EUROPEAN
COMMISSION

Brussels, 14.2.2024
COM(2024) 64 final

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

{SWD(2024) 36 final}

1. EXECUTIVE SUMMARY

Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online provides the legal framework at European level for Member States to protect citizens from being exposed to terrorist material online. The Regulation seeks to ensure the smooth functioning of the digital single market by addressing the misuse of hosting services for the dissemination to the public of terrorist content online. It aims at preventing that terrorists make use of the internet to spread their messages to intimidate, radicalise, recruit and facilitate terrorist attacks. This is particularly relevant in the current context of conflict and instability, which has an impact on Europe's security. Russia's war of aggression against Ukraine and the terrorist attack perpetrated by Hamas against Israel on 7 October 2023 resulted in an increase of terrorist content being disseminated online.

The regulatory framework to address illegal content online was further strengthened with the entry into force of the Digital Services Act on 16 November 2022. The Digital Services Act regulates the obligations of digital services that act as intermediaries in their role of connecting consumers with content, services and goods, thereby better protecting users online and contributing to a safer online environment.

The Regulation on addressing the dissemination of terrorist content online entered into application on 7 June 2022. According to Article 22 of the Regulation, the Commission shall submit a report on the application of the Regulation ("implementation report") to the European Parliament and to the Council.

This implementation report is based on the assessment of the information provided by Member States, Europol and hosting service providers in accordance with the obligations established in the Regulation. Based on such assessment, the key findings regarding the implementation of the Regulation can be summarised as follows:

- As of 31 December 2023, **twenty-three Member States** have designated competent authority(-ies) with the power to issue removal orders as established in the Regulation[1]. The list of Member States' authorities is available on the Commission's website and regularly updated.[2]

- As of 31 December 2023, the Commission has received information about at least **349 removal orders of terrorist content** issued by the competent authorities of six Member States (Spain, Romania, France, Germany, Czechia and Austria), which in most cases led to swift follow-up actions by hosting service providers to remove or block access to terrorist content. This proves that the tools provided by the Regulation are starting to be used and are successful in ensuring the swift removal of terrorist content by hosting service

[1] The online register, set up by the Commission as per Article 12(4) of the Regulation, lists the competent authorities referred to in Article 12(1) and the contact point designated or established pursuant to Article 12(2) for each competent authority. It is regularly updated upon notifications received from Member States. List of national competent authority (authorities) and contact points (europa.eu).

[2] List of national competent authority (authorities) and contact points.

providers as per Article 3(3). According to the information received by the Commission, these removal orders have not been challenged.

- **Coordination works well** between Member States' competent authorities and Europol, in particular Europol's Internet Referral Unit (EU IRU), in the application of the Regulation, especially in the processing of removal orders.
- Europol's tool "**PERCI**"[3] went live on 3 July 2023. This tool has been successfully used by some Member States to transmit both removal orders and referrals[4]. Spanish, German, Austrian, French and Czech competent authorities have used the tool to transmit removal orders. Overall, at least 14,615 referrals have been processed in PERCI between the launch of PERCI on 3 July and 31 December 2023.
- Although the Regulation does not contain any particular measures on referrals, according to information received by the Commission, there has also been an **increase in responsiveness to referrals** by hosting service providers since the entry into application of the Regulation.
- Based on the knowledge of the Commission, as of 31 December 2023, no hosting service provider has been identified as having been exposed to terrorist content, as defined in Article 5(4) of the Regulation. This identification is a prerequisite for the application of the specific measures outlined in that article. Nonetheless, according to the transparency reports provided by hosting service providers, measures have been taken by hosting service providers **to address the misuse of their services** for the dissemination of terrorist content, notably through the adoption of specific terms and conditions and the application of other provisions and measures to limit the spread of terrorist content.
- Hosting service providers have also adopted measures for the notification **of imminent threat to life** as per Article 14(5) of the Regulation.

As regards **smaller hosting service providers**, the Commission launched in 2021 a call for proposals to support them in implementing the Regulation. The Commission awarded in 2022 three projects (see under section 4.8.) which started their work in 2023 and have already delivered some results in providing support to small companies to comply with the Regulation.

The Commission launched infringement proceedings against 22 Member States for not having designated competent authorities under Article 12(1) of the Regulation and failure to comply with their obligations under Articles 12(2), 12(3) and 18(1) by sending **letters of formal notice** on 26 January 2023[5]. Following the launch of these infringement proceedings, the number of Member States notifying the competent authorities responsible for handling removal orders increased, as

[3] PERCI (*Plateforme Européenne de Retraits des Contenus illégaux sur Internet*) is a platform for the takedown of illegal content online developed and managed by Europol. It supports the implementation of the Regulation by providing a technical solution for processing referrals and removal orders to hosting service providers among other functionalities.

[4] Referrals are a mechanism for alerting hosting service providers for the provider's voluntary consideration of the compatibility of that content with its own terms and conditions. The Regulation (recital 40) states that referrals have proven to be effective and should remain available in addition to removal orders.

[5] See press release: Terrorist content online (europa.eu).

reflected in the information published in the online register[6]. In addition, 11 of the infringement cases opened in January 2023 have been closed by 21 December 2023[7].

On the basis of the information received from Member States and Europol and made available by hosting service providers, the Commission assessed that the application of the Regulation has had a **positive impact** in limiting the spread of terrorist content online.

2. CONTEXT

The Regulation entered into application on 7 June 2022. It seeks to ensure the smooth functioning of the digital single market by addressing the misuse of hosting services for the dissemination to the public of terrorist content online. It provides Member States with targeted tools, in form of removal orders, to address the dissemination of terrorist content online and enables Member States to request hosting service providers of all sizes to take specific measures to protect their services from exploitation by terrorist actors when exposed to terrorist content.

In addition, with the entering into force of the Digital Services Act on 16 November 2022, the regulatory landscape is extended by horizontal legislation with a broad scope aimed at ensuring a safer digital space for consumers, effective measures to counter illegal content and more transparent conditions of service. The Digital Services Act equips the Commission with ample supervision, investigative and enforcement powers to take actions addressed to very large online platforms and search engines. These actions include requests for information and investigations into companies' content moderation actions with the possibility of imposing fines.

The Digital Services Act enables to tackle all forms of illegal content, allowing the Commission to challenge platforms to provide data to demonstrate that they are living up to their own commitments on content removal. Whilst the Terrorist Content Online Regulation provides an even more powerful tool for this specific form of illegal content with a legal obligation to remove content within one hour of receipt of a removal order and effective sanctioning mechanisms.

As highlighted by Europol in the Terrorism Situation and Trend Reports (TE-SAT)[8] published in the last years, terrorists make extensive use of the internet to spread their messages to intimidate, radicalise, recruit and facilitate terrorist attacks. While voluntary measures and non-binding recommendations bore fruit to reduce the availability of terrorist content online, limitations including the small number of hosting service providers adopting voluntary mechanisms[9] as well as the fragmentation of procedural rules across Member States limited the effectiveness and the efficiency of cooperation among Member States and hosting service providers and made it necessary to establish regulatory measures.[10] Therefore, the effective application of the Regulation

[6] List of national competent authority (authorities) and contact points (europa.eu). There is information on 23 Member States' competent authorities for issuing removal orders pursuant to Article 12(1)(a) in the online register.
[7] Finland, Malta, Czechia, Denmark, Romania, Sweden, Latvia, Spain, Lithuania, Austria and Slovakia.
[8] Europol's TE-SAT 2023 https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2023.pdf and 2022 https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf
[9] European Commission, (2018) Impact Assessment accompanying the Proposal for a Regulation on preventing the dissemination of terrorist content online, SWD(2018) 408 final, accessed on 04/05/2023 at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN.
[10] Ibidem.

is key to address the dissemination of terrorist content online. The Commission has proactively supported national competent authorities in this process.

According to Article 22 of the Regulation, the Commission had the obligation to submit a report on the application of the Regulation ("implementation report") to the European Parliament and to the Council by 7 June 2023, building on information provided by the Member States, which in turn relied partially on information provided by hosting service providers (Article 21). The delay in the submission of the implementation report is due on the one hand to the late transmission to the Commission of key information from Member States and hosting service providers. On the other hand, it was considered important to reflect in the implementation report the use of PERCI, which became operational on 3 July 2023 and it has been used since then for the processing of removal orders according to the Regulation.

This implementation report solely aims to give a factual overview of relevant matters relating to the application of the Regulation. It does not contain any interpretations of the Regulation and it does not express any opinion on interpretations or other measures taken in application of the Regulation.

In accordance with Article 21(2) of the Regulation, the Commission had to establish by the same date (7 June 2023) a detailed programme for monitoring the outputs, results and impacts of the Regulation. More specifically, the monitoring programme should set out the indicators, means and intervals at which the data and other necessary evidence are to be collected. Such programme is established in the accompanying Staff Working Document. It specifies the actions to be taken by the Commission and the Member States in collecting and analysing the data and other evidence to monitor the progress and impacts of the Regulation and to perform an evaluation of the Regulation pursuant to its Article 23.

3. OBJECTIVE AND METHODOLOGY OF THE REPORT

The objective of this report is to assess the application of the Regulation and what has been its impact so far in limiting the dissemination of terrorist content online. This includes actions taken by Member States and hosting service providers, such as amendments to their terms of service and community guidelines and their compliance and responsiveness to removal orders.

For this purpose, the Commission gathered information from Member States, Europol's Internet Referral Unit (EU IRU) and hosting service providers, including information contained in the transparency and monitoring reports under Articles 7, 8 and 21 of the Regulation. Information pursuant to Articles 8 and 21 was received from 18 Member States. Information on actions taken by hosting service providers was collected through their annual transparency reports, Europol, and via direct voluntary communication with Commission services. This implementation report includes information received by the Commission until 31 December 2023.

Monitoring and transparency obligations (Articles 21, 7 and 8)

For the establishment of the implementation report, according to Article 21(1) of the Regulation, Member States are obliged to collect information from their competent authorities and hosting

service providers under their jurisdiction and send to the Commission by 31 March every year. This includes information about the actions that they have taken in accordance with the Regulation in the previous calendar year. Article 21(1) refers to the type of information that Member States should collect on measures taken to comply with the Regulation, such as details on removal orders, number of access requests to content preserved to allow investigations, complaint procedures, administrative and judicial reviews.

According to Article 7(1) of the Regulation, hosting service providers shall set out clearly in their terms and conditions their policy for addressing the dissemination of terrorist content, including, where appropriate, a meaningful explanation of the functioning of specific measures.

In addition, as per Article 7(2) of the Regulation, a hosting service provider that has taken action to address the dissemination of terrorist content or has been required to take action pursuant to the Regulation in a given calendar year, shall make publicly available a transparency report on those actions for that year. This report should be published before 1 March of the following year.

Article 7(3) of the Regulation sets out the minimum information that these transparency reports should include, such as measures taken to identify and disable access to terrorist content, the number of items removed and/or reinstated and the outcome of complaints.

According to Article 8 of the Regulation, Member States' designated competent authorities shall publish annual transparency reports on their activities under the Regulation. Article 8(1) refers to minimum information that these reports should include.[11]

As of 31 December 2023, eighteen Member States have sent information to the Commission about their actions taken in accordance with the Regulation, while twenty-three Member States have designated authority(-ies) with the power to issue removal orders as established in the Regulation.

4. SPECIFIC POINTS OF ASSESSMENT

4.1. REMOVAL ORDERS (Article 3)

In total, as of 31 December 2023, the Commission has been informed about at least 349 removal orders sent to Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L., FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net and Catbox by the competent authorities of Spain, Romania, France, Germany, Austria and Czechia.

Sixty-two removal orders have been sent by the Spanish competent authority - CITCO (*Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*), while the Romanian competent authority (ANCOM – Autoritatea Națională pentru Administrare și Reglementare în Comunicații) sent two removal orders and the French competent authority (OCLCTIC – L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) sent twenty-

[11] See text of Regulation (EU) 2021/784, Article 8 (1) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R0784

six removal orders. Since the terrorist attack perpetrated by Hamas against Israel, the German competent authority (BKA – Bundeskriminalamt) has sent 249 removal orders.

The Spanish competent authority has transmitted sixty-two removal orders: eighteen before the launch of PERCI and fourty-four through PERCI. It provided a detailed description of the transmission of and follow-up to the first removal orders issued, which is very relevant to better understand the implications and effects of the Regulation.

The two first removal orders were issued by the Spanish competent authority on 24 April 2023.[12] They were related to two pieces of terrorist content, one concerning right-wing terrorism and the other one concerning jihadism. The content that was subject to the first removal order was a PDF document posted on Telegram with unlimited access, which advocated for terrorist violence and glorified right-wing terrorist attacks. The piece of terrorist content subject to the second removal order was a video featuring images of jihadists from the so-called Islamic State terrorist organisation in combat uploaded on Internet Archive. These two pieces of content were removed from both platforms in less than one hour, thus in compliance with Article 3(3) of the Regulation. In the assessment provided by the Spanish competent authority it was explained that they had opted for a removal order rather than a referral for two main reasons: compliance with the requirements in the Regulation on removal orders and urgency. The Spanish competent authority then sent further removal orders.

The Spanish authority highlighted challenges related to the use of a webform by one hosting service provider (Meta) to receive removal orders instead of providing a direct contact point. This webform also led to problems to communicate with the competent authority of the Member State where the hosting service provider's main establishment is located.

The French competent authority issued their first removal order on 13 July 2023 to a sharing platform (Justpaste.it), which removed the terrorist content within one hour. The targeted content was propaganda from Al Qaeda, more specifically from the media body Rikan Ka Mimber of its Indian branch Al Qaeda Indian Sub continent (AQIS). The full removal of the content was confirmed in Europol's platform PERCI.

The German competent authority issued six, sixteen and five removal orders on 16, 18 and 24 October 2023 respectively targeting propaganda from Hamas and Palestinian Islamic Jihad. Access to the content was blocked in the EU in compliance with Article 3(3) of the Regulation. The German competent authority had first sent referrals and subsequently issued removal orders as these referrals were not acted upon. Following Hamas' attack on 7 October 2023, the German competent authority has sent 249 removal orders, mostly to Telegram.[13]

The Czech competent authority and the Austrian competent authority issued 2 and 8 removal orders, to X and Telegram respectively.

As regards the use of a webform to receive removal orders by one hosting service provider, Spanish authorities indicated two issues: 1) in the context of Article 3(2) of the Regulation, a webform does

[12] Ministerio del Interior | El CITCO culmina la retirada de Internet de dos contenidos que alentaban al terrorismo
[13] According to information available to the Commission.

not allow Member States' competent authorities to send information on the applicable procedures and deadlines before issuing the first removal order to the hosting service provider; 2) in the context of Article 4(1), a webform does not allow to submit a copy of the removal order simultaneously to the competent authority of the Member State where the hosting service provider has its main establishment and to the hosting service provider's legal representative.

4.2 CROSS-BORDER REMOVAL ORDERS (Article 4)

For the two first removal orders issued in April 2023, the Spanish competent authority could not send copies to the authority of the Member State where the hosting service provider had its main establishment or its legal representative, as none of the two hosting service providers had, at the time, their main establishment or designated a legal representative in the EU. For the subsequent removal orders, the Spanish competent authority sent copies to the competent authority of the Member State where the hosting service provider had its main establishment or had designated its legal representative.

Transmitting removal orders to hosting service providers based in third countries that have not yet fulfilled their obligation of appointing a legal representation in the EU was reported as a challenge by Member States. In this context, the Commission supported Member States to ensure that hosting service providers comply with their obligation to appoint a legal representative in the EU and to provide a contact point (Article 15(1) of the Regulation), such as an email address, to ensure immediate action. Furthermore, the Commission has reminded hosting service providers of their obligations in different fora, including in the EU Internet Forum.

According to the information available to the Commission, no competent authority of the Member State in which the hosting service provider has its main establishment has so far scrutinised a removal order pursuant to Article 4 of the Regulation to determine whether it seriously or manifestly violated the Regulation or fundamental rights and freedoms as there has been no reasoned request for scrutiny submitted yet. As a consequence, up to now, no authority has found that any removal order infringed this Regulation or fundamental rights in that manner.

No hosting service provider has so far reinstated the content (or access thereto) which had been subject to a removal order pursuant to scrutiny in accordance with Article 4 of the Regulation, because such scrutiny and requests for reinstatement have not yet taken place. Hence, there is no information available on how long it usually takes to reinstate content or access to it, or the "necessary measures" taken by the hosting service providers to reinstate the content or access to the content.

4.3. REMEDIES (Article 9)

According to the information available to the Commission, hosting service providers have not challenged removal orders or decisions pursuant to Article 5(4) before the relevant courts so far. Nevertheless, one hosting service provider argued the impossibility to execute a removal order.

According to the information provided by Member States,[14] at least twelve Member States have "effective procedures" in place to enable hosting service providers and content providers to challenge a removal order issued and/or a decision taken under Article 4(4) or Article 5(4), (6) or (7) before the courts of the competent authority of those Member States (Article 9(1) and (2)). In Member States where these procedures are in place, such procedures mostly refer to lawsuits. However, whether these procedures are "effective" or specific to the Regulation cannot be ascertained with the current data received from Member States, due to the fact that no decision was challenged so far.

4.4. SPECIFIC MEASURES AND RELATED TRANSPARENCY (Articles 5 and 7)

According to the information available, to date, no hosting service provider has been held to be exposed to terrorist content within the meaning of Article 5(4) of the Regulation. As a consequence, the requirement to take the specific measures set out in that article does not (yet) apply to any hosting service provider.

It can nonetheless be noted that, according to the transparency reports provided by hosting service providers, several hosting service providers have taken measures to address the misuse of their services for the dissemination of terrorist content, notably the adoption of specific terms and conditions and the application of other provisions and measures to limit the spread of terrorist content. As noted above, pursuant to Article 7, hosting service providers must ensure transparency in this regard not only through transparency reporting, but also by including clear information in their terms and conditions.

4.5. IMMINENT THREAT TO LIFE (Article 14(5))

According to Article 14(5) of the Regulation, where hosting service providers become aware of terrorist content involving an imminent threat to life, they shall promptly inform authorities competent for the investigation and prosecution of criminal offences in the Member States concerned. Where it is not possible to identify the Member States concerned, the hosting service provider shall transmit the information to Europol for appropriate follow-up.

By 31 December 2023, the Commission has been informed about nine instances in which Europol's EU Internet Referral Unit has received information on terrorist content involving an imminent threat to life. As Article 14(5) of the Regulation does not provide for an obligation to inform Europol in all instances, the number of notifications could be higher. The only Member State that provided information on the application of Article 14(5) was Spain. On 18 April 2023, the authorities of Spain received a communication from Amazon on a supposed piece of terrorist content involving an imminent threat to life on Twitch videogaming platform. The content was assessed not to correspond to the conditions for terrorist content involving an imminent threat to life within the meaning of the Regulation.

[14] It should be noted that the information provided is not necessarily complete. Further assessments would be needed to obtain a full and entirely up-to-date overview of the manner in which Member States gave effect to the requirement of ensuring the availability of effective redress procedures.

4.6. COOPERATION BETWEEN HOSTING SERVICE PROVIDERS, COMPETENT AUTHORITIES AND EUROPOL (Article 14)

As mentioned above, Europol has developed a platform called "PERCI" to support the implementation of the Regulation by centralising, coordinating and facilitating the **transmission of removal orders and referrals** by Member States to hosting service providers. The platform is operational since 3 July 2023. Ahead of the full implementation of PERCI, Europol had put in place contingency arrangements to support the manual transmission of removal orders, de-confliction of content to avoid interference with ongoing investigations and crisis response in "imminent threat to life" situations.

PERCI is a single system allowing cooperation among competent authorities, hosting service providers and Europol, as foreseen in Article 14 of the Regulation with regard to matters covered by the Regulation. More concretely, PERCI:

- is a cloud-based solution designed to ensure security and data protection in the cloud;
- is a single platform for collaborative and real-time communication and co-ordination, which supports the swift removal of terrorist content;
- facilitates the scrutiny process on cross-border removal orders;
- reinforces de-confliction, which is important to avoid that a Member State's competent authority sends a removal order targeting content subject to an ongoing investigation in another Member State;
- allows hosting service providers to receive removal orders in a unified and standardised manner from a single channel.

Separately, PERCI also allows for the transmission of referrals.

At present, apart from its relevance in connection to referrals (see Recital 40 of the Regulation), PERCI facilitates the transmission of removal orders (Articles 3 and 4), Member States' reporting (Article 8) and coordination, as well as de-confliction in case of conflict with ongoing investigations on the content for which a removal order is intended to be sent (Article 14). PERCI is currently undergoing further developments to support additional tasks deriving from the Regulation, such as scrutiny of cross-border removal orders (Article 4)[15].

Member States confirmed that as per Article 14 of the Regulation:

- competent authorities exchange information, coordinate, and cooperate with other competent authorities;

[15] More in detail: - Article 3 and Article 4: Transmission of Removal Orders; - Article 3(6)-(8): hosting service providers' feedback; - Article 4(3)-(7): Scrutiny mechanism; - Article 7: Reporting; - Article 14(1): de-confliction, coordination, avoidance of duplication; - Article 14(3): Secure communication channel; - Article 14(4): Use of a dedicated tool established by Europol; - Article 14(5): 'Imminent threat to life' communication; - Recital 40: Transmission of Referrals.

- competent authorities exchange information, coordinate, and cooperate with Europol;
- there are mechanisms in place to enhance cooperation while avoiding the interference with investigations occurring in other Member States;
- most Member States regard PERCI as the preferred tool to be used for transmitting removal orders, as it allows for coordination of action through de-confliction.

4.7. EFFECTS ON REFERRALS

Referrals of terrorist content are a voluntary tool that was already used before the adoption of the Regulation. Whilst the Regulation contains no particular rules on referrals, in accordance with its Recital 40, nothing in the Regulation precludes Member States and Europol from using referrals as an instrument to address terrorist content online.

Since its establishment in 2015, the EU Internet Referral Unit in Europol has been active in identifying terrorist content online and referring it to hosting service providers, as well as in establishing tools, (i.e. PERCI and previously IRMA[16]) to facilitate the transmission of referrals.

According to the information provided to the Commission, Member States' authorities continue to use referrals with certain hosting service providers, while they might consider issuing removal orders to hosting service providers that are not responding to referrals or for other reasons such as the urgency to have the content taken down.

4.8. SUPPORT TO SMALLER HOSTING SERVICE PROVIDERS FOR THE IMPLEMENTATION OF THE REGULATION

The Regulation contains various obligations for hosting service providers. While large hosting service providers typically have the technical capabilities, human verification capacity and knowledge to implement the Regulation, small ones may have more limited financial, technical and human resources and expertise for that purpose. At the same time, smaller hosting service providers are increasingly targeted by malicious actors to exploit their services. This might also be attributed to effective content moderation efforts by larger hosting service providers. While this trend showcases the success of content moderation measures, it also highlights the need to support smaller hosting service providers in increasing their capacity and knowledge to comply with the requirements of the Regulation.

To respond to this challenge, the Commission launched a call for proposals under the Internal Security Fund to support smaller hosting service providers in implementing the Regulation[17]. The

[16] Europol built the Internet Referral Management Application (IRMA) in 2016 to support the referral (flagging) of illegal content to Online Service Providers. Initially, access to IRMA was granted to Europol staff and specialised Units (IRUs) in seven Member States. IRMA was replaced by PERCI as of 3 July 2023.

[17] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/isf/wp-call/2021-2022/call-fiche_isf-2021-ag-tco_en.pdf

Commission selected three projects[18] to support them with a threefold approach. Firstly, by informing and increasing awareness about the Regulation's rules and requirements, secondly by developing, implementing and rolling out tools and frameworks needed to address the dissemination of terrorist content online, and thirdly by sharing experiences and best practices across the industry.

The three projects began their work in 2023 and have already delivered valuable results. For instance, in its mapping report, the FRISCO project[19] found that micro and small hosting service providers tend to have very limited awareness and knowledge of the Regulation and underlined potential difficulties they could face in responding to removal orders within one hour, as they often lack 24/7 services. Lack of resources is a challenge, as well as establishing lines of communication with law enforcement agencies. More than half of the hosting service providers surveyed by the contractors do not moderate user-generated content and stated that they never encountered terrorist content on their platforms. These hosting service providers are likely to take ad hoc measures if such content appears on their platforms.

Through these three projects, small hosting service providers are being supported in their efforts to comply with the rules of the Regulation also by setting up points of contact and implementing mechanisms for users' complaints.

In addition, Article 3(2) of the Regulation – which requires the timely provision of information on applicable procedures and deadlines to hosting service providers to whom no earlier removal order has been issued – can be of relevance in particular to smaller hosting service providers.

4.9. SAFEGUARDS OF FUNDAMENTAL RIGHTS

The Regulation includes various safeguards to strengthen accountability and transparency about measures taken to remove terrorist content online. In this respect, reference is made to the foregoing, in particular the information provided on remedies, reporting and the special mechanism for cross-border removal orders.

Furthermore, Article 23 of the Regulation requires that the Commission reports on the functioning and effectiveness of the safeguard mechanisms, in particular those provided for in Article 4(4), Article 6(3) and Articles 7 to 11 in the context of the evaluation of the Regulation. Such safeguards concern complaints, remedies, and penalties mechanisms adopted and implemented against the risk of erroneous removal of terrorist content online to protect content providers and hosting service providers. The assessment of the functioning and effectiveness of the safeguard mechanisms will therefore be part of the evaluation pursuant to Article 23.

[18] (1) AI-based framework for supporting micro (and small) hosting service providers on the report and removal of online terrorist content (ALLIES), (2) Fighting terrorist Content Online (FRISCO) and (3) Technology Against Terrorism Europe (TATE). link for more information: Funding & tenders (europa.eu).

[19] Conducted over a six-month period ending in May 2023.The report is based on feedback of 48 European hosting service providers, 33 answers through our online survey and 15 through interviews. FRISCO, *D2.1: Mapping Report on needs and barriers for compliance Understanding small and micro hosting service providers' needs and awareness in relation to implementing the TCO Regulation requirements*, available at Deliverables | Frisco (friscoproject.eu).

In this respect, in the programme for monitoring referred to in Article 21(2) of the Regulation, a framework of indicators is provided for the evaluation of the effects of the Regulation on fundamental rights, which will feed into the evaluation of the Regulation.

The monitoring programme will support the assessment, to be conducted as part of the evaluation, of the functioning and effectiveness of the safeguards' mechanisms implemented in the context of the Regulation, and their impact on fundamental rights. This area of impacts reflects the two areas mentioned in Article 23 of the Regulation: (a) the functioning and effectiveness of the safeguard mechanisms, in particular those provided for in Articles 4(4), 6(3) and 7 to 11; and (b) the impact of the application of this Regulation on fundamental rights, in particular the freedom of expression and information, the respect for private life and the protection of personal data.

4.10. COMPETENT AUTHORITIES (Article 13)

According to Article 13 of the Regulation, Member States have to ensure that their competent authorities have the necessary powers and sufficient resources to achieve the aims of and fulfil their obligations under the Regulation. Some Member States have implemented the following measures to ensure that competent authorities have the necessary powers and sufficient resources:

- establishment of new bodies/Directorates;
- allocation of extra funding and additional staff and
- creation of new legislative frameworks.

5. CONCLUSION

It is of utmost important that all tools and measures at EU level are fully implemented to swiftly address the illegal content disseminated online. This is especially the case in view of the sheer scale of such illegal content as witnessed recently by the dissemination of content related to the attack perpetrated by Hamas against Israel.

The Regulation contributes to increasing public security across the Union to prevent that hosting service providers operating in the internal market are used by terrorists to spread their messages to intimidate, radicalise, recruit and facilitate terrorist attacks.

Following the opening of infringement proceedings in January 2023, **progress has been achieved**. As of 31 December 2023, twenty-three Member States have designated competent authorities under Article 12(1) as reflected in the online register, resulting in a more systematic use of the measures and tools provided in the Regulation. In addition, eleven of the twenty-two infringement cases opened in January 2023 have been closed as of 21 December 2023. The Commission urges the remaining Member States to take the necessary steps in order to designate the competent authorities under Article 12(1) and comply with their obligations under Articles 12(2), 12(3) and 18(1).

Overall Member States have reported a smooth transmission of removal orders to hosting service providers with the support of Europol. On the basis of the information received from Member States and Europol, at least 349 **removal orders of terrorist content** have been transmitted since

the entry into application of the Regulation. In ten cases the terrorist content was not removed/access blocked by one hosting service provider within the one-hour maximum period established by the Regulation.

According to information received from Member States and Europol, despite the Regulation not containing any rules in this regard, there has been increased responsiveness to referrals of terrorist content since the entry into application of the Regulation. Furthermore, Europol received information from hosting service providers in nine instances about terrorist content involving an imminent threat to life, as per Article 14(5).

More efficient communication channels and procedures are in place especially since the launch of the PERCI platform on 3 July 2023, which led to a more systematic approach to the transmission of removal orders, whilst PERCI is also being used to transmit a high number of referrals. Member States and Europol expressed the expectation that the deployment of PERCI will benefit the use of these instruments to tackle terrorist content online.

On this basis, the Commission assesses that overall, the Regulation has had a **positive impact** in limiting the spread of terrorist content online. Nevertheless, in ten cases out of 349, the targeted hosting service provider exceeded the one-hour maximum period established in the Regulation to remove terrorist content or block access thereto.

The Commission is proactively supporting Member States and hosting service providers, including through technical workshops organised prior to and after the entry into application of the Regulation. The last one took place on 24 November 2023. The Commission is also supporting smaller hosting service providers to ensure full and swift application of the Regulation and assisting them in tackling the challenges encountered so far.

The Commission will continue to monitor the implementation and application of the Regulation. The Commission will closely monitor the performance of the instruments provided in the Regulation through the monitoring programme, which will feed into the evaluation of the Regulation pursuant to Article 23.