assessment. At the same time, referrals are not accompanied by the safeguards envisaged by the regulation for removal orders and their use may raise questions of accountability of public authorities and private players for removing content.

Under Article 5, competent authorities can designate HSPs that have received two removal orders within the last 12 months as 'exposed to terrorist content' and oblige them to implement 'specific measures' (such as additional technical means to identify and remove content) to counter such exposure. When putting in place such specific measures, Article 5(3) in conjunction with Recital 23 requires HSPs to ensure that users' fundamental rights, in particular freedom of expression and information, respect for private life and protection of personal data and the right to non-discrimination, are preserved.

Yet, FRA findings show that the prospect of being designated as 'exposed to terrorist content' can increase the risk that HSPs over-moderate legitimate content to pre-empt such designation. Furthermore, once ordered to implement specific measures, the requirement to more effectively combat the presence of terrorist content on their platforms may motivate HSPs to employ further restrictive policies and intrusive tools, potentially resulting in the over-blocking of legitimate content and the general monitoring of content on their platforms. At the same time, while competent authorities are obliged to undertake a review of the application of specific measures by HSPs to ensure that they comply with all the requirements under the regulation, including the one under Article 5(3), FRA's findings show that competent authorities would need more guidance about how to assess such an impact.

FRA opinion 4

The Commission could consider adjusting the mechanism for using and processing removal orders envisaged in the regulation. Namely, where a duly justified concern exists that the content does not meet the definition of terrorist content, the regulation should provide HSPs with an effective possibility to challenge the removal order before removing the content.

Furthermore, the Commission should clarify which situations and types of content justify the use of, respectively, removal orders and referrals, to increase legal clarity and foreseeability and give full effect to the safeguards envisaged by the regulation.

FRA opinion 5

The Commission should issue guidance to HSPs and Member States on how to implement specific measures in a manner that respects fundamental rights, including that such measures do not result in general monitoring of online content. To this end, the Commission could consider providing a more concrete list of available specific measures in the regulation. Member States should ensure that competent authorities have effective systems in place to monitor specific measures implemented by HSPs, and that such monitoring pays due attention to the impact of the measures on fundamental rights, such as freedom of expression and non-discrimination. Appropriate guidance and training should be made available to relevant competent authorities, ensuring that they are equipped with sufficient expertise and knowledge when it comes to assessing the impact of specific measures on fundamental rights.

Avoid discriminatory impact on particular groups

In line with Article 21 of the Charter, Recital 10 prohibits any discrimination when applying the regulation. This prohibition applies both to authorities issuing removal orders and to HSPs when they apply specific measures pursuant to Article 5. More broadly, the DSA contains a general requirement for HSPs to act with due regard to fundamental rights of the recipients of their services (Article 14 DSA) and an obligation for those HSPs which are very-large online platforms or very-large online search engines to assess the risk of discrimination, including when using algorithmic systems (Article 34 DSA).

Findings show that detection by competent authorities and content moderation by HSPs focuses predominantly on jihadist content, which is considered a key security threat in the EU. At the same time, content related to particular topics such as sensitive current political issues, or in particular languages, is challenging to correctly assess. Together with the clarity issues associated with the definition of terrorist content, these factors increase the risk of removal of legitimate content that disproportionately impacts content providers based on their ethnic origin, language, religion or belief, or political opinion, amounting to discrimination. According to the research, Muslims and Arabic speakers are at heightened risk.

HSP content moderation, driven partly by regulatory pressures, including the regulation and other EU and national laws, relies increasingly on automated tools despite persisting concerns over their reliability. FRA's findings show that this is not necessarily compensated for by sufficiently robust human oversight, as human review of content flagged by automated tools can be limited due to factors such as time constraints, language expertise and inadequate working conditions of content moderators. This can impact a wide range of rights of online users, including the right to non-discrimination.

Furthermore, interviewees express concern that the sense of over-moderation of content - particularly in the case of HSPs' own online content moderation measures - may lead people from affected communities – and beyond – to abstain from exercising their rights online due to a fear of becoming persons of interest for counterterrorism authorities or having their profile and channels of communication blocked by HSPs. Such a chilling effect can affect very large numbers of people and extend from freedom of expression and information to other rights, such as freedom of assembly and association. Reports by international organisations and bodies acknowledge the risk of a 'chilling effect' on rights in the context of counterterrorism measures.

FRA opinion 6

Member States should ensure that competent authorities applying the regulation are adequately equipped to carry out their tasks in a manner fully consistent with the prohibition of discrimination. Appropriate guidance and training should be made available, ensuring that language or association with a particular religion do not play a disproportionate role when deciding on the terrorist nature of online content. In this context, Member States should consider regularly reviewing the removal orders and referrals, as appropriate, issued by their competent authorities to detect any risk of discrimination. The European Commission could assist Member States in this regard by issuing guidance supporting a harmonised approach.

Furthermore, the European Commission should, including in the context of enforcing other applicable EU legislation, take measures to ensure that HSPs effectively safeguard the right to non-discrimination while diligently performing their online content moderation obligations to counter online terrorism.

Enhance the transparency of the use of the regulation

Articles 7 and 8 in the regulation, respectively, stipulate transparency obligations of HSPs and competent authorities, including publishing annual transparency reports. The transparent provision of information can enhance accountability, identify the risk of over-removal of content and is essential for the evaluation of the regulation's impact on fundamental rights.

FRA's findings show that the information provided in these reports varies in quality and scope. The transparency obligation of Member States under Article 8 includes only basic information about removal orders and none about referrals, limiting their information value. Transparency

reports by HSPs lack granularity and data comparability across the industry due to issues such as the use of different definitions of terrorist content, lack of reporting on referrals and disaggregation by categories such as region or language. As a result, transparency reports do not provide the information needed to detect potential risks to fundamental rights stemming from the application of the regulation and broader HSP content moderation policies.

FRA opinion 7

The Commission could consider strengthening the transparency requirements under the regulation with respect to competent authorities, ensuring in particular that the use of referrals is covered by the reporting obligation to reflect their important interplay with removal orders. This could be further supported by making publicly available statistical data about the use of PERCI, managed by Europol, for example as regards the types of terrorist content targeted by competent authorities.

The Commission could consider strengthening the transparency requirements under the regulation with respect to HSPs, ensuring sufficient granularity and comparability of reported data. This could entail using clear and harmonised categories among HSPs when it comes to what content is reported as terrorist content, distinguishing between content detected by HSPs and content flagged by authorities (referrals), and reporting data in a disaggregated manner (including separate data for the EU).

Strengthen the effectiveness of the regulation in line with the proportionality principle

Article 52(1) of the Charter requires that limitations of fundamental rights are necessary and proportionate to the objectives pursued. While the regulation pursues a legitimate goal of addressing the dissemination of terrorist content online, interviewees express concern over its impact on fundamental rights, considering factors that limit its effectiveness in achieving this objective.

FRA's findings show that a variety of factors result in a situation where competent authorities issue removal orders to a limited number of HSPs, not necessarily reflecting the spread of terrorist content across the online environment. This includes factors related to the conduct of certain HSPs, such as their lack of cooperation with competent authorities or the failure to designate legal representatives, pursuant to Article 17, of those HSPs that offer services within the EU but are established elsewhere. Other factors relate to the capacities of some competent authorities, including gaps in the mapping of HSPs in their jurisdiction and limited resources. This reduces effectiveness and at the same time places an undue burden on some HSPs. Furthermore, findings show that, despite awareness-raising and capacity-building efforts supported by the Commission, there is still limited awareness of the regulation, especially among smaller HSPs, and that HSP efforts to comply with EU law in the field of online content focus predominantly on

compliance with the more extensive due diligence and transparency reporting requirements of the DSA.

The fact that the vast majority of removal orders focus on jihadist content reflects that this type of terrorism is considered a key security threat in the EU, but – as interviews noted – also shows a possible imbalance with respect to the amount of content related to other types of terrorism and the threat it poses, in particular when it comes to right-wing terrorist content which has been a growing concern for counterterrorism experts. In this context, interviewees report challenges in applying the regulation to right-wing content. Findings show that this phenomenon is not limited to competent authorities, as HSP content moderation frequently pays limited attention to right-wing terrorist content.

Tackling these gaps in effectively and comprehensively addressing the dissemination of terrorist content online is also important from the perspective of necessity and proportionality, considering the impact the application of the regulation can have on a variety of fundamental rights guaranteed by the Charter. This should be considered in conjunction with other concerns identified in the research and outlined in other key findings of this report, such as the risks stemming from the broad definition of terrorist content, the application of the one-hour rule, the threshold for designating HSPs as exposed to terrorist content after only two removal orders or the potential disproportionate impact on the freedom of expression and other rights as a result of implementing specific measures.

FRA opinion 8

The Commission should take stock of the application of the regulation so far with respect to different types of terrorism, such as jihadist and right-wing terrorism, and consider providing guidance on its applicability in this respect. It could also support Member States in the mapping of HSPs within their jurisdictions, to ensure that competent authorities are aware of relevant HSPs beyond those that are very well known. Member States should take steps to ensure that when detecting terrorist content and issuing removal orders, due attention is given to all relevant HSPs and to all types of terrorism, including, notably, by strengthening the focus on right-wing terrorist content. Europol could support competent authorities of the Member States in this regard. Member States should ensure that competent authorities are equipped for this purpose, including having the necessary human and financial resources.

FRA opinion 9

The Commission, Member States and Europol should, within their respective mandates, consider measures to better enforce the obligation under Article 17 to designate a legal representative for all HSPs covered by the regulation that do not have their main establishment in the EU. The Commission and Member States could further promote awareness of the regulation among HSPs and the obligations stemming from it, including the interplay with other EU law that applies to

HSPs in the area of regulating illegal content online, such as the DSA.

Increase the effectiveness of safeguards and remedies

Article 47 of the Charter guarantees the right to an effective remedy. The regulation contains several mechanisms in this regard, including the possibility to challenge removal orders and other decisions in court (Article 9), and to have removal orders issued by competent authorities of another Member State scrutinised by an authority of the Member State where the HSP is established (Article 4, in conjunction with Article 12(1)(b)). It also requires HSPs to have in place complaint mechanisms for content providers (Article 10).

FRA's findings reveal several limitations and concerns related to the effectiveness of these important safeguards. This includes insufficient clarity concerning when to scrutinise cross-border removal orders and which criteria to apply, along with the risk that scrutinising competent authorities overly rely on the expertise and assessment of the issuing competent authority, potentially rendering such scrutiny ineffective.

Concerning the possibility of seeking judicial remedy against the removal of content, the research shows that incentives to do so may be low due to the time-sensitive nature of online content and its loss of relevance, especially if it relates to current events. Furthermore, while HSPs may not be motivated to challenge the decision of competent authorities, content providers might be prevented from doing so by the complexity of initiating proceedings in another Member State than their own. In some cases, content providers might also not be properly informed in the first place about the removal of their content by the HSP (something that the regulation permits only in cases where the competent authority prohibits such disclosure, for a limited time, due to reasons of public security). In this regard, processes established in some Member States to provide a degree of oversight over the issuing of removal orders, such as by involving external bodies in approving the removal order, can act as a safeguard, provided that the body that carries out such external oversight possesses sufficient expertise, capacity and independence.

The accessibility and effectiveness of complaint mechanisms set up by HSPs may likewise be limited by factors such as the inadequate provision of information to content providers about the removal of their content, or the employment of automated tools in dealing with complaints without effective human oversight.

Finally, given the gradual application of the regulation by Member States, these safeguards have been used to a limited degree so far and, in the case of the possibility to challenge removal orders in court, not at all. Bearing in mind the importance of access to an effective remedy for safeguarding all fundamental rights affected by the regulation, this renders it difficult to objectively assess the full impact of the regulation on fundamental rights and the functioning and effectiveness of its safeguards as envisaged in Article 23. To this end, the findings in this report – based on interviews with experts – offer a good basis from which to mitigate upstream any fundamental rights concerns.

FRA opinion 10

All Member States should effectively implement Article 4, in conjunction with Article 12(1)(b), as a key safeguard under the regulation in case of cross-border removal orders. They should provide clear guidance to the competent authorities as regards the application of the scrutiny of such removal orders, ensuring that it is conducted systematically and in a comprehensive and objective manner.

FRA opinion 11

The Commission could consider enhancing the accessibility of remedies for content providers by making it obligatory for HSPs to inform content providers of the reasons for the removal and their rights to challenge the removal order, without the need for content providers to request such information. This is without prejudice to the exception for reasons of public security envisaged in Article 11(3).

Furthermore, Member States could consider steps to ensure effective oversight in the course of issuing removal orders. This would offer an additional safeguard, given that once content has been removed, the effectiveness of existing remedies appears to be limited in practice.

Finally, the Commission should consider conducting an evaluation of the regulation once all of its main elements have been used in practice to a sufficient degree. This is, in particular, the case of access to remedies pursuant to Article 9, which needs to be a central element of any evaluation of the regulation's fundamental rights impact.

Support the application of the regulation in line with fundamental rights through further guidance, training and awareness-raising

The regulation aims to contribute to the protection of public security by addressing the proliferation of terrorist content online in a manner that respects fundamental rights and contains a set of safeguards to this end.

As a horizontal finding common to several thematic findings in this report (see notably Opinions 2, 3, 5, 6 and 9), the research points to a number of areas where the application and interpretation of the regulation vary, both among competent authorities and among HSPs, with potential implications for its effective enforcement as well as for the level of protection of fundamental rights.

This report highlights a number of existing initiatives and practices at the EU and Member State levels that aim to support the application of the regulation in a manner that helps safeguard fundamental rights, including through the provision of additional guidance and training, exchange of experience and awareness-raising. Further enhancing these efforts would be an important step supporting a uniform application of the regulation in line with fundamental rights.

FRA opinion 12

The Commission and Member States should, based on their respective spheres of competence, support the application of the regulation by providing appropriate guidance and training to the staff of competent authorities, as well as by enhancing the awareness about the regulation and its relevant provisions and applicable obligations among HSPs. These should be based on evidence indicating the main challenges in the application of the regulation, drawing upon relevant sources of expertise – including fundamental rights – and building upon existing initiatives where appropriate.

Introduction

By greatly facilitating the dissemination of information and ideas, the online environment amplifies freedom of expression and the enjoyment of numerous other rights. At the same time, it can be abused to spread various types of illegal content. Material promoting terrorism and terrorist groups – ranging from footage of terrorist attacks and manifestoes of their perpetrators going viral to websites of terrorist organisations hosting troves of propaganda material – poses a particular risk in this regard. The 2019 Christchurch terrorist attack, which was internationally streamed on social media platforms and has inspired numerous other attackers since, is a case in point.

Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online (the regulation) was adopted to complement voluntary cooperation mechanisms between the EU, national authorities and companies providing online hosting services. To this end, it provides authorities with enforceable tools, notably the possibility to order such hosting service providers (HSPs) to expeditiously remove content considered to be terrorist content and to implement measures to protect their platforms against the proliferation of such content. As sectoral legislation dedicated exclusively to tackling terrorist content, the regulation complements the EU Digital Services Act (DSA), which covers illegal content more broadly.

The regulation entrusts both national authorities and HSPs with significant responsibilities aimed at reducing the proliferation of terrorist content while requiring them to ensure respect for the freedom of expression and information and other fundamental rights. When it was proposed, its impact on rights was among the key issues discussed. Upon a request of the European Parliament, the European Union Agency for Fundamental Rights (FRA) issued a legal opinion on the legislative proposal, identifying risks to fundamental rights and suggesting additional safeguards [1].

In accordance with Article 23 of the regulation, the European Commission should carry out an evaluation of the regulation and, where appropriate, accompany it with legislative proposals. This assessment, scheduled for 2026, should also cover the impact of its application on fundamental rights, in particular on freedom of expression and information, the respect for private life and the protection of personal data, and the functioning of the safeguards present in the regulation. To support this evaluation, the Commission requested that FRA conduct research on the impact of the regulation on fundamental rights.

Informed by the experience of practitioners and other experts in the field, the findings and opinions deriving from this research aim to support EU institutions and EU Member States in implementing legislation, policy and other measures in the area of addressing online terrorist content in full compliance with fundamental rights obligations and help them assess the need for further action in this area.

Legislative and policy context of addressing terrorist content online

International and regional law and standards

At the international level, none of the United Nations (UN) or Council of Europe conventions addressing terrorism focus on online terrorist content or set out standards for its removal. The UN Security Council has urged states to take action to address this phenomenon through a number of its resolutions, emphasising the need to work together with the private sector and civil society to develop and implement effective means to counter the use of the internet for terrorist purposes, while respecting human rights and fundamental freedoms [2]. At the Council of Europe level, the 2018 'Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities' recommends which principles should be followed when companies block or remove content, both as a result of their own moderation policies and when ordered to do so by state authorities [3]. The European Court of Human Rights (ECtHR) has a rich body of jurisprudence applicable to combating terrorist content online and the impact on human rights enshrined under the European Convention on Human Rights (ECHR) (see Section 'Addressing terrorist content online and fundamental rights').

In the absence of international treaties specifically addressing the issue, action against terrorist content online has focused on cooperation between international organisations, governments and the online industry. Since 2016, the UN Counter-Terrorism Committee Executive Directorate (CTED) and national governments have been funding Tech Against Terrorism [4], an initiative supporting companies and authorities in addressing terrorist activity online. In 2019, a group of HSPs launched the Global Internet Forum to Counter Terrorism (GIFCT) [5] that promotes technical collaboration, conducts research and shares promising practices. Following the Christchurch terrorist attack, France and New Zealand launched the Christchurch Call, a global initiative bringing together governments, civil society and the private sector to combat terrorist content online [6].

European Union law and policy

At the EU level, Directive (EU) 2017/541 on combating terrorism [7] establishes minimum EU rules and provides for a harmonised definition of terrorist offences. It criminalises a range of offences that can take place online. This notably includes public provocation to commit terrorist offences, which explicitly covers both online and offline dimensions and requires the presence of a terrorist intent of the accused and a danger that a terrorist act may be carried out as a result. As part of its research to support its evaluation by the Commission, FRA looked into the fundamental rights impact of Directive (EU) 2017/541. It recommended, among other things, to enhance the foreseeability and clarity of the offences and apply them only to conduct that is of actual terrorist nature and avoid discriminatory impact of the legislation on specific groups in society [8].

Directive (EU) 2017/541 also obliges Member States to have in place measures for the prompt removal of online content hosted in their territory that constitutes such public provocation. Member States therefore had the possibility to the order removal of online terrorist content prior to the adoption of the regulation, but typically limited it to takedowns during criminal proceedings,

with the involvement of a judge or prosecutor.

Outside this criminal law framework, the EU's response to terrorist content online was initially based on voluntary cooperation with the online industry. In 2015, the EU Internet Forum was set up, bringing together EU institutions, Member States, tech companies and other stakeholders to address challenges posed by online terrorist content and to develop guidance for companies. Among other actions, this resulted in developing the EU Crisis Protocol, a rapid response mechanism to tackle the viral spread of terrorist and other violent extremist content. Other initiatives were taken in the broader context of countering online hate speech, notably the EU Code of Conduct agreed with major platforms in 2016 [9]. In 2018, the Commission issued a recommendation on measures to effectively tackle illegal content online [10], followed by the proposed regulation.

The regulation applies alongside other legislation dealing with online content and impacting HSP moderation policies. Notably, the DSA establishes harmonised rules preventing illegal and harmful activities online, also encompassing terrorist content [11]. The Audiovisual Media Services Directive [12], as amended by the Media Freedom Act [13], requires Member States to ensure that video-sharing platforms do not disseminate content inciting terrorism.

> *The regulation sends out a clear message. […] With other types of content, maybe you can be more lenient, but when it comes to terrorist content, there is no room for it online. It has become a priority. […] As much as all harmful content is bad, there are levels to it, and the terrorist threat that we have in Europe now has to be taken seriously.*
>
> Civil-society/academia expert

Main elements of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online

- The regulation brings under its scope all HSPs that offer services in the EU and disseminate information to the public (HSPs established outside the EU have the obligation to designate a legal representative acting on their behalf in the EU).
- Competent authorities designated for this purpose by Member States, such as law enforcement agencies or media regulatory bodies, can use removal orders, a newly established tool, requiring an HSP to remove the content from its platform (or disable access to it across the EU), within one hour.
- A competent authority can send a removal order also to an HSP in another Member State, which allows that Member State's authority to scrutinise it.
- When a competent authority considers that a particular HSP in its jurisdiction is exposed to terrorist content, this HSP is required to take 'specific measures' (technical means to identify and remove content, mechanisms for users to flag alleged terrorist

content, etc.) to address the dissemination of such content on its platform.

- Further obligations for HSPs include preserving the removed content, providing information to content providers (i.e. users whose content has been subject to removal), establishing a complaints mechanism and reporting to competent authorities any content on their platform that poses an imminent threat to life.
- It sets out transparency obligations for both HSPs and competent authorities and creates a framework for imposing penalties on HSPs for infringing their obligations under the regulation. Finally, it requires Member States to put in place effective procedures for content providers and HSPs to seek a remedy before a court.

The European Union Agency for Law Enforcement Cooperation (Europol) plays a particular role in addressing terrorist content online and supporting Member State authorities in this field. The EU Internet Referral Unit was established at Europol's European Counter-Terrorism Centre in 2015 with the task of detecting and investigating malicious online content and has been active in sending HSPs referrals, which flag suspected terrorist content on companies' platforms for their own review [14] . In July 2023, it launched the EU Platform on Illicit Content Online (PERCI) to support Member States in applying the regulation. Notably, it allows transmitting removal orders and referrals, supports the scrutiny of cross-border removal orders and facilitates deconfliction (avoiding that a removal of content by one Member State would interfere with investigations in other Member States).

Addressing terrorist content online and fundamental rights

The proliferation of terrorist content online seeking to radicalise and recruit individuals and to facilitate and direct terrorist activities poses significant risks to public safety and security and can impact a variety of fundamental rights guaranteed by the European Union Charter of Fundamental Rights (the Charter). These range from the right to life (Article 2) to freedom of expression and information (Article 11) of the broader online community, and the rights of victims of past terrorist attacks. Such content is increasingly aimed at children and young adults and can have a particularly harmful impact on them, affecting the rights of the child (Article 24) [15] . By addressing this phenomenon, the regulation helps protect these rights and interests.

At the same time, as with any counterterrorism measure, regulating online content gives rise to fundamental rights challenges. The regulation recognises its impact on specific rights. Article 1(4) emphasises freedom of expression and information, including freedom and pluralism of the media, while the preamble highlights the need to also safeguard the right to respect for private life, the protection of personal data, freedom to conduct a business, the prohibition of discrimination and the right to an effective remedy (Recitals 3 and 10). The need for any interference with rights to observe the principles of necessity and proportionality is recognised. The regulation also provides for particular protection of material disseminated for educational, journalistic, artistic and research purposes, along with material aimed at raising awareness against terrorism, and

underlines that radical, polemic or controversial views expressed in public debate should not be equated with terrorism (Article 1(3) and Recital 12). In the context of the requirement to evaluate the regulation (Article 23), the prominent place given to the impact on fundamental rights and on the functioning and effectiveness of safeguards should testify to the importance that the EU legislator attaches to this matter.

ECtHR jurisprudence on the freedom of expression is of particular relevance when analysing the interplay between combating terrorist content online and human rights [16].

According to the ECtHR, the right to freedom of expression pursuant to Article 10 of the ECHR (equivalent to Article 11 of the Charter) constitutes one of the essential foundations of a democratic society [17]. The ECtHR held repeatedly that its protection extends to forms of expression less favourably received or those that even offend, shock or disturb [18]. Furthermore, freedom of expression includes positive obligations, implying that states must establish effective mechanisms protecting content providers to create a favourable environment for participation in public debate, enabling them to express their opinions and ideas even if they counter official authorities or public opinion [19].

The ECtHR has recognised that the objective of the fight against terrorism represents a legitimate limitation to freedom of expression and that clear incitement of violence and support for terrorist activities does not enjoy the protection afforded by Article 10 of the ECHR [20]. The Court of Justice of the European Union (CJEU) has likewise indicated that the fight against terrorism may, in certain cases, restrict fundamental rights due to its legitimate aim of protecting national security [21]. However, while restrictions on idealising, condoning or commenting positively on terrorist crimes and terrorists are in principle justified, the definition of terrorist content may only cover forms of expression that manifestly incite, glorify or justify violence, hatred or other forms of intolerance relating to terrorist activities, going beyond a mere expression of sympathy [22]. Politically sensitive statements that nevertheless do not advocate violence may form part of a debate of general interest, protected by Article 10 of the ECHR [23]. Furthermore, when classifying speech as inciting violence or defending terrorism, the ECtHR found that the determination must focus on the content and the context of the publication, their potential impact and the personality and function of the person making the statements [24]. It has acknowledged the important role that the internet plays in the exercise of freedom of expression by facilitating the dissemination of information and access by the public, while recognising that it has the potential to exacerbate the impact of illegal speech [25].

The ECtHR has clarified that Article 10 permits only restrictions that are necessary and proportionate ‘within a democratic society’ and are clearly prescribed by law, which includes their accessibility and foreseeability [26]. When states take measures affecting fundamental rights, the law must indicate the scope of any discretion conferred on the authorities and the manner of its exercise with sufficient clarity, giving the individual adequate protection against arbitrary interference [27]. The ECtHR has also repeatedly emphasised the importance of judicial intervention in cases related to limitations of freedom of expression to provide a genuine safeguard against abuse, underlining that judicial review of limitations which only takes place *ex*

post and upon application might not provide a sufficient guarantee against abuse [28].

The jurisprudence illustrates the challenges of regulating this area in a manner which is both effective and complies with fundamental rights. Indeed, the draft regulation proposed by the Commission in 2018 [29] attracted considerable scrutiny and concerns over its impact on a range of fundamental rights by national and EU stakeholders, international human rights bodies, civil-society organisations, professional associations, academics and HSPs. This resulted in significant changes to the text and the insertion of additional safeguards. Some of these sources and the concerns identified by them are referenced throughout the report as they appear to remain relevant in light of the findings on the practical application of the regulation.

Methodology and scope

This report is primarily based on data collected through fieldwork involving interviews with 62 practitioners and other experts, representing three broad professional categories: staff of competent authorities applying the regulation, staff of HSPs and experts from civil society and academia. The annex provides further details on the composition of the respondent groups, the methodology of the interviews and the manner in which the respondents and the insights they shared are referred to throughout the report.

The fieldwork was supplemented by limited desk research. In addition, Europol (the EU Internet Referral Unit of the European Counter-Terrorism Centre) provided FRA with information on the functioning and use of PERCI.

The main aim of the research was to analyse the impact of the application of the regulation on fundamental rights and freedoms safeguarded by the Charter. The report builds upon and complements FRA's prior work on terrorism. In comparison with FRA's 2019 legal opinion on the proposed regulation, which provided a legal analysis of the draft text, the current report focuses on the practical insights of practitioners and experts applying the regulation. This allows for the comparison of the concerns raised during the discussions on the proposal with actual application in practice.

Coverage of hosting service providers' experience

In comparison with the openness to speak about their experience with the regulation that existed among experts from competent authorities and civil society / academia, the research encountered challenges in reaching out to HSPs. Some, whose experiences can be considered very relevant due to their size, exposure to terrorist content or declared commitment to respect fundamental rights, refused to participate in the research. As a result, the size of the respondent group of HSP experts was comparatively smaller than other respondent groups. To compensate for this, additional information about HSP practices was collected from those experts in the civil-society/academia respondent group who had experience working in the area of online content moderation, including for major HSPs, or in

supporting HSPs with capacity-building efforts.

The unwillingness of some HSPs to share their views on the fundamental rights impact of the regulation underpins one of the key findings from this research – the transparency limitations surrounding the use of the regulation.

The 2021 FRA report on Directive (EU) 2017/541, which looked at the impact on fundamental rights and freedoms of the main EU criminal law instrument in the field of counterterrorism, is likewise relevant as the regulation relies on this legal instrument when defining some of its core concepts, most notably the definition of terrorist content online, which is at the heart of some of the application challenges identified by the research.

The regulation provides new tools for the removal of online terrorist content that may present new challenges and implications for the practical exercise of fundamental rights. The research particularly concentrates on the impact its provisions may have on freedom of expression and information; the right to private and family life; freedom of thought, conscience and religion; freedom of assembly and association; freedom of the arts and sciences; freedom to conduct a business; prohibition of discrimination; and the right to an effective remedy.

While Article 23 of the regulation specifically mentions the need to evaluate the impact on the protection of personal data, FRA's research collected limited information in this respect. This is largely due to the limited number of HSPs that agreed to participate in the research (see textbox 'Coverage of HSP experience') and could share relevant insights as regards the application of the obligation to preserve removed content pursuant to Article 6 of the regulation, one of the most relevant provisions with regard to this right. Therefore, while this report recognises the impact of the regulation on the protection of personal data, it does not further examine it.

The findings of the research need to be considered in the context of the state of application of the regulation. While the regulation became applicable in June 2022, its uptake by Member States was gradual and uneven in terms of designating the competent authorities and making use of removal orders, the first of which were issued in 2023 [30] . Therefore, at the time when the fieldwork was carried out in the second half of 2024, only some competent authorities and HSPs had practical experience in applying the regulation and could share meaningful insights. Furthermore, very limited to no experience could be collected with respect to some elements of the regulation that would be necessary for a proper assessment of its impact on fundamental rights, namely specific measures, scrutiny of cross-border removal orders, penalties and, in particular, remedies. While specific measures, scrutiny and remedies are covered by this report, to the extent possible, the role of penalties is not explored given this lack of information. Despite the described limitations, interviewees provided FRA with rich information and practical insights, beyond specific fundamental rights implications, which permitted FRA to build a comprehensive framework to conduct research and analysis, and allowed for the contextualisation of the fieldwork findings.

- Chapter 1 introduces fundamental rights challenges arising in relation to the definitions used by the regulation, in particular the clarity and scope of the definition of online terrorist

content.

- Chapter 2 presents the impact on fundamental rights of the main instruments used by competent authorities to address terrorist content online – namely, the newly introduced removal orders under the regulation, alongside the pre-existing referrals, which are variously used by authorities to flag content to HSPs for their own assessment.
- Chapter 3 looks at fundamental rights issues emerging from HSPs' own content moderation efforts and their interplay with the regulation, including in the context of the obligation to implement specific measures such as employing automated detection tools.
- Chapter 4 addresses the effectiveness of the scrutiny of cross-border removal orders and of judicial remedies, two key safeguards under the regulation.

1. Defining terrorist content online

To define online terrorist content, the regulation relies on existing definitions of 'terrorist offences' and 'terrorist group' in Directive (EU) 2017/541 on combating terrorism (see textbox 'Definitions of terrorist offences and a terrorist group in EU law'). Article 2(7) of the regulation encompasses content that incites or solicits the commission of one of the terrorist offences established by Directive (EU) 2017/541 or constitutes a threat to commit one of the offences. Material that solicits participation in the activities of a terrorist group also falls under this definition. Finally, material that 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 offences, is likewise considered terrorist content.

Definitions of terrorist offences and a terrorist group in EU law

Directive (EU) 2017/541 on combating terrorism lists, in Article 3, a number of activities, ranging from attacks on the life or physical integrity of a person to interfering with information systems, that may seriously damage a country or an international organisation. These are considered to constitute terrorist offences when committed with the aim of seriously intimidating a population, unduly compelling a government or an international organisation to perform or abstain from performing any act or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.

A terrorist group is defined in Article 2(3) of Directive (EU) 2017/541 as a structured group of more than two persons, established for a period of time and acting in concert to commit terrorist offences.

Concerning incitement of the commission of terrorist offences, the regulation incorporates the definition of public provocation to commit a terrorist offence present in Article 5 of Directive (EU) 2017/541, including content which indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences.

The regulation only applies to content that is 'disseminated to the public', i.e. made available to a potentially unlimited number of persons (Article 2(3) of the regulation). As a result, content shared privately, for example via messaging applications, is exempt from its scope.

Furthermore, Article 1(3) – similarly to Recital 40 of Directive (EU) 2017/541 – specifies that material shared with the public for educational, journalistic, artistic or research purposes or for the purposes of preventing or countering terrorism, including material expressing polemic or controversial opinions within public debate, will not be classified as terrorist content, and that an assessment will determine whether material is disseminated for these purposes.

Findings related to the definition of terrorist content online have implications for the application of the regulation as a whole, including its key provisions on issuing removal orders, scrutiny of cross-border removal orders, the application of specific measures and penalties, and access to remedies, as examined in Chapters 2, 3 and 4. Besides the general principles of legal clarity and foreseeability, these issues impact, in particular, freedom of expression and information (Article 11 of the Charter). In addition, they can have an impact on a variety of other rights, including but not limited to freedom of thought, conscience and religion (Article 10 of the Charter), freedom of assembly and of association (Article 12 of the Charter), freedom of the arts and sciences (Article 13 of the Charter), freedom to conduct a business (Article 16 of the Charter), non-discrimination (Article 21 of the Charter) and the right to an effective remedy (Article 47 of the Charter).

This chapter covers respondents' experiences and views as regards the impact on fundamental rights stemming from the definition of terrorist content in the regulation and its application by competent authorities in practice. It focuses first on the suitability of the definition – its legal clarity and foreseeability. Then it discusses how the diversity in competent authorities applying the definition affects these challenges. The chapter subsequently zooms in on the interplay between the definition and the risk of over-removal when it comes to educational, journalistic, artistic and research-related content.

Summary of findings: Defining terrorist content online

- While competent authorities generally strive to issue removal orders on content that is clearly terrorist content in nature, the definition of online terrorist content in the regulation would benefit from additional clarity and foreseeability. A joint understanding among competent authorities of what types of content should fall under the scope of the regulation and a common baseline for assessing content are still missing.
- The regulation is based on definitions developed to be used in criminal proceedings rather than in an administrative context. The concept of glorification is considered especially challenging when it comes to distinguishing between terrorist content and permissible forms of expression.
- Diverse national approaches to appointing competent authorities result in the involvement of bodies with different levels of expertise and resources in the field of counterterrorism, on the one hand, and fundamental rights, on the other, exacerbating the challenges related to a uniform application of the definitions and assessment of what terrorist content is and how fundamental rights are safeguarded in the process.
- Despite limited practical experience with such cases so far, interviewees broadly acknowledge the potential impact of the regulation on protected forms of speech (such as educational, journalistic, artistic or research purposes) and the importance of carefully assessing whether particular content may fall into this category.

1.1 Suitability and legal clarity of the definition of online terrorist content

The findings, based on the views of interviewed experts across professional groups, show that the definition of online terrorist content presents one of the main challenges when it comes to the fundamental rights impact of the regulation. The clarity of the definition and foreseeability of its use are essential both to ensure uniform application of the regulation across the EU and to avoid unintended risks for a variety of rights.

During the negotiations on the proposed regulation, the definition was subject to considerable discussion. In a joint communication, three UN special rapporteurs expressed concerns that the regulation would go beyond content that is criminal in nature and called to ensure that the definition of terrorist content is narrowly construed to guarantee that measures taken pursuant to it do not unduly interfere with human rights [31]. Some of these concerns were reiterated during the parliamentary and expert discussions on national legislation implementing the regulation in a number of Member States [32]. In the adopted text of the regulation, the definition was more closely linked to the criminal law definitions in Directive (EU) 2017/541.

Several interviewees, including experts from competent authorities and civil society / academia, question the overall suitability of the definition. The definitions of terrorist offences in Directive (EU) 2017/541, which the regulation relies on, have been developed for the purpose of criminal proceedings where they are applied by a court based on the combination of objective elements of the crime in question and the perpetrator's intent. According to these experts, this makes the definitions inherently ill-suited for speedy decision-making in administrative proceedings, which are not accompanied by the same requirements and level of procedural safeguards. From this perspective, a clearer, unambiguous distinction between legal and illegal content would appear more appropriate.

In general, most interviewed experts consider that the definition of online terrorist content in the regulation would benefit from additional clarity and foreseeability. This includes the majority of experts from competent authorities. Some of them highlight that a joint understanding of what types of content should fall under the scope of the regulation and a common baseline for assessing content are still missing.

> *[The regulation] is a legal text that cannot cover all aspects of what one sees in disseminated content, so you always put your judgement as an expert into it. And […] maybe the same content is viewed a bit differently by different experts from different countries. And then, if it is country A [issuing a removal order] and country B scrutinising it, if this joint understanding, this baseline is not there, then maybe there is an issue.*
>
> Competent authority expert

Despite the harmonisation through Directive (EU) 2017/541, differences in the definitions of terrorist offences such as incitement (public provocation) to terrorism and operational realities across Member States give rise to different interpretations of what constitutes terrorist content online. Some experts from this professional group say that clarifying what content falls under the definition requires internal consultations with other institutions or legal experts. Only a minority of experts from competent authorities consider the regulation sufficiently clear, with some adding that they in fact appreciate a broader definition that leaves room for a more flexible application of the regulation within the national context.

Promising practice: Aligning the interpretation of the regulation among competent authorities through regular workshops

To support uniform application of the regulation and facilitate discussions among competent authorities, the Commission regularly organises technical workshops. In addition, Europol runs workshops dedicated to the use of PERCI. Experts from competent authorities highlight that these regular exchanges are very useful to discuss, among other things, the scope and interpretation of the regulation.

Civil-society/academia experts generally perceive the wording of the individual provisions of Article 2(7) as too vague and open to interpretation. Some warn that it is likely to lead to diverging interpretations among Member States but possibly also among practitioners within the same Member State. Besides reducing the foreseeability of how the regulation is applied, it also underlines the need for systematically and rigorously applying the mechanism for scrutiny of cross-border removal orders (see Chapter 4).

Concerns over the clarity of the definition are also raised by experts with direct content moderation perspectives. Some HSP experts and civil-society/academia experts with such experience note that the definition in the regulation is not well-suited to practical use and is difficult to apply in the context of online content. In their view, technical experts dealing with content moderation could have been involved when drafting the regulation to find a definition better suited to the specificities of online content moderation.

Interviewees across professional groups consider that the main challenge is associated with interpreting the concept of incitement to terrorism (Article 2(7)(a)), in particular the inclusion of 'glorification' of terrorist acts.

Human rights experts have long been critical of including vague concepts such as 'glorifying' or 'promoting' terrorism in the definition of incitement (public provocation), arguing that these not only miss the necessary precision but also make it difficult to establish the risk that an actual terrorist offence might be committed as a result (an element required also by Article 2(7)(a) of the regulation) [33] .

Civil-society and academic experts, in particular, highlight the distinction between glorification and

direct incitement as a source of concern. By also including in its scope, in Recital 11, dissemination of 'material depicting a terrorist attack', any content that comments on an act of terrorism could be subject to removal on this basis. Others recall that the entire concept of glorification is based on the subjective intention of the author to encourage terrorist activity, which is difficult to assess in the case of online content. As also shown in FRA's earlier research on terrorism, the link between glorification and intent is so intrinsic that the boundaries between polemic or radical, yet permissible, expression and glorification are often difficult to draw even during criminal proceedings [34]. For this reason, some civil-society/academia experts suggest opting for much narrower definitions capturing content which should be objectively subject to removal regardless of its context and intent, for example – as suggested during the fieldwork – decapitation imagery.

> *The fact that glorification made it to the final text, and that any type of expression that simply comments on a committed terrorist attack or inappropriately criticises public officials or the government, could fall into the scope of glorification […] is an enormous issue.*
>
> Civil-society/academia expert

Experts from competent authorities likewise point out issues with the concept of glorification. Pointing to the differences in Member States' legislation, some state that glorification as referred to in the regulation does not feature under their national law, and they would not be sure how to apply it in case they encountered such content. Others say that the application of this definition is straightforward only if the content relates to organisations clearly recognised as terrorist groups or if it glorifies specific past terrorist attacks or their perpetrators.

These questions surrounding the legal clarity and overall suitability of the definition can have a significant impact on freedom of expression and information, freedom of thought, conscience and religion, and freedom of assembly and association.

The majority of interviewed experts from civil society / academia warn that the definition leaves too much room for subjective assessment and removal of content that is not of a terrorist nature. In this context, some recall that Directive (EU) 2017/541 – despite its Recital 40 aimed at safeguarding the expression of radical, polemic or controversial views – has been subject to critique for being overly broad and over-inclusive, potentially leaving room for application influenced by political considerations and for covering activities that are not of a terrorist nature, such as solidarity movements or environmental activism [35]. This conflation of legitimate protest and terrorism, in turn, gives rise to a risk of over-enforcement of the regulation and could result in targeting views critical of the government, experts from civil society / academia warn.

Experts from competent authorities acknowledge the potential impact that the regulation can have, in this respect, on fundamental rights. Some of them expressly state that they are aware of the need to pay close attention to the risk of affecting, in particular, freedom of expression and capturing political opinions, when applying the regulation. According to these experts, the clarity

issues associated with the regulation's definition of terrorist content make them even more cautious and selective when applying it. This leads them to issuing removal orders only on clear-cut cases of terrorist content which can withstand judicial scrutiny.

> *We act against clear terrorist content. Nobody will be affected in their freedom of expression […]. We do not act against political opinions. […] So, we are only on safe territory.*
>
> Competent authority expert

Clarity of other provisions of the regulation

Besides the definition of terrorist content in Article 2(7), interviewees identified other provisions of the regulation that would need further clarity. Those of particular importance in terms of fundamental rights impact, relating to the use of referrals, specific measures and scrutiny of cross-border removal orders, are dealt with in the respective chapters.

In terms of the regulation's scope, the question of who can be issued a removal order for websites operated directly by terrorist organisations is of particular importance for experts from competent authorities. Some HSP and competent authority experts also point to the need to clarify the tasks of legal representatives that HSPs established outside the EU have to designate in accordance with Article 17.

1.2 Bodies interpreting the definition: independence, expertise and oversight

According to Article 12(1), Member States have to designate authorities competent to issue removal orders, scrutinise cross-border removal orders, oversee the implementation of specific measures and impose penalties. Recital 35 requires that competent authorities fulfil their tasks in an objective and non-discriminatory manner. In all other aspects, the regulation leaves the choice of competent authorities to the discretion of Member States.

In practice, this results in a diverse landscape across the EU when it comes to which authorities are responsible for interpreting and applying the definition of what constitutes terrorist content (i.e. issuing removal orders and scrutinising cross-border removal orders issued by other Member States) [36] . Depending on the jurisdiction, this may include law enforcement agencies, intelligence services, public prosecutors, media regulators or other administrative bodies. Only in a small number of Member States [37] are courts involved, to varying degrees, in the assessment of the legality of content and issuing removal orders.

This necessarily leads to the involvement of authorities with different levels of expertise in the field of counterterrorism, on the one hand, and fundamental rights, on the other, depending on the

particular set-up in each Member State. This, in turn, exacerbates the challenges related to a uniform application of the definitions and the assessment of what terrorist content is, and may further impact the clarity and foreseeability of how the regulation is applied and how fundamental rights are safeguarded in the process.

From the fundamental rights point of view, when assessing the nature of online content and the need for its removal, an independent judicial authority would be best placed to make an impartial decision to meet public security needs without violating fundamental rights, an argument voiced during the discussions on the draft regulation [38] . This was also emphasised by some experts from civil society / academia interviewed for this research, some of whom stated that even if the body making the assessment is not a court, it needs to be independent of the interests involved, both those of law enforcement and those of HSPs. This is of particular importance given that removal orders have an immediate effect on fundamental rights while a subsequent remedy may have only a limited restorative effect (see Chapter 4). Concerns over which entity would be designated as the national competent authority for issuing removal orders featured prominently in parliamentary and public debates surrounding the implementation of the regulation across Member States. Some of the concerns raised in these discussions related to an alleged risk of online monitoring and abuse by law enforcement or intelligence services [39] , questions of independence of the designated competent authorities [40] or calls to involve judicial authorities [41] . In some Member States, these concerns led to amendments integrating additional safeguards [42] .

When it comes to tasking law enforcement and intelligence authorities with assessing the nature of online content and the need for its removal, some civil-society/academia and HSP experts raise concerns in relation to the rule of law, institutional priorities and the absence of checks and balances. In the case of media regulators, interviewees' concerns focus on expertise in dealing with terrorist content and a potential conflict with their mandate to regulate internet platforms.

Positively, interviews with experts from competent authorities and civil society / academia show that in several Member States, additional safeguards are in place in the form of internal review mechanisms introducing layers of oversight. In some cases, draft removal orders are reviewed by superiors before they can be issued. In others, multiple staff with different expertise are involved in assessing content, either in a formalised manner or by means of ad hoc consultations. In some competent authorities, internal boards review selected cases, such as those which are not fully clear or are considered to be of a precedential nature.

Promising practice: Implementing external oversight when issuing removal orders

In some Member States, two different national competent authorities are involved in issuing removal orders, with one (typically a law enforcement or counterterrorism body) making the assessment of the content and one reviewing and approving the decision to issue a removal order. This approach adds a degree of external oversight and expertise. At the same time, findings show that its effectiveness as a safeguard depends on a variety of factors such as

the capacity and expertise on the topic of the reviewing body, the (non-)mandatory nature of the review, *de jure* or de facto (e.g. due to limited access to information) limitation of the review to formal elements of the removal order or the degree of independence of the reviewing body.

> *I was not sure [our authority] would be assigned this role, we thought it would be a judge. But finally, it was decided that we do it […] and it does work.*
>
> Competent authority expert

Some experts from authorities tasked with issuing removal orders or scrutiny of cross-border removal orders acknowledge that the regulation requires them to carry out tasks that go beyond their existing expertise. In particular, as regards assessing the impact of the removal of content on fundamental rights, some of these experts consider courts to be better equipped for the task. Most, nevertheless, indicate that the transition has been successful.

Interviewees across professional groups also underline the importance of sufficient resources. Experts from civil society / academia and HSPs note that capacity across Member States in terms of staffing, training to assess content and language expertise differs, which may be one of the reasons for the uneven use of the regulation across the EU.

> *In terms of capacity, it's not always easy to work on daily basis. There are tasks for [the] TCO [regulation], but there are also other things to do.*
>
> Competent authority expert

This is confirmed by experts from competent authorities. While some of them consider the resources available to them sufficiently robust, a number of experts note that the application of the regulation resulted in an increase in their workload, which has not necessarily been accompanied by a commensurate increase in resources. Recalling the vast amounts of online material, some of these experts note that resources limit their ability to focus on online terrorist content on a daily basis or to specialise in detecting and assessing particular types of content.

1.3 Content disseminated for recognised legitimate purposes

Besides the need to safeguard freedom of expression and information more broadly, Article 1(3) of the regulation recognises that material disseminated for certain legitimate purposes warrants special protection – a provision that a number of interviewees consider to be an important safeguard.

In general, interviewees across professional groups acknowledge the potential impact of the regulation on protected forms of speech and the importance of carefully assessing whether

particular content may fall into this category, which may be difficult given the definitional issues surrounding terrorist content and, in particular, glorification. Some interviewees recall past cases, unrelated to the regulation, where the content of researchers working on terrorism was removed. Such risk may arise, for example when it comes to events that involve terrorist organisations and are heavily covered by media reporting and academic research, such as the situation in Israel and Gaza following the attacks of 7 October 2023. Some interviewees point out to a possible interplay with discrimination if some languages or backgrounds are associated with terrorism more than others. As an example of such concerns, a civil-society/academia expert notes that some academics working on terrorism-related topics might be at a higher risk of having their content removed than others, due to factors such as their name or the language in which they write.

In terms of artistic expression, multiple interviewees draw parallels between terrorist content and violent content more generally and point to a case dealt with by the Oversight Board in 2022 concerning removals of drill rap music [43] content based on referrals by the UK Metropolitan Police due to alleged threats of violence. The Oversight Board overturned these decisions, namely arguing the absence of sufficient evidence that the content contained a credible threat, and for the need to give more weight to its artistic nature [44] . Interviewees, including some experts from competent authorities, note that this case illustrates possible challenges when it comes to terrorist content and artistic expression.

> *To be fair, I believe competent authorities already have enough work to do and if they see that something is from a trusted source, like a think tank or a researcher, this would not be the content they would focus on, for the most part.*
>
> Civil-society/academia expert

Respondents across professional groups generally state that concrete experience with having to assess whether potential terrorist content falls under the protective provision of Article 1(3) is limited so far. Explaining these points - one civil-society/academia expert refers to the limited capacity of competent authorities, which forces them to focus on clearly terrorist content only, such as propaganda disseminated directly by terrorist organisations, which reduces the risk of overreaching to such protected forms of content; and an expert from a competent authority shares a practical example of a video that contained what would otherwise be clearly considered terrorist content, but that was shared by a university for educational purposes rather than promoting terrorism. At the same time, some experts from competent authorities point to the existence of outlets belonging to actual terrorist organisations and intended to disseminate their propaganda (which would obviously not benefit from the protection envisaged in the regulation). Other interviewees point to the tactic of some malicious actors to disseminate terrorist content under the guise of journalistic or educational purposes in order to avoid enforcement, choosing platforms that do not apply stringent scrutiny to such content.

> *For media […], it's very difficult to assess, and I don't think we are going to*

remove it that easily. Educational platforms, we don't touch them, if we know them.

Competent authority expert

Interviewees from competent authorities also outline some approaches that, in their view, mitigate the risk of targeting content disseminated for such legitimate purposes. For example, one expert explains that they avoid targeting educational platforms, especially if they are familiar with them or if their review confirms the platform's educational nature. Some others recall that the general principle of assessing the content as well as its context (e.g. not just the actual footage but also the circumstances of its dissemination) is of particular importance when it comes to correctly recognising educational, journalistic or similar content.

Promising practice: Additional measures to safeguard media independence

FRA's desk research covering the national legislation implementing the regulation across the EU also identified that competent authorities in several Member States have the possibility to consult authorities responsible for safeguarding the independence of the media and media ethics prior to issuing a removal order or when scrutinising a removal order issued by another Member State, to assist in the assessment of the content and the fundamental rights impact of its removal [45] . Although this measure is not mandatory in any of the Member States, it can be considered a useful safeguard

2. Removal orders and referrals

The key novelty introduced by the regulation is removal orders, which national competent authorities can issue to HSPs requiring them to remove terrorist content or to disable access to it in all Member States (Article 3(1)), as soon as possible and, in any event, within one hour of the receipt of the removal order (Article 3(3)). If a competent authority has not previously issued a removal order to an HSP, that HSP should receive information on the applicable procedures and deadlines, at least 12 hours before issuing the removal order (Article 3(2)).

Terminology – removal of versus disabling access to online content

Under the regulation, removal orders can be complied with either by removing the content or by disabling access to it (blocking it) in all Member States. The choice of the measure is left up to HSPs, allowing them to keep the content online in those jurisdictions outside the EU where it is not considered illegal. Unless stated otherwise, references to the removal of content throughout this report also encompasses disabling access.

The rationale behind the one-hour limit is based on the need to counteract the 'speed at which terrorist content is disseminated across online services' (Recital 17). The regulation does not envisage the HSPs reviewing the content and potentially objecting to its removal during this one-hour period, unless there are manifest errors or technical issues preventing them from implementing the removal order (Article 3(8)).

Recital 40 also acknowledges the parallel existence of referrals. Referrals are not governed by the regulation but authorities of some Member States (typically 'internet referral units' set up within some national law enforcement and counterterrorism authorities based on national legislation) and Europol (the EU Internet Referral Unit, based on the explicit mandate to issue referrals under Article 4(1) of the Europol Regulation [46] use them to alert HSPs of content that could be considered terrorist content, for the provider's voluntary consideration of its compatibility with its own terms and conditions. The final decision on whether to remove the content flagged by a referral therefore remains with the HSP. Referrals are described in the regulation as an effective means of increasing HSPs' awareness of specific content available through their services and enabling them to take swift action. The regulation leaves it up to competent authorities whether to use a removal order or a referral when addressing terrorist content online. The interplay between the use of referrals and removal orders presents an important factor when it comes to the application of the regulation and its impact on fundamental rights.

This chapter addresses the fundamental rights implications of the mandatory nature of removal orders and the one-hour time limit for their execution. It looks at the implications for the rights of content providers and other users, notably their freedom of expression, along with the impact on HSPs and their freedom to conduct a business. Afterwards, it explores the interplay between the use of removal orders and referrals and its implications on fundamental rights.

Summary of findings: Removal orders and referrals

- The obligation to remove content within one hour of receiving a removal order does not allow HSPs to review the content, while questions arise about the proportionality of this requirement in some cases.
- The risk of erroneous assessment of content can be aggravated in the case of certain languages and subject matter, and for content related to current events or sensitive political issues. Besides the risk of removing legitimate content, this can disproportionately affect some groups of content providers and cause a chilling effect on rights.
- While jihadist terrorism is considered a key security threat in the EU, the strong focus of removal orders on jihadist content leads to questions of whether the application of the regulation adequately captures all types of terrorist content, notably that related to right-wing terrorism.
- Competent authorities largely continue to rely on referrals as a tested, less formal and more agile tool. The lack of clarity as to when removal orders and referrals, respectively, should be used, reduces foreseeability and transparency, leads to an uneven application of safeguards and can undermine the voluntary nature of referrals.
- The processing of removal orders can present a significant challenge, especially for smaller HSPs, due to their limited resources and means of operation. At the same time, the lack of cooperation by some HSPs and the present practice among competent authorities of targeting a narrow selection of HSPs, mostly larger social media platforms, can lead to gaps in addressing the proliferation of terrorist content across HSPs. Furthermore, the regulation appears to have been eclipsed by the DSA in terms of HSP awareness and compliance efforts.

2.1 Impact of removal orders on content providers and HSPs

When it comes to the impact of removal orders on content providers, interview findings reveal that respondents' concerns relate mostly to freedom of expression and information (Article 11 of the Charter) and the right to an effective remedy and a fair trial (Article 47 of the Charter). Given the risk of over-removal and a potential chilling effect, other impacted rights can include freedom of thought, conscience and religion (Article 10 of the Charter), freedom of assembly and of association (Article 12 of the Charter), freedom of the arts and sciences (Article 13 of the Charter) and non-discrimination (Article 21 of the Charter). Furthermore, the requirements for swift compliance with removal orders set out by the regulation also impact HSPs' freedom to conduct a business (Article 16 of the Charter), a concern expressed already in relation to the draft regulation in 2018 [47] .

2.1.1 Mandatory prompt removal of content

The risk that the requirements of the regulation concerning the execution of removal orders can lead to removals of legitimate content and adversely impact the freedom of expression and other rights of content providers and other users is acknowledged by interviewed experts across professional groups. This stems from the combination of two broad factors – the risk that the removal order may be issued on content that is not terrorist content in nature, coupled with the obligation for HSPs to speedily remove flagged content without an opportunity to review it first.

Prior to removal, the regulation leaves determining the terrorist nature of the content squarely in the hands of the competent authorities. It does not envisage the HSP addressed by the order to review the content in question, requiring them to implement it except for narrowly defined circumstances in Article 3(8), none of which relate to the actual nature of the content. HSPs have possibilities to voice their objections – to review the content and decide to contest the removal in court or in front of the authority conducting scrutiny of cross-border removal orders – only once they have complied with the removal order (see Chapter 4) [48] .

If an HSP considers that the content does not contravene its own terms and conditions, it has the possibility to block it within the EU only. This is important for those HSPs that operate also in other jurisdictions where the same content might be legal. Such a solution, nevertheless, still impacts the rights of content providers and users within the EU.

Experience shared by experts from HSPs shows different approaches by companies in this regard. One testifies that they systematically take down the content first, then conduct their review, and another emphasises that they would simply remove the content within minutes. Another HSP expert, without practical experience with removal orders so far, likewise indicates that they are not expected to review the legality of the order and would tend to trust the assessment of the authorities, which is their default approach to government requests.

Experts from some large HSPs with experience in receiving multiple removal orders, on the other hand, point out that they attempt to assess the content first but that the one-hour period makes it difficult to do so. As an example of practical challenges that were raised, one of these experts says that they frequently need to request clarifications and understand the reasoning behind the order, especially when the content does not appear to be terrorist content in nature, but are mostly forced to remove the content before doing so.

> *The one-hour removal requirement leaves very little time for review before enforcement. This can have unintended consequences for users' rights, particularly freedom of expression and access to information, if a takedown request is issued in error. In rare cases, legitimate content may be removed unnecessarily.*
>
> HSP expert

Some HSP and civil-society/academia experts highlight that HSPs' approach to scrutinising removal orders may depend on the business model of the company, the priority attached to combating terrorist content in its own policies, its relationship with the authorities and the degree to which it is willing to go into conflict with them over the fundamental rights of its users.

As some of these experts note, awareness of HSPs also varies significantly, not only about the regulation in general, but particularly about fundamental rights issues, which can be low among smaller HSPs. This might hamper them from assessing the fundamental rights impact of removal orders they receive, not only before but also after executing the order. An expert from a smaller HSP, which has already been subject to removal orders, highlights that the risk of fines might especially demotivate smaller HSPs from questioning the assessment of the authorities.

> *With smaller providers, this can be an issue. If […] you were going to get a fine because you didn't act fast enough, then you will obviously actively start to enforce things more on your side – better safe than sorry.*
>
> HSP expert

In this context, some interviewees question the balance between the need for urgently removing content and the impact of the one-hour deadline on HSPs, and, through them, on the rights of content providers when it comes to legitimate content that may be erroneously removed.

Some HSP and civil-society/academia experts argue that the importance attached by the regulation to the speed of removal as the main metric of compliance disregards the quality of terrorist content moderation systems implemented by HSPs themselves. These experts recall that the regulation complements HSPs' own moderation, through which they remove much more terrorist content, and much faster, than competent authorities can flag. Therefore, metrics should take into account these efforts by HSPs and the general quality of their cooperation with authorities, and also the quality of content of removal orders issued to HSPs by competent authorities, which varies and has an impact on the speed at which HSPs can process them.

Some interviewees argue that different types of content might justify different responses. Recalling the Christchurch terrorist attack, it should be noted that interviewees across *all* professional groups acknowledge the need for speedy takedowns to avoid viral sharing of footage of attacks or terrorist manifestos. Some of them question, however, whether the same urgency applies to all types of content falling within the scope of the regulation, noting that a similar obligation to remove terrorist content within one hour was already invalidated by national courts in the past [49] .

Some civil-society/academia interviewees say that the one-hour timeframe appears particularly stringent when compared with the DSA which covers illegal online content more broadly and takes into account the size of HSPs, establishes an approach based on identifying and countering systemic risks and does not impose strict deadlines.

Experts from civil society / academia also reflect that while the one-hour deadline begins to run

after a competent authority flags the content to the HSP (and not from the moment of detection), competent authorities do not always issue removal orders immediately but might instead gather information and then flag multiple pieces of content at once. As a result, HSPs might receive a batch of removal orders and have only one hour to handle them all. This can put a strain on the company's resources but also raises questions over whether the content indeed requires urgent removal.

Interviewees from competent authorities indicate that while most removal orders are complied with by HSPs (nearly 90 % resulting in the removal of content) and HSPs have been mostly managing to comply with the one-hour rule, it appears to present a challenge for some of them. Some mention a period of up to 24 hours, which, according to some experts, matches the time during which they would expect HSPs to act upon a referral, as acceptable, while others have experienced delays ranging from 15 minutes to a couple of days in a few instances. This variety and degree of lenience likewise indicate that authorities do not consider all content flagged by removal orders to necessarily warrant the urgency implied by the one-hour rule.

2.1.2 Risk of erroneous assessment of content

As discussed in Chapter 1, many interviewees consider that the definition of terrorist content is not sufficiently clear and foreseeable, which increases the likelihood of removal orders being issued in error.

This risk might be higher for certain types of content, for example based on language or subject matter requiring particular expertise. While most experts from competent authorities state that they have the necessary capacity to deal with languages in which they typically encounter potential terrorist content, many acknowledge that content in particular languages or dialects is difficult to assess, both when it comes to text and audio (like the current trend of using music such as *nasheeds* [50] to disseminate propaganda). They point to the limited usefulness of translation tools and highlight the need to work with specialised translators.

Arabic is given as a prime example of this challenge. On the one hand, the large volume of terrorist content distributed in Arabic makes it highly relevant for authorities who are detecting and assessing potential terrorist content. At the same time, experts from competent authorities and civil society / academia emphasise that Arabic is highly context-dependent, and words and phrases taken out of context could be easily misinterpreted or have different meanings in its various dialects. This can impact the accuracy with which authorities assess content.

> *Arabic is a difficult language to translate because one word can have a lot of meanings.*
>
> Competent authority expert

Interviewees across professional groups also highlight particular challenges when it comes to assessing content related to current events or sensitive political issues. They emphasise the

importance of context, saying that a particular piece of content can never be assessed in isolation, something that the regulation expressly recognises in Recital 11. Experts from competent authorities say that when they receive reports of alleged terrorist content from the public and other flaggers, these often relate to such complex topics and need to be very carefully scrutinised as they carry a high risk of disproportionately interfering with freedom of expression and freedom of thought, conscience and religion. This is also why human assessment based on experience is indispensable for their work and cannot be replaced by automated tools, most experts from competent authorities explain.

Recalling that the majority of authorities competent for issuing removal orders are law enforcement or intelligence agencies (see Section 1.2), some experts from civil society / academia express the view that such authorities might be naturally more likely to follow security-led approaches driven by their counterterrorism experience, without necessarily being equipped to fully assess the impact that ordering an expedited removal of content may have on freedom of expression and other rights. In this context, some mention that removal orders can amplify what they describe as inherent risks in counterterrorism, such as a risk that some authorities could use removal orders in accordance with their national priorities, with political motivations influencing what is labelled as terrorism, to target content that is considered undesirable and introduce state censorship over certain topics. Some interviewees warn about the risk of over-policing certain groups, with reference to existing research illustrating how certain communities can be particularly affected by the use of restrictive measures, especially after events such as terrorist attacks [51] .

> *If you keep noticing, as a member of a community, that certain expressions of solidarity or because you write in Arabic, are subject to wider restrictions and the community has been reporting those […] it is a very natural reaction you probably step back and restrict your participation in public life.*
>
> Civil-society/academia expert

Besides directly impacting the rights of users as providers of removed content, some civil society/academia interviewees express the view that the overuse of removal orders could lead people to abstain from publishing due to a fear of becoming persons of interest for counterterrorism authorities or having their profile and channels of communication blocked by HSPs (see also Section 3.1.3). Such a chilling effect could affect not only providers of content that has been taken down but also other users who see some types of discourse being censored, these civil-society/academia experts say. The risk of a chilling effect in the context of counterterrorism measures is recognised and addressed in various reports and other documents of international bodies [52] .

2.1.3 Uneven use of removal orders for different types of terrorism

Similar to Directive (EU) 2017/541, the definition of online terrorist content in the regulation does

not distinguish between different types of terrorism, such as – to use the classification applied by Europol – jihadist terrorism, right-wing terrorism, left-wing and anarchist terrorism, ethno-nationalist and separatist terrorism, and other forms [53]. At the same time, as indicated in past FRA research, the underlying focus of Directive (EU) 2017/541 and its transposition by many Member States has focused predominantly on jihadism and on the phenomenon of foreign terrorist fighters [54]. As the findings of this research show, this focus appears to be largely carried over and possibly amplified in the application of the regulation.

> *The vast majority of content [flagged by authorities to HSPs] is focused on Islamist extremist terrorism […] a lot of law enforcement across Europe is primarily focused on Islamist extremist terrorism.*
>
> Civil-society/academia expert

According to data provided by Europol, the vast majority (circa 84 %) of all removal orders issued via PERCI as of March 2025 targeted jihadist content. In comparison, only about 13 % targeted right-wing extremist content [55]. Interviews confirm this. While some experts from competent authorities state that they issue removal orders both on jihadist and right-wing (and potentially other) terrorist content, about half of those who have experience in issuing removal orders say they target predominantly or exclusively jihadist content.

Threat posed by jihadist and right-wing terrorist content

Europol data confirm the particular threat posed by jihadist terrorism in the EU. According to the European Union Terrorism Situation and Trend Report, 24 among the 58 terrorist attacks in the EU in 2024 were attributed to jihadist terrorism. These attacks were also the most lethal.

While the number of right-wing terrorist attacks is generally lower, the proliferation of right-wing online terrorist content associated with an increasing risk of radicalisation has been consistently reported. Tech Against Terrorism has highlighted its increasing presence across a wide range of online services, not only on mainstream social media platforms, but also on smaller alt-tech video-sharing or social media platforms, noting also its relatively lower removal rate by HSPs in comparison with jihadist content. Europol has repeatedly reported the increasingly young age of persons involved in online communities spreading right-wing terrorist content.

Interviewees offer several explanations for this. First, authorities deciding which content should be subject to a removal order are largely guided by international or national lists of dangerous organisations and individuals, such as the EU sanctions list [56], the UN list of designated terrorist groups [57] and the US list of foreign terrorist organisations [58]. While the definition of a 'terrorist group' applied by the regulation is not limited to such 'listed' organisations and Recital 11 of the

regulation states that a link to the EU list should be an 'important' (i.e. not necessarily decisive or definitive) factor, experts from competent authorities testify that content produced by or promoting such organisations – for example Daesh, al-Qaeda or Hamas – can be automatically considered to meet the definition of terrorist content. Experts from civil society / academia generally consider that the focus on listed organisations helps reduce the risk of affecting legitimate forms of expression. However, they highlight that these lists typically heavily focus on jihadist entities, while very few extreme right-wing or other terrorist entities have been designated.

Second, experts from competent authorities indicate that the definition of online terrorist content is better suited to jihadist content and the modus operandi of jihadist groups. Some state that the regulation captures jihadist content more clearly than other types, while others express the view that the regulation is intended to apply exclusively to jihadist content and content related to right-wing, left-wing and other types of terrorism falls outside its scope. Some civil-society/academia experts tend to agree that the definition is easier to apply to jihadist content and less suitable for capturing unaffiliated or unbranded content, while others speak of a certain lack of appetite or at least de-prioritisation by some authorities when it comes to right-wing or left-wing content, although it clearly falls within the scope of the regulation.

Third, more than half of the interviewed experts from competent authorities explicitly state that non-jihadist content is typically more difficult to assess. Right-wing content is often less clear-cut and more borderline, relying on memes and jargon, with right-wing extremists seemingly more aware of how to navigate the line between freedom of expression and illegal content. Based on their own experience of moderating content, an HSP expert likewise considers that terrorist content other than jihadism is more challenging to both detect and correctly assess. Some competent authority experts mention additional challenges when it comes to certain forms of right-wing content, such as antisemitic hate speech, blurred lines between extremism and terrorism and the fact that in certain jurisdictions, right-wing content might be easier to deal with under legislation against discrimination and extremism, not terrorism. Some interviewees across professional groups also mention the dynamic environment of right-wing terrorism, with less clear profiles that mix different ideologies from militant accelerationism and occultism to incels [59] ('pick and choose' or 'salad bar' approach) [60], along with the phenomenon of lone wolves and the frequent emergence of new groups.

> *I think [right-wing extremists] are well aware of the limits of the law and what they can do online. And it's all a joke and it's all memes […] so, yes, for the extreme right it's very difficult to prove a terrorist character.*
>
> Competent authority expert

The majority of interviewees from civil society / academia flag the overwhelming use of removal orders for jihadist content as posing certain issues. While recognising the threat from jihadist terrorism in the EU (see textbox 'Threat posed by jihadist and right-wing terrorist content'), some point to the wide proliferation of right-wing content online and the role that such content has played in triggering terrorist attacks. This raises the question whether the de facto focus on

jihadism and the limited ability to capture other content is compatible with the aim of effectively addressing the dissemination of diverse terrorist content [61].

On the other hand, the predominant focus on jihadism in the application of the regulation may result in a disproportionate impact on particular groups, notably Muslims and Arabic speakers. In this context, multiple interviewees point to the impact of the situation in Israel and Gaza following the attacks of 7 October 2023, which led to an increase in the volume of removal orders, predominantly targeting pro-Palestinian content. As reported in FRA's past research on EU counterterrorism legislation [62], such an overfocus associated with one type of terrorism might entail policing of certain content based on its association with a particular religion or language rather than an actual link with terrorism. This raises questions of compatibility with the principle of non-discrimination and freedom of expression and freedom of thought, conscience and religion.

Some experts from competent authorities acknowledge this risk and emphasise that potential jihadist content likewise requires careful assessment. Some offer examples of cases when establishing the terrorist nature of a piece of content required assessing its theological and historical context, interpreting references to the Qur'an and consulting experts on Islam. Posts related to current events are often highly contextual, one competent authority expert says, and authorities must be careful to correctly distinguish between expressions of sympathy with victims of armed conflicts or political views and content that amounts to expressing support for terrorism.

2.1.4 Impact of removal orders on HSPs, including small enterprises and microenterprises, and their freedom to conduct a business

Compliance with removal orders within the one-hour limit envisaged by the regulation can involve substantial investment and changes, especially in the case of smaller HSPs, potentially affecting their business model and, in terms of rights, their freedom to conduct a business. Concerns that the regulation puts a disproportionate administrative burden on smaller HSPs that might be unable to meet its requirements were also raised during parliamentary discussions in some Member States [63]. Challenges experienced by small and micro-sized HSPs when implementing the regulation and complying with the one-hour rule have also been reported in recent research [64].

Hosting service providers' responsiveness and the use of the EU Platform on Illicit Content Online (PERCI)

There is a broad agreement among experts from competent authorities that the PERCI platform, developed by Europol to support the application of the regulation, significantly facilitates their work, including the preparation of removal orders and their direct communication to HSPs.

While the use of PERCI is not obligatory under the regulation, some experts mention as a challenge that some large HSPs insist on the use of their own reporting templates, which are incompatible with PERCI, for receiving removal orders. This does not allow communicating all the necessary information, delays the receipt and execution of removal orders by HSPs, negatively impacts transparency and, potentially, hampers the scrutiny of cross-border removal orders, these experts say.

Experts from small-sized HSPs and civil-society/academia experts who have experience in capacity-building work with HSPs describe the one-hour rule as a practical challenge which only large HSPs – that can ensure 365-day, 24/7 availability of their staff – are in a position to meet. These experts report concerns shared by small and medium-sized HSPs about their ability to maintain their businesses, especially if the volume of removal orders increases. During the fieldwork it was stated that very practical factors need to be taken into account, such as the difference in working hours due to operating in a different time zone, and an HSP expert also questioned the application of the same approach to companies regardless of their size.

> *If you have a certain size of user base, e.g. 20 million, it should be tackled in a different way than […] a startup which has one or two people. […] Everything under 24 hours is very unlikely to be handled by startups.*
>
> HSP expert

According to some competent authority experts, responsiveness is not always determined by an HSP's size. One of these experts highlights that many small-sized HSPs have been very serious in their efforts to comply and to familiarise themselves with the new requirements, whereas even large platforms can have disproportionately small or unprepared teams.

Findings nevertheless show that understanding the requirements of the regulation and preparedness for the possibility of being targeted by removal orders is particularly important for smaller HSPs, and generally for all those having limited experience dealing with terrorist content. In this regard, experts from competent authorities state that they follow the procedure required by Article 3(2), providing those HSPs that have not received a removal order before with information at least 12 hours in advance. Only one mentions not having done so in the past due to the urgency of the removals ordered.

Promising practice: Supporting HSPs through terrorist content online capacity-building projects

Three EU-funded projects were implemented in 2022–2025 to support the implementation of the regulation among HSPs. Working together in the 'TCO cluster' to ensure complementarity, the projects ALLIES, FRISCO and Tech Against Terrorism Europe provided a mix of technical solutions, training and awareness raising tools, and networking mechanisms focusing on

small and medium-sized HSPs.

When it comes to more systematic awareness raising (see textbox 'Promising practice: Supporting HSPs through terrorist content online capacity-building projects'), however, small-sized HSPs often show limited interest and some of them appear to actively avoid involvement in such programmes, civil-society/academia experts involved in capacity-building efforts say. This may occur for a variety of reasons, for example because HSPs believe they do not fall within the scope of the regulation or do not consider themselves affected by terrorist content, but possibly also because they fear that participation in these trainings could be perceived by their users or authorities as admitting exposure to terrorist content, these experts say.

Finally, the impact of the regulation on HSPs needs to be seen in the broader context of EU regulatory efforts (and, for some HSPs, regulations emerging outside the EU). In this respect, a number of interviewees emphasise the interplay with the DSA. Some civil-society/academia experts express concerns over certain incoherence between the two frameworks, highlighting the more nuanced requirements and stronger safeguards present in the DSA (see textbox 'Obligations under the regulation and the DSA'). The prevailing view among civil-society/academia experts, confirmed by some HSP experts, however, is that the DSA has by far eclipsed the regulation in terms of HSP compliance focus, due to its broader scope and more extensive requirements. In this context, an interviewee notes that this focus on the DSA can negatively impact the awareness of the regulation among smaller HSPs.

> *From a company perspective, there is a lot of legislation fatigue. Companies try to keep up to speed with each of these [pieces of EU legislation]. Even the TCO [regulation], which is a relatively simple piece of legislation, has so many implications, and that is nothing compared to the DSA.*
>
> Civil-society/academia expert

Obligations under the regulation and the DSA

Covering illegal online content more broadly, the DSA does not specifically define terrorist content. Unlike in the regulation, HSP obligations under the DSA depend on the size and reach of the platforms, being most comprehensive for very large online platforms. While the DSA envisages the use of removal orders, it does not contain a specific deadline, instead requiring platforms to comply without undue delay. At the same time, the DSA includes broader responsibilities for HSPs in actively preventing the dissemination of illegal content on their platforms, and the transparency reporting obligations encompass a much wider range of content.

Source: Tech Against Terrorism Europe, 'Digital Services Act & Terrorist Content Online

Regulation comparison', Tech Against Terrorism Europe, 2025.

2.2. Referrals and their interplay with removal orders

Prior to the regulation, referrals served as the main tool used by internet referral units of Member States and Europol to tackle suspected terrorist content. Available statistics show that the availability of removal orders has not changed this, as referrals continue to significantly outnumber them [65] .

With the exception of those made by Europol, the use of referrals is based on national law. The legislative proposal put forward by the Commission originally sought to regulate the use of referrals alongside removal orders, prompting questions of accountability for takedowns based on referrals and calls for clear rules distinguishing when to use each tool [66] . In the adopted text, only removal orders were maintained in the regulation, while referrals remained unregulated.

Findings show that the interplay between the use of removal orders and referrals may have an impact on freedom of expression and information (Article 11 of the Charter) and freedom to conduct a business (Article 16 of the Charter). Furthermore, it relates to the broader transparency issues surrounding the application of the regulation.

2.2.1 Lack of clarity, foreseeability and transparency in the use of referrals and removal orders

There is a considerable diversity of approaches among Member States when it comes to the use of removal orders and referrals. Most continue to rely primarily on referrals and use removal orders only in particular circumstances, typically in cases of urgency (e.g. content posing an imminent threat to life or likely to go viral) or in cases where the HSP in question is known not to respond to referrals. Others use exclusively either referrals or removal orders, while others may use one tool or another depending on the circumstances.

> *For the Member States where both options are possible, the voluntary cooperation prevails over imposing the law.*
>
> Competent authority expert

Findings show that the absence of clarity of what content should be targeted, respectively, by removal orders and referrals, is a major concern among experts from civil society / academia and some HSP experts.

One risk lies in the uneven and distorted application of the regulation, where the same content is dealt with differently. If competent authorities in different Member States apply different tools to the same type of content, this increases the likelihood that some content that is terrorist content

remains online while some content that is within the margins of freedom of expression is taken down.

Furthermore, this situation blurs the distinction between the two tools and their purposes – removal orders as enforceable tools through which authorities clearly identify content as illegal and assume responsibility for potential errors, and referrals as a way of flagging content that authorities indicate an HSP should assess against its terms and conditions and, potentially, remove at its own responsibility. Given that referrals are not formal legal requests, there are no safeguards accompanying their use. While the regulation introduces specific provisions to safeguard fundamental rights of content providers and HSPs – including the scrutiny of cross-border removal orders, remedies, information obligation towards content providers, transparency reports and the right to have content reinstated – none of these apply to referrals. For example, individuals whose content is removed following a referral must rely on the HSP's regular complaint avenues (see Section 3.2.3).

A number of experts from civil society / academia, and some experts from competent authorities, express the view that referrals could be regarded as going against the spirit and underlying purpose of the regulation to establish a mandatory, urgent and transparent process for the removal of online terrorist content. Some experts from competent authorities note the absence of a legal basis for issuing referrals under their national law. Others state that terrorist content online, when encountered, should be speedily removed to prevent dissemination, something that only removal orders can ensure.

> *Ultimately, if you want to comply with the spirit of the TCO regulation and also with your obligation to have terrorist content removed, removal orders are the way to go – especially if the content is very clear.*
>
> Civil-society/academia expert

In contrast, the majority of interviewed experts from competent authorities continue to use referrals as the go-to tool. These findings show a common belief among competent authorities that referrals work well and are a more agile tool than removal orders. These experts report that HSPs usually act upon referrals within an acceptable deadline, generally up to 24 hours. They also require less time and effort than removal orders. This relates to the formal requirements for issuing removal orders, for example a statement of reasons explaining why the content is considered to be terrorist content (Article 3(4)(b)). As stated by one competent authority expert, this can be straightforward for clear-cut content, but other content requires thorough analysis. Moreover, in some Member States, removal orders require the scrutiny or consultation of other authorities or are issued or approved by other bodies, which entails having processes in place and sufficient time. This makes the use of referrals more feasible and attractive for some authorities.

> *[Removal orders] are a tool we only use from time to time […] We understand it should be like this, given that the referral system generally*

works really well.

Competent authority expert

Some interviewees from competent authorities also appreciate that referrals can capture a broader range of content. Namely, they can address any type of content incompatible with terms and conditions, leading to a takedown even if the HSP does not assess the content as terrorist content. This again raises questions, however, about the clarity of when referrals should be used and the manner in which they may be interpreted by an HSP.

Interestingly, while some experts from competent authorities and civil society / academia indicate that HSPs have a preference for the legal clarity provided by removal orders, half of the interviewed experts from HSPs, representing companies of different sizes, express a preference towards referrals as a tried-and-tested tool. These experts say that removal orders actually slow down the process due to being more formal than referrals and generally consider them unnecessary. Other HSP experts consider that they increase the risk of over-removal due to the one-hour deadline to remove content.

Issues associated with the interplay between removal orders and referrals are difficult to address due to the lack of comprehensive information about their use, including the types of terrorist content targeted by them. The transparency obligation of Member States under Article 8 of the regulation includes only basic information about removal orders and no information about referrals. While the transparency reports of some Member States provide robust information going beyond the minimum requirements of the regulation (see textbox 'Promising practice: Supporting transparency through enhanced reporting'), others have limited information value.

Promising practice: Supporting transparency through enhanced reporting

Transparency reports by some competent authorities offer additional information that, while not strictly required under Article 8, provides further transparency about the application of the regulation. In Germany, for example, transparency reports include information about the number of referrals and the response rate of HSPs. In Spain, the type of terrorism and the HSPs addressed are among the information provided.

Both HSP and civil-society/academia interviewees argue that without comparable data about how Member States apply the regulation, it is currently difficult to assess its full impact and understand the expectations of the authorities, for instance when it comes to content related to certain topics or events. The current lack of information limits the accountability for the proper application of the regulation and blurs the responsibility for potential adverse impacts on various fundamental rights, these experts say. Data on referrals and more detailed data on removal orders and their reasoning would allow experts to identify similar cases and detect trends, helping to reveal potential tendencies towards over-removal or politicising content removal. It could also help raise awareness and might motivate HSPs and content providers to challenge and appeal

removal orders where relevant, some civil-society/academia experts indicate.

Such a breakdown would also offer much-needed clarity about the use of removal orders on the one hand, and referrals on the other, and their respective use for particular types of terrorist content. As highlighted by multiple civil-society/academia experts, this would be particularly important given the persisting disproportion between the use of referrals and removal orders.

2.2.2 Impact of removal orders on the voluntary nature of referrals

A number of interviewees, including experts from competent authorities, consider that HSPs have become more responsive to referrals since the entry into force of the regulation. While other factors may contribute to this, including the regulation's broader impact on increasing HSPs' awareness and improving their content moderation work, interviewees highlight that the threat of obligatory removal orders in combination with penalties acts as a strong incentive. In fact, several experts from competent authorities highlight this as a benefit of such a hybrid system, where referrals are favoured but another, more severe, instrument is known to be available. One such expert states that this is how they perceive the aim of the regulation – incentivising HSPs to remove content already upon receiving a referral, so that a removal order would not be necessary.

> *The aim of the regulation is to get HSPs used to removing content already based on a referral, so that a removal order would not have to be used. Experience from other Member States shows that in 90 % of the cases, content is removed, so the whole process seems to work.*
>
> Competent authority expert

This interplay between referrals and removal orders, however, can also impact the scrutiny of content by HSPs and, potentially, increase the risk of removal of legitimate content. In accordance with the relevant guidelines of the Council of Europe, public authorities should avoid any activity that exerts pressure on internet intermediaries through non-legal means [67] . The knowledge that a removal order can follow in case the content is not taken down based on a referral may diminish the voluntary nature of referrals and de facto restrict HSPs' freedom to assess content, also given the potential consequence of being ordered to implement specific measures after receiving two or more removal orders (see Section 3.2).

Some HSPs may be inclined to trust that authorities have done their due diligence and remove content rather than review it, some experts from civil society / academia and also competent authorities say. This might particularly be the case for HSPs that lack large moderation teams or specific subject matter experts on terrorism. It may also pressure HSPs to process referrals quicker and further reduce the time available for reviewing the content, some civil-society/academia experts warn, pointing to the fact that HSPs typically process all law enforcement requests through expedited channels. Considering the volume of referrals issued by competent authorities in comparison with that of removal orders, this reliance on referrals,

combined with the threat of removal orders, can therefore impact the rights of users and companies.

> *Now that you have the threat of removal orders in the background […] platforms are a lot more likely to listen to the informal referral first. The threat of formal orders and the threat of sanctions has actually created a lot more 'voluntariness.' […] It's voluntariness in a certain sense because you've got the big stick being waved if someone doesn't voluntarily cooperate.*
>
> Civil-society/academia expert

In this context, some experts from civil society / academia comment more broadly on referrals as a tool transferring responsibility from competent authorities to HSPs, bypassing the accountability of competent authorities that initiated the process. These experts express doubts about whether private companies are better positioned to assess potential terrorist content than public authorities, citing several reasons. First, HSP terms and conditions are not subject to the same requirements as national legislation and lack transparency, legal clarity and fundamental rights standards. They also vary considerably among platforms. Second, HSPs might not necessarily have the necessary expertise and training to assess the terrorist nature of content and the impact of the takedown on rights. Finally, some civil-society/academia experts emphasise that due to the threats associated with terrorist content, but also due to reputational risks and potential economic consequences, many HSPs tend to review alleged terrorist content less rigorously than other illegal content, and err on the side of over-enforcement rather than risk its under-enforcement.

2.2.3 The differential treatment of HSPs

According to the Commission's implementation report, by the end of 2023, competent authorities issued removal orders to 13 HSPs [68] . HSP transparency reports indicate that while additional companies have been subject to removal orders throughout 2024, the list remains relatively modest and the majority of orders target a small number of HSPs, focusing on social media platforms [69] .

Findings show that several factors play a role in this regard. Already at the stage of detecting potential terrorist content, authorities are more likely to focus on those HSPs where they know they are more likely to find terrorist content, particularly social media. Some competent authority experts specifically acknowledge that they prioritise larger social media platforms as they offer a 'bigger pool of fish' compared to smaller platforms, making the best of their limited resources.

When it comes to deciding between sending a referral and issuing a removal order, referrals continue to be prioritised where authorities and HSPs already have established relationships of effective cooperation in place. In this context, an expert from a competent authority shares an example where an otherwise cooperative HSP expressed concerns over the feasibility of the one-hour rule, which prompted the authority to approach it with referrals first. Another competent

authority expert states that referrals also help HSPs to better develop their own content moderation, which is important in view of the vast amount of online content.

However, this approach is not necessarily used across the board. While authorities may send referrals to small or medium-sized HSPs to avoid overrunning their moderation teams, they can opt to send removal orders to bigger HSPs that are deemed more likely to have all the channels and processes in place to implement them.

As some experts from competent authorities and civil society / academia explain, active engagement by HSPs makes it easier for authorities to issue removal orders. Some platforms, on the other hand, hesitate to cooperate with law enforcement or are difficult to reach. This is the case of many HSPs located outside the EU that have not fulfilled the obligation of Article 17 to designate a legal representative. Such HSPs are less likely to respond to removal orders and might require intensive follow-up work. This reduces the incentive for competent authorities to issue removal orders to such HSPs in the first place.

> *Small [HSPs] have no knowledge at all about the regulation, and it's difficult to reach them because you have no awareness of their existence at all. […] It's difficult to make the internet a safer place when you have no clue who the actors are.*
>
> Competent authority expert

More work is also needed on mapping the HSP landscape, even within the EU, some experts from competent authorities acknowledge. Findings show that regulatory bodies that are often also responsible for the implementation of the DSA do not necessarily have an overview of companies qualifying as HSPs under the regulation, which de facto excludes some HSPs from being targeted by removal orders or referrals.

> *When you look at the list of platforms that have received removal orders, […] they were mostly big platforms or what I would call the 'usual suspects.' […] What I would see as quite a glaring gap in the enforcement is smaller platforms that are less well known but actually are hosting vast amounts of content.*
>
> Civil-society/academia expert

While these approaches might reflect the working methods of competent authorities and allow them to leverage their resources, they also leave room for arbitrariness and raise questions of proportionality and transparency. Freedom to conduct a business for certain HSPs may be affected more than others and the legal provisions of the regulation, including its safeguards, may be applied differently. Furthermore, the focus on certain HSPs risks diverting attention away from other, less obvious yet relevant platforms, potentially negatively affecting the effectiveness of efforts to address the dissemination of terrorist content online.

3. The regulation and HSP content moderation

The regulation complements efforts of HSPs to address the proliferation of terrorist content based on their own terms and conditions, supported by EU initiatives such as the EU Internet Forum and the Code of Conduct on Countering Illegal Hate Speech Online. In fact, the vast majority of terrorist content, especially on large social media platforms, is detected by HSPs' own detection tools and subsequently removed on the basis of such terms and conditions (community guidelines, terms of service, etc.) rather than being triggered by law enforcement or other government requests [70].

In general, the regulation does not regulate the content of these HSP moderation policies. However, it interacts with them at several levels. Recital 5 underlines that HSPs have 'particular societal responsibilities to protect their services from misuse by terrorists and to help address terrorist content disseminated through their services online, while taking into account the fundamental importance of the freedom of expression.' This complements obligations of HSPs to act with due regard to fundamental rights of the recipients of their services under Article 14 DSA and, for very large online platforms and very large online search engines, to assess the risk for fundamental rights stemming from the design, functioning and use of their services, including when using algorithmic systems, under Article 34 DSA. When setting out their transparency obligations under the regulation, Article 7 also requires HSPs to report on their own content moderation measures.

Furthermore, in accordance with Article 5, when a competent authority decides that an HSP is exposed to terrorist content, for example due to having received two or more removal orders in 12 months, such an HSP must enhance its content moderation and implement specific measures to prevent the dissemination of terrorist content. While the HSP retains discretion in choosing the measures, they may involve technical means to identify and expeditiously remove content, including automated tools that must be subject to human oversight. The specific measures must meet the requirements set out in Article 5(3). Besides effectiveness, this includes a targeted and proportionate nature; taking full account of the rights and legitimate interests of the users, in particular users' fundamental rights concerning freedom of expression and information, respect for private life and protection of personal data; and diligent and non-discriminatory application. Article 5(5) in conjunction with Recital 24 requires HSPs to report their measures to competent authorities for assessment, which should also cover the fundamental rights impact. This mechanism embodies the positive obligation of the Member States to secure the effective exercise of fundamental rights and prevent fundamental rights violations, including by providing an oversight over the application of the specific measures by HSPs under the regulation [71]. HSPs also have the possibility to request a review of the decisions related to being exposed to terrorist content and specific measures (Article 5(7)) and challenge them in court (Article 9).

Article 10 of the regulation also requires HSPs to set up effective and accessible complaint mechanisms for content providers whose content has been removed due to specific measures and ensure that such complaints are dealt with expeditiously.

This chapter does not analyse in detail companies' content moderation policies. Instead, it focuses on some of the key fundamental rights issues arising in that context, including the shift towards automation and the limits of human moderation, and the resulting risk of the disproportionate impact on specific groups and content. Against this backdrop, it looks at how the regulation interplays with HSP content moderation and, in particular, how specific measures might further aggravate these challenges. When it comes to describing the impact of HSP policies on issues, the chapter relies strongly on examples related to Meta as the transparent operation of its Oversight Board offers comparatively more insight into its operations than what is available for other HSPs [72] .

Summary of findings: The regulation and HSP content moderation

- The regulation has contributed to an increased focus of HSPs on addressing terrorist content. This, however, includes growing reliance on automated tools to detect, assess and remove content. Concerns arise over the reliability of automation in combination with the limitations of human review and oversight.
- Furthermore, similar to competent authorities, HSP content moderation relies on international and national lists of dangerous organisations and individuals that focus heavily on jihadist entities. Together with the issues related to automation, this puts legitimate content related to particular topics or posted by users from a particular region or speaking a particular language at a disproportionate risk of over-removal, notably impacting Muslims and Arabic speakers. This goes hand in hand with the risk of a chilling effect on freedom of expression and other rights of people belonging to certain groups. Right-wing terrorist content, on the other hand, appears to be under-moderated by platforms, indicating different standards in the protection of free speech.
- Transparency reporting by HSPs does not provide sufficient information to measure and address the risk of HSPs over-blocking content or to enhance accountability.
- In the context of specific measures, and to assist the correct application of the regulation in practice, more guidance appears to be needed on how to determine when an HSP can be considered exposed to terrorist content and what specific measures to apply. Concerns arise that this lack of clarity can contribute to HSPs implementing intrusive specific measures, leading to the over-removal of legitimate content or measures de facto constituting indiscriminate surveillance of content.

3.1 Fundamental rights impact of HSP content moderation policies

Findings from the research indicate that the regulation affects how HSPs approach content moderation, going beyond the direct impact of individual removal orders.

Interviewees across professional groups acknowledge that addressing terrorist content has been

high on the list of priorities for many large HSPs for some time, as evidenced by voluntary initiatives such as the GIFCT and responses to events such as the Christchurch terror attack, and that most companies are willing to counter terrorist use of their platform. At the same time, a number of experts from civil society / academia, along with competent authorities, consider that the regulation and the discussions surrounding its adoption have been an important factor in promoting HSPs' enhanced focus on terrorist content in recent years. While this can be considered a positive development, it also entails an increased use of automated tools to detect terrorist content and a general tendency to prioritise compliance with regulatory frameworks and government requests and err on the side of over-blocking content, avoiding the risk of penalties and ideally exposure to removal orders, which carry the risk of having to implement specific measures (see Section 3.2). Experts from civil society / academia, including those with content moderation experience, recall that major HSPs stepped up their moderation efforts at the time when the regulation was proposed, in an apparent hope to pre-empt its adoption.

> *I believe that the platforms were thinking: 'If we do this voluntarily, we can avoid the regulation.'*
>
> Civil-society/academia expert

Some competent authority experts emphasise that, in their view, shaping how HSPs approach moderation of terrorist content is one of the underlying aims of the legislation.

> *The regulation has helped in improving the moderation by service providers, […] so that providers learn and know we are putting some pressure on them, that they start protecting themselves.*
>
> Competent authority expert

Content moderation by HSPs necessarily differs from the detection of terrorist content conducted by competent authorities. HSP terms and conditions are considerably broader in their scope than the regulation, prohibiting a range of content that may include illegal and 'borderline' content that may, depending on the HSP, cover hate speech, violent and graphic content, harassment and even some types of disinformation [73] . At least in the case of major HSPs, content moderation by companies operates on a considerably larger scale in terms of the volume of content processed and geographical scope. At the same time, it is based on enforcing terms and conditions that are not subject to the same standards and degree of scrutiny as national or international law. From this perspective, effective content moderation by HSPs is a prerequisite for successfully addressing the proliferation of terrorist contentonline. At the same time, incentivising HSPs towards stricter content moderation can generate a significant impact on fundamental rights, without safeguards equivalent to those which apply to competent authorities in the context of the regulation.

This impact includes in particular freedom of expression and information (Article 11 of the Charter), along with respect for private and family life (Article 7 of the Charter), freedom of

thought, conscience and religion (Article 10 of the Charter), freedom of assembly and of association (Article 12 of the Charter), freedom to conduct a business (Article 16 of the Charter), non-discrimination (Article 21 of the Charter) and the right to an effective remedy and a fair trial (Article 47 of the Charter).

3.1.1 Risk of over-blocking due to reliance on automated tools

Automated tools such as machine learning models and hash matching (see textbox 'Automated tools for the identification of terrorist content') allow HSPs, in particular large social media platforms, to detect and remove large amounts of illegal content [74]. Although HSP experts highlight that potential terrorist content detected through such means is generally not taken down without being first assessed by a human moderator (see Section 3.1.2), the findings confirm a widespread trend towards entrusting more content moderation to automation and reducing the role of human review or oversight. Some interviewees note that the regulation, due to its focus on quick removal of content and the reputational risks associated with being labelled as hosting terrorist content, further incentivises the use of such automation.

Automated tools for the identification of terrorist content

- **Machine learning models** are developed by using available content data (often text data in this context) to identify patterns and correlations in the data. These patterns are used to classify whether the content fits one of the categories of data. These patterns can be updated and improved by adding more data at a later stage.
- **Hash matching** technology uses a mathematical algorithm to create a unique signature (hash) for images and videos. The hash is then compared to a database of previously identified terrorist content.

Source: Macdonald, S., Mattheis, A. and Wells, D., Using artificial intelligence and machine learning to identify terrorist content online, Tech Against Terrorism Europe, 2024, pp. 15–22.

Findings indicate serious concerns over the reliability of automated tools, something that FRA has flagged in the context of its work on algorithmic bias [75]. Interviewees underline that while machine learning detection and classification models have improved considerably over recent years, their quality tends to be overestimated. Due to the scale of operation of major HSPs, even a small error rate can have major consequences and affect the freedom of expression and information and freedom of thought, conscience and religion of a large number of people globally.

> *In my experience, there is a lot more faith in automation than is warranted. [Automated content moderation] is really still a developing field, and yet we already have a regulation that encourages that.*

The nature of the tools and the quality of data to train them both play an important role. Compiling comprehensive datasets of sufficient quality for training machine learning tools remains a challenge, especially outside major languages. Many interviewees, including those with experience working on content moderation, refer to difficulties with African or Asian languages, for which less training data is available, languages with multiple dialects or languages written in non-Latin script, with which the models have difficulty working. In this context, civil-society/academia experts call for more transparency of the use of automated tools, their accuracy and the nature of the datasets.

FRA activity: Challenges and limitations of hate speech detection and AI-supported content moderation

FRA's work on the content moderation of hate speech shows that challenges related to detecting and assessing content are not limited to terrorist content. Based on the data collection of hate speech incidents on selected online platforms, FRA showed that hate speech easily slips through content moderation systems. Most notably, hate targeting women is very easy to find online using selected keywords. Assessing if certain content falls under the definition of hate speech, be it illegal hate speech or hateful content that is prohibited under a platform's terms and conditions, is also challenging. This is not only because the definitions in the law may not provide the necessary clarity, but also because decisions based on the content of a post alone, without context and further assessments, are difficult. The requirements and safeguards included in the DSA can be used to mitigate disproportionate over- and under-removal of hate speech.

What is more, the use of artificial intelligence (AI), most notably machine learning, to support and partly even automate content moderation has proliferated in recent years. In the first half of 2025, providers of online platforms submitted over 10 billion statements of reason to the DSA Transparency Database, indicating measures taken on online content, mainly disabling access to content or removals. More than half of these measures were fully automated. While using automated tools to detect certain content for action may be needed to support content moderation efforts, it comes with additional challenges, most notably biased algorithms that show higher error rates for content linked to certain groups compared to others.

FRA's report on bias in algorithms highlights that offensive speech detection algorithms easily overreact to certain words, such as 'Muslim' or 'Jew', which may lead to the over-removal of content mentioning these words. On the other hand, these results also show that other content that avoids using certain terms may easily slip through automated detection systems. As a consequence, before using any AI tools for supporting or even fully automating content moderation decisions, thorough checks and tests need to be implemented to assess whether or not such tools are fit for purpose. As biases may also increase over time in machine learning tools, such checks need to be repeated.

Sources: FRA, Online Content Moderation – Current challenges in detecting hate speech, Publications Office of the European Union, Luxembourg, 2023; FRA, Bias in Algorithms – Artificial intelligence and discrimination, Publications Office of the European Union, Luxembourg, 2022; European Commission, 'DSA Transparency Database', European Commission website.

> *One problem that we have is that we don't know the type of content [HSPs] block, we cannot know how much legitimate content is taken down based on their own assessment criteria.*
>
> Competent authority expert

Automated tools are less accurate when working with some types of content. Videos, in particular livestreamed ones, have a higher inaccuracy rate than images. Text and speech carry the highest risk of false positives (content wrongly flagged as terrorist content) as machine-learning classification does not take context into account, which makes recognising non-violent terrorist content, such as propaganda, or distinguishing an actual call to violence from sarcasm or historical references, difficult for automated tools. According to experts with content moderation experience, this sometimes results in the removal of news reports or the suspension of social media accounts for discussing current political topics, limiting people's ability to freely discuss current events and share non-harmful content.

If a detection model is based on the name of a terrorist organisation, for example, any content that references that organisation (e.g. reporting or expressing views on the Taliban takeover in Afghanistan or the activities of Hezbollah in Lebanon) may be flagged by the algorithm to a human moderator as glorifying terrorism. Unless the human moderator recognises this as a false positive case (see Section 3.1.2), the content will be taken down.

Content identified based on hash matching as known terrorist content or an altered version of it is taken down automatically. Some interviewees express concerns that hash detection cannot distinguish when content is used for legitimate purposes (e.g. academic research or journalism) and that sharing hashes among HSPs (e.g. in the context of the GIFCT Hash Sharing Database) raises issues of transparency and accountability for possible mistakes.

> *Typically, content goes via humans, but some goes automatically, via tools. If someone is trying to reupload the same content, or very similar content after they altered [the original], it is prevented from being uploaded.*
>
> HSP expert

While content detected through machine learning models typically undergoes some form of human review, some interviewees with content moderation experience note that this is not always the case. If the tool, based on certain pre-set phrases or other parameters (for example, the

presence of a headless body in an image), assesses the content as sufficiently clearly violating the HSP's terms and conditions, the content can also be taken down automatically.

Furthermore, even if human review is involved, in some cases, it might only take place *ex post*. As an example, an interviewee with content moderation experience refers to cases of particular high-risk events (e.g. public protests), where all content assessed by automated tools as potentially problematic is preventively removed pending human review, which might take as long as 24 hours. This can have a particular impact on material expressing polemic or controversial views, the coordination of political activities, etc., affecting not only freedom of expression and information but also freedom of assembly and association.

3.1.2 Limitations of HSP human moderation

The limits of automation demonstrate that a thorough human review of content detected by automated tools is necessary to avoid over-blocking some content [76] . However, as a number of interviewees point out, the trend towards more automation has gone hand in hand with reduced investment in human moderation teams characterised by lay-offs and outsourcing driven by economic considerations, affecting the effectiveness of human oversight of automated decisions.

Interviewed experts from large HSPs state that their companies have robust human moderation in place where experts with different specialisations deal with terrorist content. Smaller companies might rely on a single person covering terrorism among other tasks. Civil-society/academia interviewees observe that the quality and capacity of content moderation teams differ significantly based on company size and their focus on terrorist content, but that even HSPs with sufficient resources might lack appropriate human rights expertise. According to some interviewees, investment in different languages likewise varies partly due to the regulatory pressure to moderate content coming mostly from Europe and the United States, aggravating the uneven performance of automated tools in different languages.

Importantly, while content flagged by authorities is routed directly to specialist in-house teams, content detected by automated tools – i.e. the overwhelming majority of content flagged as potentially terrorist content – is assessed by frontline moderators. Interviewees point to several factors that significantly reduce the effectiveness of human review as a safeguard to address over-blocking.

While the training of frontline moderators in large HSPs typically also covers terrorism, the training is usually limited to recognising obvious signs of terrorist content, without considering cultural and religious specificities and other nuances that help to safeguard free speech. Where detailed internal guidance exists for how to assess different types of content, it might be only available in English and not the languages moderators work with.

In addition, frontline moderation is increasingly outsourced. Interviewees point out that outsourced moderators work under particular time pressure, with strict quotas not only on how many pieces of content they need to process but also on how many cases they can escalate to in-

house content moderation teams in case of doubt. Making a decision whether content flagged by automated tools is indeed terrorist content within the available 10–20 seconds might be possible for simple cases, interviewees say, but not for more complex scenarios involving local context or a dialect a moderator is not familiar with. Lack of systematic oversight over frontline moderators also leaves room for biases and subjective decisions, which tend to err on the side of removal. The online response to events such as the Israeli-Palestinian conflict after 7 October 2023 can overwhelm moderation systems easily, one interviewee with content moderation experience says, turning moderation into a numbers game where moderators cannot keep up with the amount of content and might remove content nearly automatically.

> *Moderators are treated somewhat like AI. They're given a target number of things to do in an hour. There are few allowances for a break or to make a mistake […] One can only escalate one case this hour so they will just be going to click this button that says 'Remove' and move on, because that's the safer thing.*
>
> Civil-society/academia expert

Pointing also to known testimonies of whistleblowers and studies on the conditions of human moderation in large HSPs [77], civil-society/academia experts state that while the conditions for in-house moderation teams have somewhat improved, outsourced moderators continue to be treated as an extended form of automation and a disposable resource in terms of low wages, poor working conditions, psychological harm due to exposure to often highly traumatising content and lack of support. Besides a very real impact on the fundamental rights of moderators themselves, this may also have consequences for freedom of expression and other rights by affecting the quality of moderation and increasing the likelihood of the over-removal of content. Given these shortcomings, some interviewees question the push for human moderation over automation and emphasise the need to first ensure adequate human resources, better working conditions and guidance for moderators.

> *This over-flagging, so false positives, is slightly higher by the automatic machine learning model, but the human moderators also happen to have a quite a lot of work, so it happens with them as well.*
>
> Civil-society/academia expert

3.1.3 Disproportionate impact of HSP content moderation on certain types of content and particular groups

While the issues with automation and human moderation of suspected terrorist content increase the risk of over-blocking content across the board, findings show that they have an impact on certain types of content and groups in society more than on others – a challenge explored in the

context of assessment of content by competent authorities in Chapter 2. When it comes to content moderation by HSPs, findings show a widely shared concern that legitimate content related to particular topics or posted by users (content providers) from a particular region or speaking a particular language is at a disproportionate risk of over-removal. This amounts to a risk of discrimination based on, among other things, ethnic origin, language, religion or belief, or political opinion.

In terms of languages, Arabic, due to its non-Latin script and multiple dialects that might use the same terms differently, is considered a particularly vulnerable language in content moderation. Interviewees point to, among other examples, a human rights review contracted by Meta to assess the impact of its moderation policies and activities during the 2021 events in Israel and Palestine [78] (see textbox 'Discriminatory impact of HSP content moderation – example of Meta'). Interviewees with content moderation experience highlight that these issues exist across the industry and that other HSPs likewise encounter lower accuracy rates for speakers of certain dialects of Arabic. Lack of attention to the cultural context of particular terms in certain languages can generate lots of false positives and lead to over-removal, as shown by the policy advisory opinion of the Oversight Board, which found the company's approach to moderating the term *shaheed* ('martyr' in Arabic) to be overbroad and disproportionately restrict freedom of expression and civic discourse.

Discriminatory impact of HSP content moderation – example of Meta

At the recommendation of its Oversight Board, Meta requested an independent human rights due diligence of the impact of its policies during the May 2021 crisis in Israel and Palestine. The exercise provided several examples of HSP over-moderation of content with a disproportionate impact on specific groups.

Given the similarity with the name of the Al Aqsa Brigade, a listed terrorist organisation, the hashtag #AlAqsa was mistakenly added to Meta's block list, hiding it from search results. This, however, also affected any posts referring to one of the holiest sites in Islam, the Al-Aqsa Mosque.

While content in Hebrew experienced relative under-enforcement, Arabic content was over-removed as machine learning classification for this language appeared to have higher error rates for Palestinian Arabic. Furthermore, Arabic content flagged for review by automated tools may not have been routed to moderators speaking the specific dialect.

Source: Business for Social Responsibility, 'Human rights due diligence of Meta's impacts in Israel and Palestine in May 2021', 2022.

Similar to competent authorities, HSPs rely on international and national lists of dangerous organisations and individuals when detecting terrorist content online [79]. As outlined in Chapter 2, these lists are heavily skewed towards jihadist entities, with far fewer designations of

right-wing extremist and other non-jihadist organisations and individuals. Individuals living in, or posting about, the situation in regions where organisations present on these lists play a particular role (e.g. refugees from Afghanistan or Syria living in the EU), and in particular Muslims, face an increased likelihood that their content will be either automatically blocked by automated tools or scrutinised and potentially wrongly assessed by a human moderator and removed.

> *Whenever content is referring to a certain area, it can be unclear if it's glorification or if the person lives in the area and is just reporting and making observations of that area like in the Taliban region. [The company] errs on the side of over-enforcement rather than under-enforcement.*
>
> Civil-society/academia expert

Researchers and journalists can be likewise affected. In fact, civil-society/academia experts explain that the work of actors documenting human rights abuses has been impacted by HSP takedowns, as this is content that is indeed related to terrorism but has important documentary value and potential to bring to justice perpetrators of war crimes and genocide [80].

Some civil-society/academia interviewees say that the lack of attention paid by HSPs to right-wing extremist content is worrying, both given its radicalising potential and the fact that it is significantly more relevant in some parts of Europe than jihadism [81]. In this context, some interviewees highlight the EU–US divide in approaching free speech and the growing political acceptance of far-right views, both as an explanation for the under-moderation of right-wing extremism online and as a challenge for the near future.

The majority of experts from civil society / academia also highlight that the over-moderation of online content by HSPs can contribute to a chilling effect on rights, in particular freedom of expression and freedom of assembly and association, as people from communities that feel over-moderated withdraw from public debate and restrict their involvement in solidarity movements and activism (see also Section 2.1.2). While such an effect is hard to measure, some civil-society/academia experts refer to testimonies by migrant communities in Member States stating that they refrain from posting certain content, resort to measures to bypass moderation (e.g. by slightly altering texts, using different expressions and symbols) or restrict their involvement in solidarity movements and activism, due to a fear of being perceived as supporting terrorism [82].

> *People are absolutely self-censoring, including in the context of what is currently happening in Gaza and Lebanon where it is difficult to discuss certain topics without mentioning, e.g. Hezbollah. Particularly in these emergency situations, many people are scared about losing access to their accounts and are really limiting what they say. In this way, we are already seeing a chilling effect among specific communities.*
>
> Civil-society/academia expert

3.1.4 HSP transparency reporting as a missed opportunity

Findings show that transparency reporting by HSPs under Article 7 of the regulation, including statistics on the removal of content under their own terms and conditions, complaints and reinstated content, does not provide sufficient information to measure and address the risk of HSP over-blocking and to enhance accountability.

> *In transparency reports, intentionally, the numbers are presented in such a way that you have numbers, but it is really hard to say [what they really mean]. There is obviously granularity, but they hide behind the global average.*
>
> Civil-society/academia expert

According to civil-society/academia experts, data in these transparency reports lacks granularity and comparability across the industry. In many cases, the data does not clearly show what content has been taken down on terrorist grounds (rather than based on broader categories like 'public security' or 'violent content'), how many takedowns resulted from own detection and how many from content flagged by referrals. It also does not disaggregate data by criteria such as region or language. Furthermore, not all HSPs issue these reports, and when they do, they do not necessarily meet the requirement of making them public, for example making them only accessible to their own users instead.

Promising practice: Systematically monitoring the impact of own content moderation policies on removals and complaints

Some HSP experts expressly recognise the need for collecting and analysing data to counter the risk of over-blocking and disproportionate impact on certain groups of users, and the need for human rights assessments. One company, for example, systematically monitors changes in removals and appeals (complaints) to see if there is a need to reassess its content moderation policies.

> *We are very closely monitoring those metrics. If we see a spike in enforcements or a big spike in the number of appeals coming in, we can deep dive into that to understand why this is happening, like if we might be potentially over-enforcing or perhaps just seeing a change in [user] behaviour.*
>
> HSP expert

3.2 Challenges related to specific measures

Having looked at the main fundamental rights issues arising in the context of existing HSP content moderation policies, this section outlines how the obligation to address exposure to terrorist content by enhancing moderation efforts might further exacerbate some of these challenges.

In general, due to the limited use of Article 5 so far (see textbox 'Limited practical experience with the use of specific measures'), most competent authorities and HSPs currently have no practical experience with specific measures. As a result, during the research, some interviewees were only able to share insights based on the rules and procedures they have set up for this purpose so far, or on existing frameworks that they envisaged to apply in such cases.

Limited practical experience with the use of specific measures

According to publicly available information, one HSP (SoundCloud) was designated as exposed to terrorist content and ordered to put in place specific measures by the competent authority in Germany in 2023. According to the transparency report issued by the competent authority, the Federal Network Agency (Bundesnetzagentur), the specific measures taken by the HSP were considered appropriate to curb the dissemination of terrorist content online on its platform.

In November and December 2024, TikTok, X and Meta (for Instagram and Facebook) were designated by the competent authority in Ireland as exposed to terrorist content. As their obligation to put in place specific measures only came into effect in 2025, transparency reports of these HSPs and the competent authority for 2024 do not yet contain information about the implemented measures.

When it comes to the number of removal orders triggering HSP designation, data indicates different approaches by competent authorities. While SoundCloud was designated after receiving 2 removal orders, the other platforms were issued 33 (Facebook), 23 (Instagram), 43 (X) and 191 (TikTok) removal orders by the end of 2024 when the designation took place.

The draft regulation foresaw that all HSPs, regardless of the degree of exposure to terrorist content, could adopt such measures proactively, on their own initiative, while those who have received a removal order would be obliged to adopt them and report on them to the competent authorities. Concerns that this would be disproportionate and might amount to imposing a general monitoring obligation upon HSPs (see Section 3.2.2) resulted in the adopted wording that only requires the implementation of specific measures from those HSPs designated as exposed to terrorist content.

The provision relating to specific measures impacts, in particular, the rights to respect for private

and family life (Article 7 of the Charter), protection of personal data (Article 8 of the Charter), freedom of expression and information (Article 11 of the Charter), freedom to conduct a business (Article 16 of the Charter) and non-discrimination (Article 21 of the Charter).

3.2.1 Lack of clarity when an HSP is exposed to terrorist content

The regulation limits the obligation to implement specific measures to HSPs designated as exposed to terrorist content. However, according to a range of interviewees, Article 5(4) only provides loose criteria for when to designate HSPs and trigger this requirement. Experts from competent authorities responsible for dealing with specific measures generally indicate that the provisions would serve as guidance rather than a set of strict criteria. Some say they would primarily base their decision on the receipt of two or more removal orders within the past 12 months, the example provided by the regulation. Others emphasise they would also consider other factors to assess each case individually and to determine whether a systemic issue exists. The practice in designating HSPs, albeit limited so far, confirms that approaches of competent authorities diverge (see textbox 'Limited practical experience with the use of specific measures').

Some experts from competent authorities indicate that a certain degree of regulatory flexibility is beneficial, allowing for more proportionality and an individual approach. The majority of interviewees from competent authorities entrusted with this task nevertheless highlight that clearer guidance would be necessary on how to determine when an HSP can be considered exposed to terrorist content. Some argue that the concept and criteria are too vague, leading to uncertainty for both the HSPs and the authorities themselves, reducing foreseeability and resulting in a lack of transparency in authorities' assessments. As for deciding that an HSP is no longer exposed to terrorist content, the regulation provides even less guidance, stating in Article 5(7) that a reasoned decision should be taken by the competent authority upon the HSP's request based on objective factors.

Promising practice: Providing additional information on specific measures to HSPs at the national level

Competent authorities in the two Member States that ordered HSPs to put in place specific measures by the end of 2024 issued additional regulatory frameworks or guidance to inform HSPs about the different aspects of the process. In Germany, the Federal Network Agency (Bundesnetzagentur) published, among other documents, a more elaborate list of possible specific measures with an indication of their suitability to different types of content and HSP size. In Ireland, the media regulator, Coimisiún na Meán, issued a decision framework describing the steps it would follow when deciding if an HSP is exposed to terrorist content.

Some experts question the logic of defining exposure based on just two removal orders, a low standard for larger HSPs whose scale of operations makes it very likely that some terrorist

content appears on their platforms, despite having dedicated staff and resources handling content moderation. This threshold, one competent authority expert argues, might be more relevant for smaller HSPs that struggle to protect their platforms from terrorist content. Another expert from a competent authority recalls that, in accordance with the logic of the regulation, an HSP receiving just two removal orders can be treated in the same manner as one receiving hundreds, and questions the proportionality of this approach, given the impact such measures can have on the companies and their users.

> *I think it is normal for a HSP to host terrorist content two times or more […] One has to be careful with these measures, because they can be very hard and have a big effect.*
>
> Competent authority expert

To further elaborate specific criteria for determining whether an HSP is exposed to terrorist content, some experts from competent authorities emphasise the need to collaborate with other authorities and learn from their approaches and emerging good practices, both with relevant authorities nationally, such as regulators in related fields, or in discussions with their counterparts in other Member States. Due to the limited experience with specific measures across the EU, comparing experience and exchanging best practices nevertheless remains difficult. In this regard, some experts mention the experience and discussions in the related context of DSA implementation as useful.

3.2.2 Specific measures as an incentive to use intrusive tools

In accordance with Article 5(6), the choice of what particular specific measures to implement in the case of being designated as exposed to terrorist content is left to the HSP. The research confirms that experts from competent authorities are aware that they cannot require HSPs to implement particular measures. Some highlight the advantages of this approach, granting HSPs discretion in determining the responses and tools most suitable to their own unique context. Others state they could support the HSPs with ideas and recommendations, for example based on what tools and approaches work well for other companies.

As to what measures HSP can choose to implement, the majority of experts from civil society / academia point to the overall lack of clarity provided by the regulation's broad list of potential measures (including 'any other measure that [the HSP] considers to be appropriate to address the availability of terrorist content on its services'). As a result, the interpretation of this obligation by HSPs is likely to vary from case to case, necessarily also differently impacting the rights of users. Some experts from competent authorities, on the other hand, highlight that the differences in capacity between HSPs of different sizes, along with variations in hosting models, make a flexible approach to ordering and implementing specific measures essential.

When it comes to the potential fundamental rights impact of specific measures, findings show

several areas of concern.

One relates to a risk of incentivising HSPs to implement changes to their policies that are likely to result in excessive takedowns of legitimate content. As described in Section 3.1, content moderation policies of many HSPs already run the risk of over-blocking and having a disproportionate impact on certain groups. In its formal comments on the proposed regulation, the European Data Protection Supervisor (EDPS) underlined the importance of ensuring that specific measures comply with the principle of necessity, are proportionate to the level of HSP's exposure to terrorist content and are accompanied by appropriate accountability tools [83].

In order to comply with authorities' expectations and avoid potential penalties, HSPs' terms and conditions may slide further towards over-compliance, over-removal and the unnecessary censorship of content, experts from civil society / academia warn. Some experts from competent authorities also advise caution when it comes to ordering HSPs to implement specific measures, highlighting that they can easily become overly stringent and have significant consequences for the rights of users. Other competent authority experts, on the other hand, argue that HSPs implementing specific measures would seek to avoid over-removal due to their business model [84].

> *There's no legal risk for platforms if they over-censor, but there is one if they under-censor.*
>
> Civil-society/academia expert

Furthermore, the regulation allows the use of automated tools as part of specific measures. As described in Section 3.1.1, these tools are increasingly deployed by HSPs to prevent the reappearance of prohibited content and to speed up the detection process. Even without being explicitly instructed to use these tools, the fact that the HSP is required to combat the presence of terrorist content on its platform more effectively, in combination with the vague and open-ended list of possible specific measures provided by the regulation, is likely to create strong pressure to employ these tools despite their known limitations and the likelihood of producing large numbers of false positives, experts from across professional groups say. For HSPs that have no experience with employing such tools or that lack strong fundamental rights expertise, it might be particularly difficult to avoid a disproportionate effect on rights.

Some experts from competent authorities consider automated tools a necessity for companies that deal with large amounts of content. They argue that their use should be acceptable as long as appropriate safeguards are in place, including the human oversight required in such cases by Article 5(3) of the regulation. Others consider them insufficiently transparent or draw attention to their limitations on accurately detecting and assessing potential terrorist content.

> *We do not know of any tools so good that they do not require human analysis. Keywords help, hashes help, but mainly it is analyst work.*
>
> Competent authority expert

Another concern relates to whether the obligations imposed on them by virtue of Article 5 might effectively require HSPs to resort to general content monitoring, particularly through automated tools. Amounting to indiscriminate surveillance, such general monitoring would impact not only freedom of expression and information but, notably, also the rights to privacy and protection of personal data.

The risk of incentivising HSPs to adopt measures de facto constituting indiscriminate surveillance of all content was among the chief concerns highlighted during the negotiations of the regulation [85] . While states can require providers of online services to address the dissemination of specific illegal content [86] , they are prohibited under Article 8 of the DSA and Article 15 of the e-Commerce Directive from imposing a general monitoring obligation, and the same principle is reflected in Article 5(8) of the regulation [87] . In accordance with international standards, states should also avoid any action that may indirectly lead to such general content monitoring [88] . However, some interviewees observe that the regulation effectively encourages HSPs to implement such general monitoring by leaving the choice of measures up to HSPs, permitting them to use automation and, at the same time, expecting them to arrive at outcomes that can be difficult to achieve without implementing general monitoring of content [89] .

Monitoring of specific measures by competent authorities should help ensure that such measures do not infringe on fundamental rights. However, replies by experts from competent authorities with this responsibility indicate a lack of clarity and a divergence of views on this topic. Some of these experts stress that fundamental rights would be integral to the assessment criteria and they would require HSPs to take adequate measures to protect these rights. Some other competent authority experts, on the other hand, state that the national legal frameworks governing their activities do not envisage them to monitor fundamental rights impacts. Others doubt whether they are equipped with sufficient training and knowledge when it comes to assessing issues such as discrimination.

> *I do not know if [fundamental rights] would be our focus. Not sure we have sufficient training or knowledge, unless it is evident. But any violation of fundamental rights could be taken by users to the judicial authority. […] We are not experts in that area; we implement the regulation.*
>
> Competent authority expert

3.2.3 Effectiveness of internal complaint mechanisms of HSPs

Article 10 obliges HSPs to establish effective and accessible complaint mechanisms for content providers whose content was removed because of specific measures. HSP experts confirm that existing complaint mechanisms that allow users to challenge takedowns based on HSP terms and conditions would be used for this purpose.

Complaint mechanisms can provide content providers with access to low-threshold non-judicial

remedies and contribute to greater transparency and accountability of HSPs towards content providers. This could help address some of the challenges arising in the context of HSP moderation policies. Findings from this research nevertheless reveal gaps in the application of these complaint mechanisms, which limit their effectiveness and accessibility in practice.

First, content providers can only use their right to complain to HSPs in case they are meaningfully informed about the takedown of their content, something that is not necessarily guaranteed and largely depends on HSP policies (see Chapter 4).

> *Access to an appeal does not mean anything if it is not a meaningful appeal.*
>
> Civil-society/academia expert

Second, the mechanism for processing complains may limit the effectiveness of the remedy. Some experts from civil society / academia note that, in some HSPs, complaints are assessed by the same person who decided on the takedown. Others refer to the use of automation by HSPs to review complaints, where the same tool trained on the same dataset, which determined that content is illegal, is used to determine the outcome of a complaint procedure. If this is done without human intervention, there is no meaningful remedy.

The regulation does not stipulate a specific deadline for handling complaints, and findings show that appeals are not necessarily prioritised by content moderation teams [90] . In some HSPs, an appeal against a removal of content is only queued for a limited period of time (e.g. 48 hours) and if it is not handled by then, the case is automatically closed without restoring the content, some interviewees say. In this context, a civil-society/academia expert with content moderation experience also highlights that violations of terms and conditions that are considered particularly severe, such as those related to terrorism, are subject to more stringent measures such as immediately blocking the entire account (rather than issuing a warning or temporary suspension, as would otherwise be the case). Loss of access to an account may make it very difficult in practice for the user to actually submit a complaint to the platform.

As the same mechanisms would be used when appealing against takedowns based on specific measures and those initiated by a referral (see Section 2.2), these gaps are relevant both in the context of an HSP's own content moderation and in response to takedowns initiated by competent authorities.

4. Selected safeguards and remedies

In line with the ECHR and the Charter, Member States are under an obligation to secure the rights of everyone within their jurisdiction. This also means that HSPs and content providers have the right to an effective remedy in the territory where they claim that their rights were abused without having to turn to another Member State [91].

Article 4 of the regulation contains an important set of safeguards in this regard. When a competent authority issues a removal order to an HSP that has its main establishment or legal representative in another Member State, it has the obligation to notify the competent authority in such host Member State of the removal order. PERCI, launched by Europol, supports this information exchange. This latter competent authority can, on its own initiative or upon request of HSPs or content providers, scrutinise such cross-border orders. If it determines that the order seriously or manifestly infringes the regulation or the fundamental rights enshrined in the Charter, it can invalidate it and order the HSP to reinstate the content.

Article 9 of the regulation requires Member States to ensure that HSPs and content providers can effectively challenge decisions taken under the regulation, including removal orders, decisions related to cross-border scrutiny, specific measures or penalties before a court of the Member State whose competent authority took that decision.

In addition, as discussed in Chapter 3, the regulation envisages in Article 10 an obligation for HSPs to have in place effective and accessible complaint mechanisms for content providers affected by specific measures.

Owing partly to the relatively slow uptake of the regulation across the EU, these key safeguards have only been tested in practice to a limited degree, and some of them not at all. Given its cross-border nature, scrutiny pursuant to Article 4 has typically only been applied by competent authorities in those Member States which host larger HSPs receiving removal orders from different Member States. Concerning judicial remedies pursuant to Article 9, fieldwork findings and additional data collected by FRA through desk research in all Member States did not identify any cases by the end of 2024 where HSPs or content providers availed themselves of their right to challenge a removal order or another decision issued under the regulation before national courts. This makes it challenging to adequately assess the effectiveness of this provision as a fundamental rights safeguard at this stage and to fully evaluate the impact of the regulation in this respect.

The mechanisms for scrutinising cross-border removal orders and seeking remedies are particularly relevant from the perspective of the right to an effective remedy and a fair trial (Article 47 of the Charter). However, they serve, in their application, to protect all other rights impacted under the regulation.

This chapter first summarises the findings of the research as regards the fundamental rights implications arising from the practical application of the mechanism for scrutinising cross-border

removal orders. Afterwards, it looks at the main concerns regarding the impact on the right to an effective remedy as arising from the research.

Summary of findings: Selected safeguards and remedies

- Several factors appear to limit the effective use of scrutiny of cross-border removal orders, including the non-mandatory nature of the scrutiny, mutual trust between authorities, limited experience and training, and clarity concerning the applicable standards.
- Practical obstacles to seeking remedies may include insufficient information about removal and the complexity of challenging decisions in another Member State.
- Incentives to seek *ex post* reinstatement of removed content may be reduced by the time-sensitive nature and relevance of online content, along with the unwillingness of some HSPs to enter into conflict with authorities.

4.1 Effective scrutiny of cross-border removal orders

The mechanism for scrutinising cross-border removal orders can only be functional if Member States appoint the competent authorities for this task. This factor hindered the use of this safeguard in the period following the adoption of the regulation, when such authorities did not exist in some Member States, including those hosting large HSPs that have been addressed by multiple cross-border removal orders. While this gap has been largely addressed since then, some interviewees from competent authorities and civil society / academia nevertheless note that the main attention of implementation efforts across the EU has been on removal orders, and cross-border scrutiny largely remains an afterthought despite the importance attached to it by the regulation.

> *All the emphasis has been put on the removal orders, but the scrutiny is left behind.*
>
> Competent authority expert

In practice, several specific obstacles adversely impact the effectiveness of the scrutiny mechanism. As noted by many experts from civil society / academia and experts from competent authorities entrusted with this task, Member States' authorities do not necessarily actively use the scrutiny option in practice. The regulation envisages it as mandatory only in case it is requested by an HSP or a content provider, and while competent authorities can choose to scrutinise any cross-border removal order they receive, they are not compelled to do so. Some experts from competent authorities entrusted with this task state that they conduct (or would conduct) scrutiny systematically in each case, to also have an overview of what content appears on platforms in their Member State. Some others, however, assume that the mechanism is triggered only upon an

HSP or content provider's request, or perceive it as a spot check rather than a systematic exercise.

> *I don't always open the file to see the content. Sometimes, yes. But it's only because I am curious about the matter. […] It's a matter of trust between states in Europe. Maybe if [the removal order came from] the Chinese, the Russians …*
>
> Competent authority expert

Findings also show a sense of mutual trust among some competent authorities responsible for scrutiny towards authorities of other Member States, which in practice means they might not critically review, if at all, each other's removal orders for possible infringement of the regulation or fundamental rights. Some experts responsible for scrutiny say that they consider the expertise of their colleagues issuing removal orders to be a sufficient guarantee, which, however, deprives this safeguard of its intended effect. Interviewed experts from competent authorities who either themselves conduct scrutiny of cross-border removal orders or who have had their removal orders scrutinised by other Member States confirm that there have not yet been cases where a removal order would be invalidated by the scrutinising competent authority.

As discussed in Chapter 1, some interviewees also suggest that some authorities designated to carry out scrutiny, such as law enforcement or regulatory bodies, might not be equipped with the appropriate experience and training to undertake a fundamental rights review of decisions issued by authorities of other countries, something that courts have experience with and therefore would be better suited to do in practice.

Responses by competent authorities also indicate a certain lack of clarity on how to implement the scrutiny in practice. This includes core questions such as what criteria should be used to determine whether the removal order infringes fundamental rights. Interviewees also offer different views on what legal framework and national interpretation should be applied by the scrutinising authority in light of the absence of a common baseline for interpreting the definition of terrorist content under Article 2(7) (see Section 1.2).

4.2 Practical obstacles to accessing remedies

A key precondition for exercising the right to an effective remedy, whether by seeking scrutiny in the case of cross-border removal orders pursuant to Article 4 or by challenging removal orders in court under Article 9, is the provision of sufficient information to content providers and HSPs [92] . The regulation acknowledges this by including a detailed list of information to be included in the removal order that national competent authorities are obliged to communicate to HSPs, including easily understandable information about the redress (Article 3(4)). It also provides a model removal order in its annex.

However, findings show limitations in this regard. Some HSPs and civil-society/academia experts note that the information provided in removal orders in practice is frequently insufficient. While some competent authorities provide elaborate reasoning, others do not include enough details or do not point to specific issues.

Promising practice: Integrating information on remedies into PERCI

Information on where to challenge the removal order has been reported to be incomplete or missing from removal orders in some cases in the past. According to some experts from competent authorities, this issue has been addressed by Europol by integrating Member-State-specific information on remedies directly into the removal order templates in PERCI. As a result, removal orders issued through the platform now contain this information automatically.

When it comes to content providers, the regulation leaves the specific implementation of this obligation up to the HSP, which can decide to only share the information about the reasons for the removal and possible remedies (not necessarily the full removal order), upon the content provider's request (Articles 11(1) and 11(2)). Interviewees indicate limited effectiveness of this system in practice, stating that some HSPs might not inform – either at all or in a meaningful way – users about the fact that their content was removed under the regulation. Experts from HSPs which have not yet received removal orders indicate they might apply their general policies on removing content: one referring to making a case-by-case decision whether or not to inform content providers and the other stating that they do not currently have a system in place, although they envisage implementing it due to DSA requirements. This points to gaps in HSP awareness of this obligation under the regulation and its uniform future application, including in comparison with knowledge concerning DSA obligations.

> *[The absence of remedies so far] means that either the content is very clear and there is no question that it shouldn't be circulated online [or] that many people do not know that they have the option to ask for the content to be re-assessed and re-uploaded.*
>
> Civil-society/academia expert

Furthermore, Article 11(3) allows competent authorities to instruct HSPs to temporarily withhold information about the removal from content providers for reasons of public security, including in the context of an investigation. While most interviews with experts from competent authorities and HSPs indicate that this option has not been frequently used in practice, some of them refer to this option as being used regularly, possibly systematically. While this exception can be justified in specific cases, if used widely, it risks rendering the remedies envisaged by the regulation inaccessible in practice.

Even where HSPs do notify content providers about the removal, some interviewees with content moderation experience recall that the manner in which HSPs inform users about their content being taken down (including those based on government requests such as removal orders under the regulation) is not always effective or transparent. Examples include putting a label in place of the content stating it was removed (not even mentioning what rules it violated specifically), which the user may not even notice, or sending a brief, low-profile notification to the user's inbox. In such cases, the content provider may not realise the removal of the content, its reasons or its legal basis, which subsequently affects whether they use their right to challenge the removal.

Besides access to information about the removal, findings highlight the complexity of challenging decisions under the regulation in other Member States, particularly when it comes to content providers. The regulation requires that remedies under Article 9 be sought in the Member State whose authority issued the removal order, while cross-border scrutiny under Article 4 can be requested in the Member State in which the HSP has its main establishment or legal representative. However, given the transnational nature of the online environment, content providers may be nationals of another Member State or even a non-EU country, especially when it comes to large social networks that are most frequently addressed by removal orders. Initiating legal procedures before a foreign court, in a country with a different legal regime and facing language barriers, is likely to be a considerable obstacle for content providers, some experts from civil society / academia emphasise, making the threshold for obtaining a remedy for a possible violation of rights impossible to reach in practice.

4.3 Limited incentives to seek a remedy

The regulation does not offer content providers or HSPs any mechanism to effectively challenge the removal order in court before the removal is carried out. Even if such an appeal were possible within the one-hour period, it would not automatically suspend the removal of content.

While the presence of a specific provision of Article 9 on remedies can be considered positive, interviewees question whether the possibility to seek a remedy only *ex post* (which also applies to requesting the scrutiny of a cross-border removal order under Article 4) makes the remedy effective in the context of online content.

Several experts from competent authorities explain the underuse of remedial options by content providers due to the fact that removal orders are only issued on content that is clearly terrorist content.

> *Most of the time, the content is clearly terrorist in nature so I would not expect content providers come asking 'Why did you take down my content?'*
>
> Competent authority expert

Interviewed experts from civil society / academia, and HSPs, on the other hand, emphasise that a large share of online content is time sensitive in its nature, such as a political statement related to

recent and specific events. The impact of such content is effectively lost if it is only restored weeks later. For some types of content, such as livestreaming, reinstating is not possible or meaningful at all. In this context, some experts from these professional groups believe there is an imbalance between the speed of removals that have to take place very quickly and the speed of processing appeals that can take much longer. Unless it is compensated for by additional safeguards in the course of adoption of a removal order, such as ensuring the involvement of independent oversight (see Section 1.2), this risks undermining the core component of the right to an effective remedy as defined by the ECtHR and CJEU, namely its ability to offer effective redress given the circumstances and nature of the rights violation at stake [93] . It may also reduce the incentive for content providers to seek a remedy in the first place.

> *Let's say the content is taken down and then it is not online for six months, the story is dead, the website is dead, the organisation is dead. So, on one hand, you have to be extremely quick and everything has to be done within an extremely short time frame. But the ability to go against it and say, well, this might be not legal, […] takes much longer.*
>
> HSP expert

When it comes to HSPs, several interviewees across all professional groups warn that they might feel dissuaded from challenging removal orders. This can be due to trust in the authorities' expertise but also due to elements of the regulation, such as the possibility for national competent authorities to impose high penalties for non-compliance and strict deadlines imposed on HSPs, and because the broader EU regulatory framework motivates companies towards compliance with requests from competent authorities. Experts from civil society / academia and some HSPs explain that, given the potential impact of non-compliance, only platforms that bill themselves as freedom of expression or privacy champions and that invest in having specific teams with critical awareness in terms of fundamental rights might decide to push back against the removal of content that they do not consider to be terrorist in nature.

> *It's dangerous then when the competent authorities are thinking 'well, the platform will provide the scrutiny', and the platform is thinking 'well, we defer to the expertise of the authorities'. So […] a loophole emerges which goes back to the concerns about freedom of expression and over enforcement.*
>
> Civil-society/academia expert

Findings also indicate that there might be diverging expectations among competent authorities and HSPs as to who should carry the main responsibility for ensuring that the application of the regulation does not violate fundamental rights. It is notable that while experts from competent authorities refer to the different safeguards and remedies available to the HSPs and content providers, testimonies of experts from other professional groups – and the underuse of Article 9

so far – tend to point to their limitations and show a degree of scepticism over their effectiveness. As one civil-society/academia expert highlights, if competent authorities believe that it is up to HSPs to provide further review of flagged content and, at the same time, HSPs tend to trust the assessment and due diligence of authorities, this can create a gap in accountability and in fundamental rights protection.

Conclusion

Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online seeks to contribute to the effective protection of public security. At the same time, it acknowledges the profound impact that the application of its provisions can have on a broad range of fundamental rights and contains several important safeguards in this regard.

However, as shown by empirical findings presented in this report, addressing the proliferation of online terrorist content while respecting fundamental rights is a complex task in practice. Limited experience still exists with respect to some elements of the regulation, including key safeguards, which does not allow for the mapping of its implications on fundamental rights in full. Nevertheless, the experience of practitioners and other experts confirms that the application of the regulation affects a variety of rights, allowing for the identification of concrete challenges. Therefore, this report recommends taking different measures to:

- ensure clarity of the definition of terrorist content and the foreseeability of its application;
- avoid incentivising HSPs to unduly restrict freedom of expression by over-removing content;
- avoid a discriminatory impact on particular groups and a chilling effect on their rights;
- enhance transparency of the use of the regulation;
- strengthen the effectiveness of the regulation in line with the proportionality principle, including by enhancing the focus of its application on right-wing terrorist content;
- increase the effectiveness of safeguards and remedies.

These findings can assist EU institutions and Member States in assessing the need for further steps to ensure that the application of the regulation complies fully with fundamental rights. At the same time, they present a contribution to the wider discussions on regulating online content in a manner that effectively addresses the presence of illegal content while safeguarding freedom of expression and information and other rights.

Annex: Methodology

This report is primarily based on data collected through fieldwork interviews. These interviews involved 62 practitioners and experts from three broad respondent groups defined by professional categories.

- **Staff of competent authorities** tasked with applying or supporting the application of the different provisions of the regulation (e.g. law enforcement authorities and media regulators). Experts responsible for different aspects of the regulation (issuing removal orders, conducting scrutiny of cross-border removal orders, etc.) were interviewed. The focus was primarily, but not exclusively, on authorities that already have practical experience in applying the regulation.
- **Staff of HSPs** involved with the regulation, or more broadly, in dealing with illegal content. The HSPs were selected to cover companies of different sizes, types and business models, and include those that already have practical experience with applying the regulation (e.g. receiving removal orders) and those that do not.
- **Experts from civil-society organisations and academic experts** familiar with the regulation and related areas. These experts were selected to cover a wide range of expertise relevant to the regulation, including in the areas of privacy, freedom of expression, human rights and counterterrorism, capacity-building work with HSPs, and online content moderation.

All interviews took place in person and online between July 2024 and January 2025 and were conducted directly by FRA staff. Each interview was conducted with one or more interviewees from the same organisation and lasted on average 90 minutes.

Interviewees replied orally to questions from a predefined questionnaire, sharing their experience and views as regards fundamental rights challenges, concerns and good practices related to the application of the regulation against the backdrop of the broader picture of addressing the dissemination of terrorist content online. The interviewers could ask follow-up questions or request clarifications and encouraged respondents to speak freely and draw on their personal experiences. Interviews were audio-recorded, if the respondent consented, and were documented using an interview-reporting template in full compliance with FRA's data protection standards.

All interviews took place under the guarantee of anonymity of individual interviewees and the organisations they represent. This was necessary given both the confidentiality of counterterrorism work and the sensitivity of the topic for HSPs.

Therefore, this report does not list individual interviewees or the authorities, HSPs or civil-society organisations they are affiliated to. When reporting on the views shared or information provided by a particular interviewee, the report refers to them only by the professional group they represent. This allows for comparing the experience across the three professional groups where relevant. Given the clearly defined competences for applying the regulation at the national level, specific Member States where interviews took place are not listed in order not to jeopardise this anonymity. Where references are made in this report to particular Member States, HSPs or other

organisations, these are based on open-source material or information collected through desk research, which covered all 27 Member States (see further below), not on interviews.

The fieldwork was supplemented by limited desk research conducted by FRA's multidisciplinary research network, Franet, between January and February 2025. The desk research collected basic information about the implementation of the regulation's requirements into national legal and institutional frameworks in all 27 Member States.

In addition, Europol (i.e. the EU Internet Referral Unit of the European Counter Terrorism Centre) provided FRA with information on the functioning and use of PERCI, which is managed by Europol and supports Member States in applying the regulation.

Acronyms and Abbreviations

- **Charter** European Union Charter of Fundamental Rights
- **CJEU** Court of Justice of the European Union
- **DSA** Digital Services Act
- **ECHR** European Convention on Human Rights
- **ECtHR** European Court of Human Rights
- **EDPS** European Data Protection Supervisor
- **EU** European Union
- **Europol** European Union Agency for Law Enforcement Cooperation
- **FRA** European Union Agency for Fundamental Rights
- **GIFCT** Global Internet Forum to Counter Terrorism
- **HSP** hosting service provider
- **PERCI** EU Platform on Illicit Content Online
- **TCO** Terrorist Content Online
- **UN** United Nations

Endnotes

[1] FRA, Proposal for a regulation on preventing the dissemination of terrorist content online and its fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg, 2019.

[2] For example, UN Security Council Resolutions 1963 (2010), 2129 (2013), 2170 (2014), 2178 (2014), 2253 (2015), 2322 (2016), 2354 (2017), 2395 (2017), 2396 (2017) and 2617 (2021).

[3] Council of Europe, Appendix to Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries, 7 March 2018.

[4] See Tech Against Terrorismwebsite.

[5] See Global Internet Forum to Counter Terrorism website.

[6] See The Christchurch Call website.

[7] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6, ELI: http://data.europa.eu/eli/dir/2017/541/oj.

[8] FRA, Directive (EU) 2017/541 on Combating Terrorism – Impact on fundamental rights and freedoms, Publications Office of the European Union, Luxembourg, 2021.

[9] Its revised version, 'Code of conduct on countering illegal hate speech online+', was integrated into the framework of the DSA in 2025.

[10] Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, OJ L 63, 6.3.2018, p. 50, ELI: http://data.europa.eu/eli/reco/2018/334/oj.

[11] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

[12] Consolidated text: Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 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), ELI: http://data.europa.eu/eli/dir/2010/13/2025-02-08, Article 28b(1)(c).

[13] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act), OJ L 2024/1083, 17.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1083/oj.

[14] Europol, 'EU Internet Referral Unit – EU IRU', Europol website.

[15] See, for example, Europol, European Union Terrorism Situation and Trend Report – 2024, Publications Office of the European Union, Luxembourg, 2024.

[16] On this topic, see also ECtHR Press Unit, 'Terrorism and the European Convention on Human Rights – Factsheet', February 2024; and Council of Europe and ECtHR, 'Guide on Article 10 of the European Convention on Human Rights – Freedom of expression', 31 August 2022.

[17] Judgment of the Court of the ECtHR of 7 December 1976, Handyside v the United Kingdom, No 5493/72, paragraph 49.

[18] Judgment of the Grand Chamber of the ECtHR of 15 May 2023,Sanchez v France, No 45581/15, paragraph 151; judgment of the Court of the ECtHR of 26 November 1991, Observer and Guardian v the United Kingdom, No 13585/88, paragraph 59.

[19] Judgment of the Second Section of the ECtHR of 14 December 2010, Dink v Turkey, Nos 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, paragraph 137; judgment of the Fifth Section of the ECtHR of 10 April 2019, Khadija Ismayilova v Azerbaijan, Nos 65286/13 and 57270/14, paragraph 158.

[20] For example, judgment of the Fifth Section of the ECtHR of 6 April 2009, Leroy v France, No 36109/03, paragraph 36.

[21] Judgment of the Grand Chamber of 3 September 2008, Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, C-402/05 P and C-415/05 P, ECLI:EU:C:2008:461, paragraph 363; judgment of the Third Chamber of 15 November 2012, Al-Aqsa v Council and Pays-Bas / Al-Aqsa, C-539/10 P, ECLI:EU:C:2012:711, paragraph 130; judgment of the Grand Chamber of 8 April 2014, Digital Rights Ireland and Seitlinger and Others, C-293/12, ECLI:EU:C:2014:238, paragraph 42.

[22] Judgment of the Third Section of the ECtHR of 8 October 2018, Stomakhin v Russia, No 52273/07, paragraphs 89, 99–107; judgment of the Fifth Section of the ECtHR of 12 November 2015, Bidart v France, No 52363/11, paragraphs 42–43; decision of the Second Section of the ECtHR of 17 April 2018, Roj TV A/S v Denmark, No 24683/14, paragraphs 46–48; decision of the Fifth Section of the ECtHR of 12 June 2012, Hizb Ut-Tahrir and Others v Germany, No 31098/08, paragraphs 73–74 and 78.

[23] Judgment of the Third Section of the ECtHR of 22 September 2021, Erkizia Almandoz v Spain, No 5869/17, paragraphs 40–41.

[24] Judgment of the Grand Chamber of the ECtHR of 8 July 1999, Erdoğdu and İnce v Turkey, Nos 25067/94 and 25068/94, paragraph 47; judgment of the Third Section of the ECtHR of 12 July 2007, Demirel and Ateş v Turkey, Nos 10037/03 and 14813/03, paragraph 37; judgment of the Fourth Section of the ECtHR of 16 March 2000, Özgür Gündem v Turkey, No 23144/93, paragraph 63; judgment of the Second Section of the ECtHR of 6 October 2010, Gözel and Özer v Turkey, Nos 43453/04 and 31098/05, paragraph 52; judgment of the Third Section of the ECtHR of 8 October 2018, Stomakhin v Russia, No 52273/07, paragraphs 93 and 131; judgment of the Fifth Section of the ECtHR of 12 November 2015, Bidart v France, No 52363/11, paragraphs 35 and 45; decision of the Fifth Section of the ECtHR of 20 October 2015, M'Bala M'Bala v France, No 25239/13, paragraphs 37–39.

[25] Judgment of the Grand Chamber of the ECtHR of 16 June 2015, Delfi AS v Estonia, No 64569/09, paragraphs 110 and 133; judgment of the Fourth Section of the ECtHR of 10 June 2009, Times Newspapers Ltd (Nos 1 and 2) v the United Kingdom, Nos 3002/03 and 23676/03, paragraph 27.

[26] Judgment of the Grand Chamber of the ECtHR of 22 December 2020, Selahattin Demirtaş v Turkey (No 2), No 14305/17, paragraphs 249–254 and 270; judgment of the Grand Chamber of the ECtHR of 15 October 2015, Perinçek v Switzerland, No 27510/08, paragraph 131.

[27] Judgment of the Fourth Section of the ECtHR of 6 June 2016, Szabo and Vissy v Hungary, No 37138/14, paragraphs 59 and 65.

[28] Judgment of the Fifth Section of the ECtHR of 12 November 2015, Bidart v France, No 52363/11, paragraphs 38–41; judgment of the Third Section of the ECtHR of 17 October 2001, Association Ekin v France, No 39288/98, paragraph 61.

[29] Proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online – A contribution from the European Commission to the Leaders' meeting in Salzburg on 19–20 September 2018, COM(2018) 640 final of 12 September 2018, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018PC0640.

[30] In January 2023, the Commission launched infringement proceedings against 22 Member States for not having designated competent authorities under Article 12(1) and failure to comply with other obligations under the regulation. See Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, COM(2024) 64 final of 14 February 2024, p. 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2024%3A64%3AFIN.

[31] See UN, Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, OL OTH 71/2018, 2018, pp. 2–5. See also Meijers Committee, 'CM1904 Comments on the proposal for a regulation on preventing the dissemination of terrorist content online (COM(2018) 640 final)', 2019, pp. 1–2; European Digital Rights, 'Letter to Member States calls for safeguards in terrorist content regulation', European Digital Rights website, 16 December 2019.

[32] See, for example, In-Cyprus, 'New bill aims to crack down on online "terrorist content"', In-Cyprus website, 17 May 2024; the lower house of the German parliament (Deutscher Bundestag), Stenografischer Bericht 44. Sitzung, Plenarprotokoll 20/44, 23 June 2022, pp. 4598–4602 (Annex 9); Estonian Parliament (Riigikogu), Protocol of the session on 13 December 2023; Hellenic Parliament (Βουλή των Ελλήνων), Minutes of K' Period, Plenary Session NB', (Πρακτικά Ολομέλειας, Κ' Περίοδος, Σύνοδος Α', Συνεδρίαση ΝΒ'), 16 November 2023, p. 5605 et seq.; Arangüena Fanego, C., 'New steps against terrorism in the EU: Regulation (EU) 2021/784 and orders for the removal of terrorist content online', Revista de Estudios Europeos, 2023; French National Assembly (Assemblée nationale), 'Referral to the Constitutional Council by 60 deputies, No 2022-841 DC received by the court registry of the Constitutional Council', ('Saisine du Conseil constitutionnel par 60 députés, No2022-841 DC reçue par le greffe du Conseil constitutionnel'), 29 July 2022; the Parliament of Luxembourg (Chambre des Députés), 'Verbatim – Debate on file 8325 – Session of 02.07.2024' ('Verbatim – Débat sur le dossier 8325 – Séance du 02.07.2024'), 2 July 2024, p. 3; National Council of the Judiciary of Poland, 'Opinion on the draft law amending the Anti-Terrorism Act and the Act on the Internal Security Agency and the Intelligence Agency', 28 November 2024.

[33] See Scheinin, M., UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'Ten areas of best practices in countering terrorism', A/HRC/16/51, 22 December 2010, pp. 15–16.

[34] FRA, Directive (EU) 2017/541 on combating terrorism – Impact on fundamental rights and freedoms, Publications Office of the European Union, Luxembourg, 2021, pp. 57–66.

[35] FRA, Directive (EU) 2017/541 on combating terrorism – Impact on fundamental rights and freedoms, Publications Office of the European Union, Luxembourg, 2021, p. 10.

[36] The updated list of national competent authorities and contact points is available on the Commission website.

[37] This is notably the cases in Cyprus (The prevention of the dissemination of terrorist content on the internet Act of 2024 (Ο περί της Πρόληψης της Διάδοσης Τρομοκρατικού Περιεχομένου στο Διαδίκτυο Νόμος του 2024), Article 3(1)); in Denmark (Act on supplementary provisions to the regulation on handling the dissemination of terrorist content online (Lov om supplerende bestemmelser til forordning om håndtering af udbredelsen af terrorrelateret indhold online), Article 4(1)); in Malta (Addressing the dissemination of terrorist content online regulations, Legal Notice 7 of 2023, Article 4(1)); and in Slovenia (Act implementing the Regulation (EU) on addressing the dissemination of terrorist content online (Zakon o izvajanju Uredbe (EU) o obravnavanju razširjanja terorističnih spletnih vsebin (ZIUORTSV)), 23 September 2024, Article 3(1)). In Italy, the preliminary investigations judge is competent for scrutinising cross-border removal orders (see Legislative Decree No 107 of 24 July 2023 on adaptation of national legislation to the provisions 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 (Decreto Legislativo 24 luglio 2023, n. 107, Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online), Article 4.

[38] See, for example, Kuczerawy, A., The proposed regulation on preventing the dissemination of terrorist content online: Safeguards and risks for freedom of expression, Center for Democracy and Technology, 5 December 2018, p. 10; FRA, Proposal for a regulation on preventing the dissemination of terrorist content online and its fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg, 2019, pp. 23–26.

[39] See, for example, Nomoplatform, 'Εναρμόνιση πρόληψης διάδοσης τρομοκρατίας στο διαδίκτυο και διαχείριση περιουσίας ανίκανων προσώπων' ('Harmonising the prevention of the dissemination of online terrorism and the management of assets of incapacitated persons'), Nomoplatform website, 9 September 2024; National Council of the Judiciary of Poland, 'Opinion on the draft law amending the Anti-Terrorism Act and the Act on the Internal Security Agency and the Intelligence Agency', 28 November 2024.

[40] See, for example, the Danish Parliament (Folketinget), Parliamentary debate (L 166 Forslag til lov om supplerende bestemmelser til forordning om håndtering af udbredelsen af terrorrelateret indhold online), pp. 27–31; the Minister of Justice and Security of the Netherlands (Minister van Justitie en Veiligheid), 'Explanatory Memorandum. Regulation on preventing the dissemination of terrorist content online implementation Act', ('Memorie van Toelichting. Uitvoeringswet verordening terroristische online-inhoud'), 2022, pp. 15–16.

[41] See, for example, Arangüena Fanego, C., 'New steps against terrorism in the EU: Regulation (EU) 2021/784 and orders for the removal of terrorist content online', Revista de Estudios Europeos, 2023; the Assembly of the Republic of Portugal (Assembleia da República), Draft Law 44/XVI. Proposed amendments to Article 2 (Proposta de Lei 44/XVI. Propostas de alteração ao artigo 2.º), 5 February 2025.

[42] In Slovenia, for example, only one court (District Court Nova Gorica) can issue removal orders. This model was selected to ensure proportionality of measures and legal certainty, given that removal orders are considered to interfere with constitutional rights, and also to ensure specialisation and a uniform decision-making practice. See the National Assembly of Slovenia (Državni zbor Republike Slovenije), '23rd Regular meeting of the Committee on Home Affairs, Public Administration and Local Self-Government' ('Odbor za notranje zadeve, javno upravo in lokalno samoupravo'), selected transcript of the meeting (Izbrani zapis seje), 9 October 2024.

[43] A subgenre of rap, drill features confrontational lyrics and deals with themes such as gang rivalries and violence.

[44] Oversight Board, 'UK drill music', Oversight Board website, 22 November 2022.

[45] See the Federal Law Gazette of Germany (Bundesgesetzblatt), Act for the Implementation of Regulation (EU) 2021/784 of the European Parliament and the Council of 29 April 2021 to Combat the Dissemination of Terrorist Online Content and for the Amendment of Further Laws (Gesetz zur Durchführung der Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte und zur Änderung weiterer Gesetze), 21 July 2022, Article 2; the Croatian Parliament (Hrvatski sabor), Law on the Implementation of the Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Combating the Dissemination of Terrorist Content Online (Zakon o provedbi Uredbe (EU) 2021/784 Europskog Parlamenta i Vijeća od 29. travnja 2021. o borbi protiv širenja terorističkog sadržaja na internetu), 19 July 2022, Articles 4(5) to 4(6) and Articles 5(3) to 5(4); and the Lithuanian Parliament (Seimas), Law on the Provision of Information to the Public (Visuomenės informavimo įstatymas), No. I-1418, 2 July 1996, last amendment No. XIV-3120, 12 November 2024, Article 19(10).

[46] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53, ELI: http://data.europa.eu/eli/reg/2016/794/oj.

[47] See, for example, EDPS, 'Formal comments of the EDPS on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online', 12 February 2019, p. 5; FRA, Proposal for a regulation on preventing the dissemination of terrorist content online and its fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg, 2019, pp. 26–28.

[48] In France, the rules for implementing removal orders were one of the main concerns raised by civil-society organisations, including La Quadrature du Net, which referred the implementing national legislation to the Council of State (Conseil d'Etat) in November 2023. The application was pending at the time of writing this report.

[49] In a decision of 18 June 2020, the French Constitutional Council (Conseil Constitutionnel) invalidated certain provisions of the law aimed at fighting online hate content, known as the Avia Law, stating that they infringed on freedom of speech and communication and are not necessary, appropriate and proportionate to the aim pursued. This included a provision obliging HSPs to remove illegal terrorist content and child sexual abuse material within one hour after the receipt of a notification by an administrative authority.

[50] A nasheed is a form of Islamic vocal music, frequently exploited by terrorist organisations to spread jihadist propaganda. See Europol, European Union Terrorism Situation and Trend Report – 2024, Publications Office of the European Union, Luxembourg, 2024, p. 28.

[51] See, for example, Equality and Human Rights Commission, Choudhury, T. and Fenwick, H., 'The impact of counter-terrorism measures on Muslim communities', Equality and Human Rights Commission Research Report series, 2011; Amnesty International, A human rights guide for researching racial and religious discrimination in counter-terrorism in Europe, 2021; European Network Against Racism and Choudhury, T., Suspicion, Discrimination and Surveillance: The impact of counter-terrorism law and policy on radicalised groups at risk of racism in Europe, 2021.

[52] See, for example, UN, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009; or Council of Europe, Limiting the Use of Criminal Law to Restrict Freedom of Expression: A Guide to Council of Europe standards, September 2025.

[53] Europol, European Union Terrorism Situation and Trend Report – 2024, Publications Office of the European Union, Luxembourg, 2024, p. 4.

[54] FRA, Directive (EU) 2017/541 on combating terrorism – Impact on fundamental rights and freedoms, Publications Office of the European Union, Luxembourg, 2021, pp. 9, 63–64, 86–87.

[55] Information provided by Europol at FRA's request on 18 June 2025, covering the period from the start of the operation of PERCI on 3 July 2023 until 31 March 2025.

[56] Council of the European Union and the European Council, 'Sanctions against terrorism', Council of the European Union and the European Council website, 29 July 2025.

[57] UN, 'United Nations Security Council consolidated list', UN Security Council website.

[58] US Department of State, 'Foreign terrorist organizations', US Department of State website.

[59] Incel (involuntary celibate) refers to a mostly online subculture that has been associated with cases of misogynist attacks. See, for example, European Commission and Radicalisation Awareness Network, Incels: A first scan of the phenomenon (in the EU) and its relevance and challenges for P/CVE, Publications Office of the European Union, Luxembourg, 2021.

[60] See, for example, in this regard, The International Centre for the Study of Radicalisation, 'Academic and Practical Research Working Group white paper: Extremism research horizons', GIFCT, 2021, p. 2.

[61] This has been recognised by counterterrorism experts, with some calling for designating more far-right terrorist groups to accurately reflect and respond to the danger stemming from these groups. See, for example, Tech Against Terrorism, Who Designates Terrorism? – The need for legal clarity to moderate terrorist content online, Tech Against Terrorism, 2023, p. 5.

[62] FRA, Directive (EU) 2017/541 on combating terrorism – Impact on fundamental rights and freedoms, Publications Office of the European Union, Luxembourg, 2021, pp. 8–9.

[63] See, for example, the lower house of the German parliament (Deutscher Bundestag), Stenografischer Bericht 44. Sitzung, Plenarprotokoll 20/44, 23 June 2022, pp. 4598–4602 (Annex 9); Ministry of the Interior of Bulgaria, Ex-ante impact assessment of the Draft Law amending and supplementing the Ministry of the Interior Act, 15 January 2025.

[64] See Tech Against Terrorism Europe, 'Report: The challenges that small and micro HSPs face in implementing the TCO Regulation', Tech Against Terrorism Europe website, 8 October 2024.

[65] In 2023, Member States transmitted 329 removal orders and 35 164 referrals to HSPs through PERCI. While the use of removal orders by Member States has increased in the meantime, referrals still far outnumber them. See Europol: EU Internet Referral Unit, 2023 EU Internet Referral Unit Transparency Report, Publications Office of the European Union, Luxembourg, 2025, p. 10.

[66] See also FRA, Proposal for a regulation on preventing the dissemination of terrorist content online and its fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg, 2019, pp. 35–37.

[67] Council of Europe, Appendix to Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries, 7 March 2018, paragraph 1.1.1.

[68] This includes, in alphabetical order, Archive.org, Catbox, Data Room, FlokiNET, Jumpshare.com, Justpaste.it, Krakenfiles.com, Meta, SoundCloud, Telegram, TikTok, Top4Top.net and X. See European Commission, Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, COM(2024) 64 final of 14 February 2024, p. 5.

[69] According to available HSP transparency reports, the highest number of removal orders pursuant to Article 3 of the regulation in 2024 was received by Telegram (requestable and accessible with a Telegram account only), followed by TikTok, Spotify, Facebook, Instagram and X.

[70] See, for example, Macdonald, S. and Staniforth, A., 'Tackling terrorist content online – Propaganda and content moderation', Tech against Terrorism Europe whitepaper, 2023, pp. 14–15.

[71] See, for example, Council of Europe, Appendix to Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries, 7 March 2018, Recital 6. For relevant jurisprudence, see judgment of the Second Section of the ECtHR of 14 December 2010, Dink v Turkey, Nos 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, paragraph 137; judgment of the Fifth Section of the ECtHR of 10 April 2019, Khadija Ismayilova v Azerbaijan, Nos 65286/13 and 57270/14, paragraph 158.

[72] For more details, see the Oversight Board website.

[73] See Centre on Regulation in Europe and Broughton Micova, S., Systemic Risk in Digital Services: Benchmarks for evaluating management of risk of terrorist content dissemination, 2024, p. 11; Saltman, E. and Hunt, M., 'Borderline Content: Understanding the gray zone', GIFCT, 2023.

[74] On the use of automation by HSPs, see, for example, Organisation for Economic Cooperation and Development (OECD), 'Transparency reporting on terrorist and violent extremist content online', OECD Digital Economy Papers, No 367, June 2024, pp. 29–31.

[75] See, in particular, FRA, Bias in Algorithms – Artificial intelligence and discrimination, Publications Office of the European Union, Luxembourg, 2022.

[76] On the role and importance of 'human-in-the-loop' processes, see, for example, Thorley, T. G. and Saltman, E., 'GIFCT Tech Trials: Combining behavioural signals to surface terrorist and violent extremist content online', Studies in Conflict and Terrorism, 2023, pp. 1–26.

[77] See, for example, Barrett, P. M., Who Moderates the Social Media Giants? – A call to end outsourcing, NYU Stern Center for Business and Human Rights, 2020; Miceli, M., Tubaro, P., Casilli, A. A., Le Bonniec, T., Salim Wagner, C. et al., Who Trains the Data for European Artificial Intelligence? – Report of the European Microworkers Communication and Outreach Initiative (EnCOre, 2023–2024), DiPLab, Weizenbaum Institute, and DAIR Institute, 2024, pp. 22–26.

[78] This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of the Member States on this issue.

[79] On this topic, see Tech Against Terrorism, Who Designates Terrorism? – The need for legal clarity to moderate terrorist content online, 2023.

[80] See, for example, the work of the non-governmental organisation Mnemonic, including the Syrian Archive. See also Goodman, J. and Korenyuk, M., 'AI: War crimes evidence erased by social media platforms', BBC website, 1 June 2023, concerning the removals of footage capturing human rights abuses during the Russian war of aggression in

Ukraine.

[81] Data by Tech Against Terrorism shows that HSPs also tend to remove a smaller percentage of right-wing terrorist content that is flagged to them by other players in comparison with flagged jihadist content. Tech Against Terrorism, 'Mapping far-right terrorist propaganda online', Terrorist Content Analytics Platform, May 2024, p. 24.

[82] See, for example, European Network Against Racism and Choudhury, T., Suspicion, Discrimination and Surveillance: The impact of counter-terrorism law and policy on radicalised groups at risk of racism in Europe, 2021, pp. 53–56.

[83] EDPS, 'Formal comments of the EDPS on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online', 12 February 2019, pp. 6–7.

[84] On the role of private players in enforcing law online and the impact on fundamental rights, see for example, Bellanova, R. and De Goege, M., 'Co-producing Security: Platform content moderation and European security integration', Journal of Common Market Studies, Vol. 60, 28 December 2021; Tosza, S., 'Internet service providers as law enforcers and adjudicators. A public role of private actors', Computer Law & Security Review, Vol. 43, November 2021.

[85] See, for example, UN, Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, OL OTH 71/2018, 2018, pp. 9–10; FRA, Proposal for a regulation on preventing the dissemination of terrorist content online and its fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg, 2019, pp. 38–42.

[86] For a distinction between general and specific monitoring, see, for example, Senftleben, M. and Angelopoulos, C., The odyssey of the prohibition on general monitoring obligations on the way to the Digital Services Act: Between Article 15 of the e-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market, October 2020.

[87] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1, ELI: http://data.europa.eu/eli/dir/2000/31/oj.

[88] Council of Europe, Appendix to Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries, 7 March 2018, paragraph 1.3.5.

[89] See also Meijers Committee, 'CM1904 Comments on the proposal for a Regulation on preventing the dissemination of terrorist content online (COM(2018) 640 final)', 2019, p. 5.

[90] When commenting on the proposed regulation, EDSP recommended introducing a deadline within which HSPs would be obliged to decide on a complaint. EDPS, 'Formal comments of the EDPS on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online', 12 February 2019, p. 11.

[91] See also FRA, Proposal for a regulation on preventing the dissemination of terrorist content online and its fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg, 2019, p. 29.

[92] FRA, Proposal for a regulation on preventing the dissemination of terrorist content online and its fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg, 2019, pp. 30–32.

[93] See FRA, Handbook on European law relating to access to justice, Publications Office of the European Union, Luxembourg, 2016, notably Sections 5.1 and 7.2.