EUROPEISKA
KOMMISSIONEN

Bryssel den 14.2.2024
COM(2024) 64 final

RAPPORT FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

om genomförandet av förordning (EU) 2021/784 om åtgärder mot spridning av terrorisminnehåll online

{SWD(2024) 36 final}

1. SAMMANFATTNING

Genom förordning (EU) 2021/784 om åtgärder mot spridning av terrorisminnehåll online ges medlemsstaterna en rättslig ram på EU-nivå för att skydda medborgarna från exponering för terrorisminnehåll online. Förordningen syftar till att säkerställa att den digitala inre marknaden fungerar smidigt genom att motverka att värdtjänster missbrukas för att sprida terrorisminnehåll online till allmänheten. Avsikten är att förhindra att terrorister använder internet för att sprida sina budskap i syfte att skrämma, radikalisera och rekrytera människor och underlätta terroristattacker. Detta är särskilt relevant i den rådande kontext som präglas av konflikter och instabilitet och som påverkar säkerheten i Europa. Rysslands anfallskrig mot Ukraina och den terroristattack som Hamas utförde mot Israel den 7 oktober 2023 ledde till en ökad spridning av terrorisminnehåll online.

Den rättsliga ramen för att hantera olagligt innehåll online stärktes ytterligare när förordningen om digitala tjänster trädde i kraft den 16 november 2022. I förordningen om digitala tjänster regleras skyldigheterna för digitala tjänster som fungerar som mellanhänder genom att de förmedlar innehåll, tjänster och varor till konsumenter. Därigenom gör den användarna bättre skyddade online och bidrar till en säkrare onlinemiljö.

Förordningen om åtgärder mot spridning av terrorisminnehåll online trädde i kraft den 7 juni 2022. Enligt artikel 22 i förordningen ska kommissionen lägga fram en rapport om tillämpningen av förordningen (en *genomföranderapport*) för Europaparlamentet och rådet.

Denna genomföranderapport bygger på en bedömning av den information som medlemsstaterna, Europol och värdtjänstleverantörerna tillhandahåller i enlighet med de skyldigheter som fastställs i förordningen. På grundval av en sådan bedömning kan de viktigaste iakttagelserna rörande genomförandet av förordningen sammanfattas som följer:

- Den 31 december 2023 hade **23 medlemsstater** utsett en eller flera behöriga myndigheter med befogenhet att utfärda avlägsnandeorder i enlighet med förordningen[1]. Förteckningen över medlemsstaternas myndigheter finns på kommissionens webbplats och uppdateras regelbundet[2].

- Fram till den 31 december 2023 hade kommissionen fått information om minst **349 avlägsnandeorder för terrorisminnehåll** som utfärdats av de behöriga myndigheterna i sex medlemsstater (Spanien, Rumänien, Frankrike, Tyskland, Tjeckien och Österrike). I de flesta fall ledde avlägsnandeorderna till att värdtjänstleverantörerna vidtog snabba uppföljningsåtgärder för att avlägsna terrorisminnehållet eller göra det oåtkomligt. Detta bevisar att de verktyg som föreskrivs i förordningen börjar användas och fungerar för att säkerställa att värdtjänstleverantörer snabbt avlägsnar terrorisminnehåll i enlighet med

[1] I onlineregistret, som upprättats av kommissionen i enlighet med artikel 12.4 i förordningen, förtecknas de behöriga myndigheter som avses i artikel 12.1 samt för varje myndighet den kontaktpunkt som utsetts eller inrättats i enlighet med artikel 12.2. Registret uppdateras regelbundet när underrättelser inkommit från medlemsstaterna. Förteckning över nationella behöriga myndigheter och kontaktpunkter (europa.eu).
[2] Förteckning över nationella behöriga myndigheter och kontaktpunkter.

artikel 3.3. Enligt de uppgifter som inkommit till kommissionen har dessa avlägsnandeorder inte bestridits.

- **Samordningen fungerar väl** mellan medlemsstaternas behöriga myndigheter och Europol, i synnerhet Europols enhet för anmälan av innehåll på internet (EU IRU), vid tillämpningen av förordningen, särskilt vid behandling av avlägsnandeorder.
- Europols verktyg **Perci**[3] togs i bruk den 3 juli 2023. Vissa medlemsstater har med goda resultat använt detta verktyg för att överföra både avlägsnandeorder och anmälningar[4]. Spanska, tyska, österrikiska, franska och tjeckiska behöriga myndigheter har använt verktyget för att överföra avlägsnandeorder. Sammanlagt har minst 14 615 anmälningar behandlats i Perci från det att verktyget lanserades den 3 juli 2023 fram till den 31 december 2023.
- Även om förordningen inte innehåller några särskilda åtgärder avseende anmälningar har tjänsteleverantörernas **lyhördhet för anmälningarna ökat sedan förordningen trädde i kraft**, enligt uppgifter som inkommit till kommissionen.
- Såvitt kommissionen känner till har ingen värdtjänstleverantör fram till den 31 december 2023 ansetts vara exponerad för terrorisminnehåll i den mening som avses i artikel 5.4 i förordningen. Att en värdtjänstleverantör anses vara exponerad för terrorisminnehåll är en förutsättning för att de specifika åtgärder som beskrivs i den artikeln ska tillämpas. Enligt värdtjänstleverantörernas transparensrapporter har de dock vidtagit åtgärder **för att förhindra att deras tjänster missbrukas** för att sprida terrorisminnehåll, särskilt genom att införa specifika användarvillkor och genom att tillämpa andra bestämmelser och åtgärder för att begränsa spridningen av terrorisminnehåll.
- Värdtjänstleverantörerna har också infört åtgärder för anmälan av **överhängande hot mot en eller flera personers liv** i enlighet med artikel 14.5 i förordningen.

När det gäller **mindre värdtjänstleverantörer** inledde kommissionen 2021 en ansökningsomgång för att stödja dem i genomförandet av förordningen. Kommissionen valde under 2022 ut tre projekt (se avsnitt 4.8). Dessa projekt inleddes under 2023 och har redan levererat vissa resultat när det gäller att ge mindre företag hjälp med att efterleva förordningen.

Den 26 januari 2023 inledde kommissionen, genom att skicka **formella underrättelser**, överträdelseförfaranden mot 22 medlemsstater för att de inte hade utsett behöriga myndigheter i enlighet med artikel 12.1 i förordningen och för att de underlåtit att fullgöra sina skyldigheter enligt artiklarna 12.2, 12.3 och 18.1[5]. Efter det att överträdelseförfarandena inletts ökade antalet medlemsstater som meddelat vilka myndigheter de utsett som behöriga för handläggningen av

[3] Perci (*Plateforme Européenne de Retraits des Contenus illégaux sur Internet*, EU:s plattform för avlägsnande av olagligt innehåll på internet) är en plattform för borttagning av olagligt innehåll online som utvecklats och förvaltas av Europol. Plattformen stöder genomförandet av förordningen genom att erbjuda en teknisk lösning för behandling av anmälningar och avlägsnandeorder till tjänsteleverantörer samt andra funktioner.

[4] Anmälningar är en mekanism som används för att uppmärksamma värdtjänstleverantörer på innehåll så att de frivilligt kan bedöma om det innehållet är förenligt med deras egna användarvillkor. I förordningen (skäl 40) anges att anmälningar har visat sig vara ett effektivt verktyg och att de bör förbli tillgängliga vid sidan av avlägsnandeorder.

[5] Se pressmeddelande: Terrorisminnehåll online (europa.eu).

avlägsnandeorder, vilket återspeglas i den information som offentliggjorts i onlineregistret[6]. Dessutom hade elva av de överträdelseförfaranden som inleddes i januari 2023 avslutats den 21 december 2023[7].

På grundval av den information som mottagits från medlemsstaterna och Europol och som gjorts tillgänglig av värdtjänstleverantörer bedömer kommissionen att tillämpningen av förordningen har haft en **positiv inverkan** när det gäller att begränsa spridningen av terrorisminnehåll online.

2. BAKGRUND

Förordningen trädde i kraft den 7 juni 2022. Den syftar till att säkerställa att den digitala inre marknaden fungerar smidigt genom att motverka att värdtjänster missbrukas i syfte att sprida terrorisminnehåll online till allmänheten. Den ger medlemsstaterna riktade verktyg, i form av avlägsnandeorder, för att ingripa mot spridningen av terrorisminnehåll online och gör det möjligt för medlemsstaterna att begära att värdtjänstleverantörer av alla storlekar när de är exponerade för terrorisminnehåll vidtar särskilda åtgärder för att skydda sina tjänster från att utnyttjas av terroristaktörer.

När förordningen om digitala tjänster trädde i kraft den 16 november 2022 utvidgades dessutom regelverket genom övergripande lagstiftning med ett brett tillämpningsområde som syftar till att säkerställa ett säkrare digitalt utrymme för konsumenter, effektiva åtgärder för att motverka olagligt innehåll och mer transparenta tjänstevillkor. Förordningen om digitala tjänster ger kommissionen omfattande tillsyns-, utrednings- och verkställighetsbefogenheter för att kunna vidta åtgärder riktade mot mycket stora onlineplattformar och sökmotorer. Dessa åtgärder omfattar begäranden om information och utredningar av företagens åtgärder för innehållsmoderering med möjlighet att ålägga böter.

Förordningen om digitala tjänster gör det möjligt att ta itu med alla former av olagligt innehåll och ger kommissionen möjlighet att uppmana plattformarna att tillhandahålla uppgifter för att visa att de lever upp till sina egna åtaganden om avlägsnande av innehåll. Förordningen om terrorisminnehåll online utgör ett ännu kraftfullare verktyg för denna specifika form av olagligt innehåll med en rättslig skyldighet att avlägsna innehåll inom en timme efter mottagandet av en avlägsnandeorder och effektiva sanktionsmekanismer.

Som Europol har betonat i de senaste årens upplagor av rapporten om den rådande situationen och tendenserna inom terrorismen i Europa (TE-SAT-rapporten)[8] använder terrorister i stor utsträckning internet för att sprida sina budskap i syfte att skrämma, radikalisera och rekrytera människor och underlätta terroristattacker. Frivilliga åtgärder och icke-bindande rekommendationer gav visserligen resultat när det gäller att minska tillgången till terrorisminnehåll

[6] Förteckning över nationella behöriga myndigheter och kontaktpunkter (europa.eu). För 23 medlemsstater finns det uppgifter i onlineregistret om vilka myndigheter som är behöriga att utfärda avlägsnandeorder i enlighet med artikel 12.1 a.

[7] Finland, Malta, Tjeckien, Danmark, Rumänien, Sverige, Lettland, Spanien, Litauen, Österrike och Slovakien.

[8] Europols TE-SAT-rapporter från 2023 https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2023.pdf respektive 2022 https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf.

online, men begränsningar, inklusive det faktum att endast få värdtjänstleverantörer införde frivilliga mekanismer[9], samt fragmenteringen av förfarandereglerna mellan olika medlemsstater ledde till att samarbetet mellan medlemsstaterna och värdtjänstleverantörerna inte kunde bli fullt ut ändamålsenligt och effektivt. Det var därför nödvändigt att vidta lagstiftningsåtgärder[10]. Därför är en effektiv tillämpning av förordningen avgörande för att åtgärda spridningen av terrorisminnehåll online. Kommissionen har proaktivt stött de nationella behöriga myndigheterna i denna process.

Enligt artikel 22 i förordningen skulle kommissionen senast den 7 juni 2023 ha lagt fram en rapport för Europaparlamentet och rådet om förordningens tillämpning (en *genomföranderapport*). Rapporten skulle ha byggt på information från medlemsstaterna, vilka i sin tur delvis skulle fått informationen från värdtjänstleverantörerna (artikel 21). Den försenade inlämningen av genomföranderapporten beror delvis på att medlemsstaterna och värdtjänstleverantörerna har dröjt med att översända viktig information till kommissionen. Dessutom ansågs det viktigt att i genomföranderapporten behandla användningen av Perci, som togs i drift den 3 juli 2023 och som sedan dess har använts för att behandla avlägsnandeorder i enlighet med förordningen.

Denna genomföranderapport syftar endast till att ge en faktamässig överblick över relevanta frågor som rör tillämpningen av förordningen. Den innehåller inga tolkningar av förordningen och uttrycker inga åsikter om tolkningar eller andra åtgärder som vidtagits i enlighet med förordningen.

Enligt artikel 21.2 i förordningen skulle kommissionen senast samma datum (7 juni 2023) ha inrättat ett detaljerat program för övervakning av förordningens utfall, resultat och effekter. Mer specifikt ska det i övervakningsprogrammet anges vilka indikatorer och metoder som ska användas för att samla in uppgifter och andra nödvändiga belägg samt med vilka intervaller insamlingen ska ske. Detta program återfinns i det åtföljande arbetsdokumentet från kommissionens avdelningar. I programmet anges de åtgärder som kommissionen och medlemsstaterna ska vidta för att samla in och analysera uppgifter och andra belägg för att övervaka framsteg och effekter av förordningen samt utvärdera den enligt dess artikel 23.

3. RAPPORTENS MÅL OCH METOD

Denna rapport syftar till att bedöma tillämpningen av förordningen samt vilken inverkan den hittills haft när det gäller att begränsa spridningen av terrorisminnehåll online. Detta inbegriper åtgärder som vidtagits av medlemsstater och värdtjänstleverantörer, såsom ändringar av leverantörernas användarvillkor och riktlinjer för nätgemenskaper och deras efterlevnad av och lyhördhet för avlägsnandeorder.

För detta ändamål har kommissionen samlat in information från medlemsstaterna, Europols enhet för anmälan av innehåll på internet (EU IRU) och värdtjänstleverantörerna, inklusive information som inkluderats i transparens- och övervakningsrapporterna i enlighet med artiklarna 7, 8 och 21 i förordningen. 18 medlemsstater inkom med information i enlighet med artiklarna 8 och 21.

[9] Europeiska kommissionen (2018), *Impact Assessment accompanying the Proposal for a Regulation on preventing the dissemination of terrorist content online* (inte översatt till svenska), SWD(2018) 408 final, hämtad den 4 maj 2023 från adressen https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN.
[10] Ibid.

Information om åtgärder som vidtagits av värdtjänstleverantörer samlades in via leverantörernas årliga transparensrapporter, Europol samt frivillig direktkommunikation med kommissionens avdelningar. I denna genomföranderapport ingår information som kommissionen mottagit till och med den 31 december 2023.

Skyldigheter avseende övervakning och transparens (artiklarna 21, 7 och 8)

För upprättandet av genomföranderapporten är medlemsstaterna enligt artikel 21.1 i förordningen skyldiga att från sina behöriga myndigheter och från värdtjänstleverantörer under sin jurisdiktion samla in information och sända den till kommissionen senast den 31 mars varje år. Detta inbegriper information om de åtgärder som de har vidtagit i enlighet med förordningen under det föregående kalenderåret. I artikel 21.1 anges den typ av information som medlemsstaterna bör samla in om åtgärder som vidtagits för att följa förordningen, såsom uppgifter om avlägsnandeorder, antalet begäranden om åtkomst till innehåll som bevaras för att möjliggöra utredningar, klagomålsförfaranden och administrativa och rättsliga prövningar.

Enligt artikel 7.1 i förordningen ska värdtjänstleverantörer i sina användarvillkor klart och tydligt ange sin strategi för att åtgärda spridningen av terrorisminnehåll, när så är lämpligt med en meningsfull förklaring av hur specifika åtgärder fungerar.

Dessutom ska, i enlighet med artikel 7.2 i förordningen, varje värdtjänstleverantör som under ett visst kalenderår har vidtagit åtgärder mot spridningen av terrorisminnehåll eller har ålagts att vidta åtgärder enligt förordningen offentliggöra en transparensrapport om dessa åtgärder för det året. Denna rapport ska offentliggöras före den 1 mars följande år.

I artikel 7.3 i förordningen fastställs den information som transparensrapporterna som minimum ska innehålla, såsom information om åtgärder för att identifiera terrorisminnehåll och göra det oåtkomligt, om antalet inslag med terrorisminnehåll som har avlägsnats och/eller återställts samt om utfallet av klagomål.

Enligt artikel 8 i förordningen ska medlemsstaternas utsedda behöriga myndigheter offentliggöra årliga transparensrapporter över den verksamhet de bedrivit enligt förordningen. I artikel 8.1 anges det vilken information dessa rapporter som minimum bör innehålla[11].

Den 31 december 2023 hade 18 medlemsstater inkommit med information till kommissionen om de åtgärder de vidtagit i enlighet med förordningen, medan 23 medlemsstater hade utsett en eller flera myndigheter med behörighet att utfärda avlägsnandeorder såsom föreskrivs i förordningen.

4. SÄRSKILDA BEDÖMNINGSPUNKTER

4.1. AVLÄGSNANDEORDER (artikel 3)

Sammantaget har kommissionen fram till den 31 december 2023 underrättats om minst 349 avlägsnandeorder som skickats till Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L.,

[11] Se texten i förordning (EU) 2021/784, artikel 8.1 https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32021R0784.

FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net och Catbox av behöriga myndigheter i Spanien, Rumänien, Frankrike, Tyskland, Österrike och Tjeckien.

62 avlägsnandeorder har skickats av den spanska behöriga myndigheten, CITCO (*Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*), medan den behöriga rumänska myndigheten (ANCOM [*Autoritatea Națională pentru Administrare și Reglementare în Comunicații*]) har skickat två avlägsnandeorder och den franska behöriga myndigheten (OCLCTIC [*L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication*]) har skickat 26 avlägsnandeorder. Sedan Hamas terroristattack mot Israel har den tyska behöriga myndigheten (BKA [*Bundeskriminalamt*]) skickat 249 avlägsnandeorder.

Den spanska behöriga myndigheten har skickat 62 avlägsnandeorder: 18 innan Perci lanserades och 44 genom Perci. Den har lämnat en detaljerad beskrivning av översändandet och uppföljningen av de första avlägsnandeorderna. Dessa upplysningar är högst relevanta för att uppnå en bättre förståelse av förordningens inverkan och effekter.

De två första avlägsnandeorderna utfärdades av den spanska behöriga myndigheten den 24 april 2023[12]. De rörde två inslag med terrorisminnehåll. I det ena fallet handlade det om högerextrem terrorism och i det andra om jihadism. Det innehåll som var föremål för den första avlägsnandeordern var ett PDF-dokument som hade lagts ut på Telegram med obegränsad åtkomst, och som förespråkade terroristvåld och förhärligade terroristattacker från högerhåll. Det inslag med terrorisminnehåll som var föremål för den andra avlägsnandeordern var en video med bilder av jihadister från terroristorganisationen ”islamiska staten” i strid som hade laddats upp på Internet Archive. Båda inslagen togs bort från respektive plattform inom en timme, alltså i enlighet med artikel 3.3 i förordningen. Den spanska behöriga myndigheten förklarar i sin bedömning att den valde att utfärda avlägsnandeorder, snarare än att göra anmälningar, främst av två skäl: överensstämmelse med förordningens krav avseende avlägsnandeorder och ärendenas brådskande karaktär. Den spanska behöriga myndigheten skickade senare ytterligare avlägsnandeorder.

Den spanska myndigheten underströk de utmaningar som uppstått i och med att en värdtjänstleverantör (Meta) använde ett webbformulär för att ta emot avlägsnandeorder i stället för att tillhandahålla en direkt kontaktpunkt. Webbformuläret försvårade också kommunikationen med den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe.

Den franska behöriga myndigheten utfärdade sin första avlägsnandeorder den 13 juli 2023 till en delningsplattform (Justpaste.it), som tog bort terrorisminnehållet inom en timme. Det berörda innehållet var propaganda från al-Qaida, mer specifikt från medieorganet Rikan Ka Mimber, från dess indiska gren al-Qaida på den indiska subkontinenten (Aqis). Det bekräftades via Europols plattform Perci att innehållet helt och hållet hade avlägsnats.

Den tyska behöriga myndigheten utfärdade 6, 16 respektive 5 avlägsnandeorder den 16, 18 respektive 24 oktober 2023 rörande propaganda från Hamas och Palestinska islamiska jihad. Innehållet gjordes oåtkomligt i EU i enlighet med artikel 3.3 i förordningen. Den tyska behöriga

[12] Ministerio del Interior | El CITCO culmina la retirada de Internet de dos contenidos que alentaban al terrorismo.

myndigheten hade först gjort anmälningar och senare utfärdat avlägsnandeorder eftersom anmälningarna inte hörsammades. Efter Hamas attack den 7 oktober 2023 har den tyska behöriga myndigheten skickat 249 avlägsnandeorder, de flesta till Telegram[13].

Den tjeckiska behöriga myndigheten och den österrikiska behöriga myndigheten utfärdade 2 respektive 8 avlägsnandeorder till X respektive Telegram.

När det gäller en värdtjänstleverantörs användning av ett webbformulär för att ta emot avlägsnandeorder påtalar spanska myndigheter följande två problem: 1. Gällande artikel 3.2 i förordningen medger ett webbformulär inte att en medlemsstats behöriga myndigheter skickar information om tillämpliga förfaranden och tidsfrister innan de utfärdar den första avlägsnandeordern till värdtjänstleverantören. 2. Gällande artikel 4.1 medger ett webbformulär inte att man samtidigt översänder en kopia av avlägsnandeordern dels till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe, dels till värdtjänstleverantörens rättsliga företrädare.

4.2 GRÄNSÖVERSKRIDANDE AVLÄGSNANDEORDER (artikel 4)

När det gäller de två första avlägsnandeorderna som utfärdades i april 2023 kunde den spanska behöriga myndigheten inte skicka kopior till myndigheten i den medlemsstat där värdtjänstleverantören hade sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare, eftersom ingen av de två värdtjänstleverantörerna vid den tidpunkten hade sitt huvudsakliga verksamhetsställe i EU eller någon utsedd rättslig företrädare i EU. När det gäller de efterföljande avlägsnandeorderna skickade den spanska myndigheten kopior till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören hade sitt huvudsakliga verksamhetsställe eller en utsedd rättslig företrädare.

Att överföra avlägsnandeorder till värdtjänstleverantörer som är baserade i tredjeländer och som ännu inte har fullgjort sin skyldighet att utse en rättslig företrädare i EU rapporterades som en utmaning av medlemsstaterna. I detta sammanhang har kommissionen hjälpt medlemsstaterna att säkerställa att värdtjänstleverantörerna fullgör sin skyldighet att utse en rättslig företrädare i EU och att tillhandahålla en kontaktpunkt (artikel 15.1 i förordningen), t.ex. en e-postadress, för att säkerställa omedelbara åtgärder. Kommissionen har dessutom påmint värdtjänstleverantörerna om deras skyldigheter i olika forum, såsom EU:s internetforum.

Enligt den information som kommissionen har tillgång till har ingen behörig myndighet i en medlemsstat där en värdtjänstleverantör har sitt huvudsakliga verksamhetsställe hittills granskat en avlägsnandeorder i enlighet med artikel 4 i förordningen för att fastställa huruvida den på ett allvarligt eller uppenbart sätt är oförenlig med förordningen eller med grundläggande rättigheter och friheter, eftersom det ännu inte har lämnats in någon motiverad begäran om granskning. Som en följd av detta har ingen myndighet hittills funnit att en avlägsnandeorder varit oförenlig med förordningen eller med grundläggande rättigheter på det sätt som avses ovan.

[13] Enligt de uppgifter som kommissionen har tillgång till.

Hittills har ingen värdtjänstleverantör återställt innehåll (eller åtkomst till innehåll) som har varit föremål för en avlägsnandeorder efter granskning i enlighet med artikel 4 i förordningen, eftersom ingen sådan granskning och inga begäranden om återställande hittills har gjorts. Det finns därför ingen tillgänglig information om hur lång tid det vanligtvis tar att återställa innehåll eller åtkomst till innehåll, eller om de ”åtgärder som krävs” som värdtjänstleverantörer vidtagit för att återställa innehåll eller åtkomst till innehåll.

4.3. RÄTTSMEDEL (artikel 9)

Enligt den information som kommissionen har tillgång till har ingen värdtjänstleverantör hittills bestridit en avlägsnandeorder som utfärdats eller ett beslut som fattats i enlighet med artikel 5.4. inför behörig domstol. En värdtjänstleverantör har dock hävdat att det inte var möjligt att verkställa en avlägsnandeorder.

Enligt den information som lämnats av medlemsstaterna[14] har minst tolv medlemsstater inrättat ”effektiva förfaranden” för att göra det möjligt för värdtjänstleverantörer och innehållsleverantörer att inför domstol i dessa medlemsstater bestrida en avlägsnandeorder som utfärdats och/eller ett beslut som fattats av medlemsstaternas behöriga myndigheter i enlighet med artikel 4.4, 5.4, 5.6 eller 5.7 (artikel 9.1 och 9.2). I medlemsstater där sådana förfaranden har införts utgörs de främst av stämningar. Huruvida dessa förfaranden är ”effektiva” eller specifika för förordningen kan dock inte fastställas med de uppgifter som mottagits från medlemsstaterna, eftersom inga beslut hittills har bestridits.

4.4. SPECIFIKA ÅTGÄRDER OCH TRANSPARENS I SAMBAND MED DESSA (artiklarna 5 och 7)

Enligt den information som finns tillgänglig har ingen värdtjänstleverantör hittills befunnits vara exponerad för terrorisminnehåll i den mening som avses i artikel 5.4 i förordningen. Följaktligen omfattas ännu ingen värdtjänstleverantör av kravet på att vidta de specifika åtgärder som anges i den artikeln.

Det kan dock noteras att flera värdtjänstleverantörer, enligt dessas transparensrapporter, har vidtagit åtgärder för att förhindra att deras tjänster missbrukas för att sprida terrorisminnehåll, särskilt genom att införa specifika användarvillkor och genom att tillämpa andra bestämmelser och åtgärder för att begränsa spridningen av terrorisminnehåll. Som nämnts ovan måste värdtjänstleverantörerna enligt artikel 7 säkerställa transparens i detta avseende, inte bara genom transparensrapportering, utan även genom att inkludera tydlig information i sina användarvillkor.

4.5. ÖVERHÄNGANDE HOT MOT EN ELLER FLERA PERSONERS LIV (artikel 14.5)

Enligt artikel 14.5 i förordningen ska värdtjänstleverantörer som får kännedom om terrorisminnehåll som medför ett överhängande hot mot en eller flera personers liv omgående underrätta de myndigheter som är behöriga att utreda och lagföra brott i de berörda

[14] Observera att de uppgifter som lämnats inte nödvändigtvis är fullständiga. Ytterligare bedömningar skulle behövas för att få en fullständig och aktuell överblick över hur medlemsstaterna verkställer kravet på att säkerställa tillgång till effektiv prövning.

medlemsstaterna. Om det är omöjligt att identifiera de berörda medlemsstaterna ska värdtjänstleverantören vidarebefordra informationen till Europol för lämplig uppföljning.

Den 31 december 2023 hade kommissionen underrättats om nio fall där Europols enhet för anmälan av innehåll på internet hade fått information om terrorisminnehåll som medförde ett överhängande hot mot en eller flera personers liv. Eftersom artikel 14.5 i förordningen inte föreskriver någon skyldighet att i samtliga fall informera Europol kan antalet fall där en myndighet i en medlemsstat underrättats vara högre. Den enda medlemsstat som lämnat information om tillämpningen av artikel 14.5 är Spanien. Den 18 april 2023 mottog de spanska myndigheterna ett meddelande från Amazon om förmodat terrorisminnehåll som medförde ett överhängande hot mot en eller flera personers liv på videospelsplattformen Twitch. Innehållet bedömdes inte uppfylla kriterierna för att utgöra terrorisminnehåll som medför ett överhängande hot mot en eller flera personers liv i den mening som avses i förordningen.

4.6. SAMARBETE MELLAN VÄRDTJÄNSTLEVERANTÖRER, BEHÖRIGA MYNDIGHETER OCH EUROPOL (artikel 14)

Som nämnts ovan har Europol utvecklat en plattform som kallas Perci i syfte att stödja genomförandet av förordningen genom att centralisera, samordna och underlätta medlemsstaternas **översändande av avlägsnandeorder och anmälningar** till värdtjänstleverantörer. Plattformen är i drift sedan den 3 juli 2023. Innan Perci tagits i bruk fullt ut hade Europol inrättat beredskapsarrangemang för att stödja manuellt översändande av avlägsnandeorder, konfliktlösning avseende innehåll för att undvika störningar av pågående utredningar samt krishantering för situationer med ”överhängande hot mot en eller flera personers liv”.

Perci är ett enhetligt system som möjliggör samarbete mellan behöriga myndigheter, värdtjänstleverantörer och Europol, i enlighet med artikel 14 i förordningen, när det gäller frågor som omfattas av förordningen. Mer konkret kan systemet beskrivas på följande sätt. Perci

- är en molnbaserad lösning som utformats för att säkerställa säkerhet och dataskydd i molnet,
- är en enhetlig plattform för samarbetsinriktad kommunikation och samordning i realtid som stöder ett snabbt avlägsnande av terrorisminnehåll,
- underlättar granskningen av gränsöverskridande avlägsnandeorder,
- stärker konfliktlösningen, vilket är viktigt för att undvika att en medlemsstats behöriga myndighet skickar en avlägsnandeorder som avser innehåll som är föremål för en pågående utredning i en annan medlemsstat och
- gör det möjligt för värdtjänstleverantörer att ta emot avlägsnandeorder på ett enhetligt och standardiserat sätt från en enda kanal.

Åtskilt från detta kan Perci också användas för översändande av anmälningar.

Utöver Percis relevans i samband med anmälningar (se skäl 40 i förordningen) underlättar systemet i dagsläget översändandet av avlägsnandeorder (artiklarna 3 och 4), medlemsstaternas rapportering (artikel 8) och samordning samt konfliktlösning i situationer där det uppstår en konflikt mellan en pågående utredning rörande visst innehåll och en avlägsnandeorder som en myndighet avser

utfärda för samma innehåll (artikel 14). Perci vidareutvecklas för närvarande för att kunna stödja fler av de uppgifter som följer av förordningen, såsom granskning av gränsöverskridande avlägsnandeorder (artikel 4)[15].

Medlemsstaterna har bekräftat att artikel 14 i förordningen följs i så måtto att

- behöriga myndigheter utbyter information, samordnar sig och samarbetar med andra behöriga myndigheter,
- behöriga myndigheter utbyter information, samordnar sig och samarbetar med Europol,
- det har inrättats mekanismer som syftar till att förbättra samarbetet och undvika att störa utredningar i andra medlemsstater.
- De flesta medlemsstater anser att Perci är det lämpligaste verktyget för att överföra avlägsnandeorder, eftersom det gör det möjligt att samordna åtgärder genom konfliktlösning.

4.7. EFFEKTER PÅ ANMÄLNINGAR

Anmälningar av terrorisminnehåll är ett frivilligt verktyg som användes redan innan förordningen antogs. Även om förordningen inte innehåller några särskilda regler om anmälningar finns det, såsom anges i skäl 40, ingenting i förordningen som hindrar medlemsstaterna och Europol från att använda anmälningar som ett verktyg för åtgärdande av terrorisminnehåll online.

Sedan den inrättades 2015 har Europols enhet för anmälan av innehåll på internet arbetat med att identifiera terrorisminnehåll online och anmäla det till värdtjänstleverantörer, samt med att upprätta verktyg (Perci och tidigare Irma[16]) för att underlätta översändandet av anmälningar.

Enligt den information som lämnats till kommissionen fortsätter medlemsstaternas myndigheter att använda anmälningar när det gäller vissa värdtjänstleverantörer, medan de kan överväga att utfärda avlägsnandeorder till värdtjänstleverantörer som inte svarar på anmälningar eller av andra skäl, t.ex. att det är brådskande att få innehållet avlägsnat.

4.8. STÖD TILL MINDRE VÄRDTJÄNSTLEVERANTÖRER FÖR GENOMFÖRANDET AV FÖRORDNINGEN

Förordningen innehåller en rad skyldigheter för värdtjänstleverantörer. Medan större värdtjänstleverantörer vanligtvis har tillräcklig teknisk kapacitet, tillräckliga personalresurser för

[15] Närmare bestämt: artiklarna 3 och 4: översändande av avlägsnandeorder, artikel 3.6–3.8: återkoppling från värdtjänstleverantörer, artikel 4.3–4.7: granskningsmekanism, artikel 7: rapportering, artikel 14.1: konfliktlösning, samordning, undvikande av dubbelarbete, artikel 14.3: säker kommunikationskanal, artikel 14.4: användning av ett särskilt verktyg som inrättats av Europol, artikel 14.5: underrättelser om ”överhängande hot mot en eller flera personers liv”, skäl 40: översändande av anmälningar.

[16] Europol utvecklade Irma (*Internet Referral Management Application*) 2016 i syfte att stödja anmälning (flaggning) av olagligt innehåll till onlinetjänsteleverantörer. Till en början gavs Europols personal och specialiserade enheter (IRU-enheter) i sju medlemsstater tillgång till Irma. Irma ersattes av Perci den 3 juli 2023.

kontroller och tillräcklig kunskap för att genomföra förordningen kan mindre leverantörers tillgång till ekonomiska, tekniska och personalmässiga resurser samt expertis för detta syfte vara mer begränsad. Samtidigt utsätts mindre värdtjänstleverantörer i allt större utsträckning för fientliga aktörer som försöker utnyttja deras tjänster. Denna utveckling kan eventuellt också hänföras till effektiva åtgärder för moderering av innehåll från de större värdtjänstleverantörernas sida. Denna trend visar hur framgångsrika åtgärderna för innehållsmoderering varit, men belyser också behovet av att hjälpa mindre värdtjänstleverantörer att öka sin kapacitet och kunskap så att de kan uppfylla kraven i förordningen.

För att möta denna utmaning inledde kommissionen en ansökningsomgång inom ramen för Fonden för inre säkerhet för att stödja mindre värdtjänstleverantörer i genomförandet av förordningen[17]. Kommissionen valde ut tre projekt[18] för att stödja leverantörerna med hjälp av en tredelad strategi. För det första genom att informera och öka medvetenheten om förordningens regler och krav, för det andra genom att utveckla, genomföra och införa de verktyg och ramar som behövs för att åtgärda spridningen av terrorisminnehåll online, och för det tredje genom att utbyta erfarenheter och bästa praxis inom branschen.

Arbetet med de tre projekten inleddes under 2023 och har redan gett värdefulla resultat. I FRISCO-projektets kartläggningsrapport[19] konstaterade man till exempel att de värdtjänstleverantörer som är mikroföretag eller små företag tenderar att ha mycket begränsad medvetenhet och kunskap om förordningen och underströk att dessa aktörer kan ha svårt att svara på avlägsnandeorder inom en timme, eftersom de sällan är tillgängliga dygnet runt, alla dagar. Resursbrist är en utmaning, liksom upprättandet av kommunikationskanaler med brottsbekämpande myndigheter. Över hälften av de värdtjänstleverantörer som undersökts av uppdragstagarna modererar inte användargenererat innehåll och uppger att de aldrig stött på terrorisminnehåll på sina plattformar. Dessa värdtjänstleverantörer kommer sannolikt att vidta ad hoc-åtgärder om sådant innehåll skulle dyka upp på deras plattformar.

Via dessa tre projekt får mindre värdtjänstleverantörer stöd i sina ansträngningar att följa förordningens regler, även genom inrättandet av kontaktpunkter och införandet av mekanismer för hantering av klagomål från användare.

Dessutom kan artikel 3.2 i förordningen – som kräver att information om tillämpliga förfaranden och tidsfrister i god tid ska tillhandahållas värdtjänstleverantörer till vilka inga avlägsnandeorder tidigare har utfärdats – vara särskilt relevant för mindre värdtjänstleverantörer.

[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.

[18] 1. En AI-baserad ram som ska stödja värdtjänstleverantörer som är mikroföretag (eller små företag) när det gäller rapportering och avlägsnande av terrorisminnehåll online (ALLIES), 2. *Fighting terrorist Content Online* (FRISCO) och 3. *Technology Against Terrorism Europe* (TATE). Mer information finns här: Finansiering och anbud (europa.eu).

[19] Arbetet med rapporten genomfördes under en sexmånadersperiod med slut i maj 2023. Rapporten bygger på återkoppling från 48 europeiska värdtjänstleverantörer, 33 svar via vår onlineundersökning samt 15 via intervjuer. 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* (inte översatt till svenska), tillgänglig på Deliverables | Frisco (friscoproject.eu).

4.9. SKYDD AV GRUNDLÄGGANDE RÄTTIGHETER

Förordningen innehåller olika skyddsåtgärder för att stärka ansvarighet och transparens avseende de åtgärder som vidtas för att avlägsna terrorisminnehåll online. I detta avseende hänvisas till det som anges ovan, särskilt informationen om rättsmedel, rapportering och den särskilda mekanismen för gränsöverskridande avlägsnandeorder.

Enligt artikel 23 i förordningen ska kommissionen dessutom rapportera om funktionen hos och ändamålsenligheten i skyddsmekanismerna, särskilt de som föreskrivs i artiklarna 4.4, 6.3 och 7–11, i samband med utvärderingen av förordningen. Dessa skyddsåtgärder utgörs av klagomålsförfaranden, rättsmedel och sanktionsmekanismer som antagits och genomförts för att hantera risken att innehåll online avlägsnas på felaktig grund och syftar till att skydda leverantörer av innehåll och värdtjänster. En bedömning av skyddsåtgärdernas funktion och ändamålsenlighet ingår därför i utvärderingen i enlighet med artikel 23.

I detta avseende fastställs i det övervakningsprogram som avses i artikel 21.2 i förordningen en ram med indikatorer som ska ligga till grund för en utvärdering av förordningens effekter på de grundläggande rättigheterna, som kommer att bidra till utvärderingen av förordningen.

Övervakningsprogrammet kommer att stödja den bedömning av funktionen hos och ändamålsenligheten i de skyddsmekanismer som införts i samband med förordningen och dessas inverkan på de grundläggande rättigheterna vilken ska genomföras som en del av utvärderingen. Denna typ av inverkan motsvarar de två områden som nämns i artikel 23 i förordningen, nämligen a) funktionen hos och ändamålsenligheten i skyddsmekanismerna, särskilt de som föreskrivs i artiklarna 4.4, 6.3 och 7–11 och b) den inverkan som tillämpningen av förordningen har på de grundläggande rättigheterna, särskilt yttrande- och informationsfriheten, respekten för privatlivet och skyddet av personuppgifter.

4.10. BEHÖRIGA MYNDIGHETER (artikel 13)

Enligt artikel 13 i förordningen måste medlemsstaterna säkerställa att deras behöriga myndigheter har de befogenheter och resurser som krävs för att uppnå målen och fullgöra sina skyldigheter enligt förordningen. Vissa medlemsstater har vidtagit följande åtgärder för att säkerställa att de behöriga myndigheterna har de befogenheter och resurser som krävs:

- Inrättande av nya organ/direktorat.
- Tilldelning av ytterligare medel och personal.
- Inrättande av nya rättsliga ramar.

5. SLUTSATS

Det är ytterst viktigt att alla verktyg och åtgärder på EU-nivå genomförs fullt ut för att snabbt ta itu med det olagliga innehåll som sprids online. Detta särskilt med tanke på det olagliga innehållets omfattning, vilket märkts nyligen genom spridningen av innehåll i samband med Hamas attack mot Israel.

Förordningen bidrar till att öka den allmänna säkerheten i hela unionen för att förhindra att värdtjänstleverantörer som är verksamma på den inre marknaden utnyttjas av terrorister i syfte att skrämma, radikalisera och rekrytera människor och underlätta terroristattacker.

Efter det att överträdelseförfaranden inleddes i januari 2023 **har framsteg gjorts**. Den 31 december 2023 hade 23 medlemsstater utsett behöriga myndigheter i enlighet med artikel 12.1, såsom återspeglas i onlineregistret, vilket leder till en mer systematisk användning av de åtgärder och verktyg som föreskrivs i förordningen. Dessutom hade elva av de 22 överträdelseförfaranden som inleddes i januari 2023 avslutats den 21 december 2023. Kommissionen uppmanar de återstående medlemsstaterna att vidta nödvändiga åtgärder för att utse behöriga myndigheter enligt artikel 12.1 och fullgöra sina skyldigheter enligt artiklarna 12.2, 12.3 och 18.1.

Generellt sett har medlemsstaterna rapporterat ett smidigt översändande av avlägsnandeorder till värdtjänstleverantörer med stöd av Europol. Baserat på den information som mottagits från medlemsstaterna och Europol har minst 349 **avlägsnandeorder för terrorisminnehåll** överförts sedan förordningen trädde i kraft. I tio fall genomförde en värdtjänstleverantör inte avlägsnandet/blockeringen av åtkomsten till terrorisminnehållet inom den tidsfrist på en timme som fastställs i förordningen.

Enligt den information som inkommit från medlemsstaterna och Europol har lyhördheten för anmälningar av terrorisminnehåll ökat sedan förordningen började tillämpas, trots att den inte innehåller några regler om detta. Europol har också i nio fall mottagit underrättelser från värdtjänstleverantörer om terrorisminnehåll som medför ett överhängande hot mot en eller flera personers liv, i enlighet med artikel 14.5.

Mer effektiva kommunikationskanaler och förfaranden har införts, särskilt i och med lanseringen av plattformen Perci den 3 juli 2023 som medförde en mer systematisk metod för överföring av avlägsnandeorder, samtidigt som Perci också i stor utsträckning används för att översända anmälningar. Medlemsstaterna och Europol förväntar sig att införandet av Perci kommer att främja användningen av dessa instrument för att bekämpa terrorisminnehåll online.

På grundval av detta bedömer kommissionen att förordningen generellt sett har haft en **positiv inverkan** när det gäller att begränsa spridningen av terrorisminnehåll online. I 10 fall av 349 överskred dock den berörda värdtjänstleverantören den tidsfrist på en timme för avlägsnande eller blockering av åtkomsten till terrorisminnehåll som fastställs i förordningen.

Kommissionen stöder proaktivt medlemsstaterna och värdtjänstleverantörerna, bland annat genom tekniska workshoppar som anordnats både före och efter förordningens ikraftträdande. Den senaste ägde rum den 24 november 2023. Kommissionen stöder också mindre värdtjänstleverantörer för att säkerställa en fullständig och snabb tillämpning av förordningen och hjälpa dem att hantera de utmaningar som hittills har uppstått.

Kommissionen kommer att fortsätta att övervaka genomförandet och tillämpningen av förordningen. Med hjälp av övervakningsprogrammet kommer kommissionen att noga övervaka hur de instrument som föreskrivs i förordningen fungerar. Resultaten av denna övervakning

kommer att utgöra en del av underlaget för utvärderingen av förordningen i enlighet med artikel 23.