EUROPESE
COMMISSIE

Brussel, 14.2.2024
COM(2024) 64 final

VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

over de uitvoering van Verordening (EU) 2021/784 inzake het tegengaan van de verspreiding van terroristische online-inhoud

{SWD(2024) 36 final}

1. SAMENVATTING

Verordening (EU) 2021/784 inzake het tegengaan van de verspreiding van terroristische online-inhoud voorziet de lidstaten van het rechtskader op Europees niveau om burgers tegen blootstelling aan terroristisch online-materiaal te beschermen. De verordening heeft tot doel te zorgen voor de goede werking van de digitale eengemaakte markt, door misbruik van hostingdiensten voor de verspreiding van terroristische online-inhoud onder het publiek tegen te gaan. Met de verordening moet worden voorkomen dat terroristen gebruikmaken van het internet om hun boodschap uit te dragen met het oog op intimidatie, radicalisering en aanwerving, en het faciliteren van terroristische aanslagen. Dit is bijzonder relevant in de huidige situatie van conflicten en instabiliteit, die gevolgen heeft voor de veiligheid van Europa. De Russische aanvalsoorlog tegen Oekraïne en de terroristische aanslag van Hamas tegen Israël op 7 oktober 2023 hebben ertoe geleid dat online meer terroristische inhoud wordt verspreid.

Het regelgevingskader om illegale online-inhoud aan te pakken werd verder versterkt met de inwerkingtreding van de digitaledienstenverordening op 16 november 2022 De digitaledienstenverordening regelt de verplichtingen van digitale diensten die optreden als tussenpersoon in hun rol om consumenten te verbinden met inhoud, diensten en goederen, waardoor gebruikers online beter worden beschermd en wordt bijgedragen aan een veiligere online omgeving.

De verordening inzake het tegengaan van de verspreiding van terroristische online-inhoud is op 7 juni 2022 in werking getreden. Overeenkomstig artikel 22 van de verordening dient de Commissie bij het Europees Parlement en bij de Raad een verslag in over de toepassing van deze verordening (“uitvoeringsverslag”).

Dit uitvoeringsverslag is gebaseerd op de beoordeling van de informatie die door de lidstaten, Europol en aanbieders van hostingdiensten is verstrekt in overeenstemming met de in de verordening vastgestelde verplichtingen. Op basis van een dergelijke beoordeling kunnen de belangrijkste bevindingen met betrekking tot de uitvoering van de verordening als volgt worden samengevat:

- Op 31 december 2023 hadden **23 lidstaten** (een) bevoegde autoriteit/autoriteiten aangewezen die bevoegd is/zijn om verwijderingsbevelen uit te vaardigen, zoals vastgesteld in de verordening[1]. De lijst van de autoriteiten van de lidstaten is beschikbaar op de website van de Commissie en wordt regelmatig bijgewerkt[2].

- Op 31 december 2023 had de Commissie informatie ontvangen over ten minste **349 verwijderingsbevelen voor terroristische inhoud** die door de bevoegde autoriteiten van zes lidstaten (Spanje, Roemenië, Frankrijk, Duitsland, Tsjechië en Oostenrijk) waren

[1] In het onlineregister, dat op grond van artikel 12, lid 4, van de verordening door de Commissie is opgezet, zijn de in artikel 12, lid 1, bedoelde bevoegde autoriteiten opgenomen, evenals het op grond van artikel 12, lid 2, voor elke bevoegde autoriteit aangewezen of opgerichte contactpunt. Het onlineregister wordt regelmatig bijgewerkt naar aanleiding van kennisgevingen van de lidstaten. Lijst van nationale bevoegde autoriteit(en) en contactpunten (europa.eu).

[2] Lijst van nationale bevoegde autoriteit(en) en contactpunten.

uitgevaardigd en die in de meeste gevallen leidden tot snelle vervolgacties van aanbieders van hostingdiensten om de terroristische inhoud te verwijderen of de toegang hiertoe te blokkeren. Hieruit blijkt dat de instrumenten waarin de verordening voorziet steeds vaker worden gebruikt en hiermee het doel wordt behaald om ervoor te zorgen dat aanbieders van hostingdiensten terroristische inhoud snel verwijderen, in overeenstemming met artikel 3, lid 3. Volgens de informatie die de Commissie heeft ontvangen, werden deze verwijderingsbevelen niet betwist.

- Er is sprake van een **goede coördinatie** tussen de bevoegde autoriteiten van de lidstaten en Europol, met name de eenheid voor de melding van internetuitingen van Europol (EU IRU), bij de toepassing van de verordening, met name bij de verwerking van verwijderingsbevelen.

- "**PERCI**"[3], een instrument van Europol, ging op 3 juli 2023 van start. Dit instrument is door sommige lidstaten met succes gebruikt voor het doorsturen van zowel verwijderingsbevelen als meldingen[4]. De Spaanse, Duitse, Oostenrijkse, Franse en Tsjechische bevoegde autoriteiten gebruikten het instrument voor het doorsturen van verwijderingsbevelen. In totaal werden tussen de start van PERCI op 3 juli en 31 december 2023 ten minste 14 615 meldingen in PERCI verwerkt.

- Hoewel de verordening geen specifieke maatregelen met betrekking tot meldingen bevat, werd er volgens de door de Commissie ontvangen informatie sinds de inwerkingtreding van de verordening ook **vaker gereageerd op meldingen** door aanbieders van hostingdiensten.

- Volgens de informatie waarover de Commissie beschikt, was op 31 december 2023 geen aanbieder van hostingdiensten blootgesteld aan terroristische inhoud in de zin van artikel 5, lid 4, van de verordening. Deze vaststelling is een voorwaarde voor de toepassing van de specifieke maatregelen die in dat artikel uiteen zijn gezet. Volgens de door de aanbieders van hostingdiensten verstrekte transparantieverslagen hebben zij desalniettemin maatregelen genomen om **het misbruik van hun diensten** voor de verspreiding van terroristische inhoud **aan te pakken**, met name door het goedkeuren van specifieke voorwaarden en de toepassing van andere bepalingen en maatregelen om de verspreiding van terroristische inhoud te beperken.

- Aanbieders van hostingdiensten hebben bovendien maatregelen vastgesteld voor de melding **van onmiddellijk levensbedreigend gevaar** op grond van artikel 14, lid 5, van de verordening.

Wat betreft **kleinere aanbieders van hostingdiensten** heeft de Commissie in 2021 een oproep tot het indienen van voorstellen gepubliceerd om hen te ondersteunen bij de uitvoering van de verordening. De Commissie gunde in 2022 een opdracht voor drie projecten (zie punt 4.8),

[3] PERCI (*Plateforme Européenne de Retraits des Contenus illégaux sur Internet*) is een platform voor het verwijderen van illegale online-inhoud dat door Europol is ontwikkeld en wordt beheerd. Het dient ter ondersteuning van de uitvoering van de verordening door, naast andere functies, een technische oplossing te bieden voor de verwerking van meldingen en verwijderingsbevelen voor aanbieders van hostingdiensten.

[4] Meldingen zijn een mechanisme om aanbieders van hostingdiensten te waarschuwen, opdat de aanbieder vrijwillig nagaat of die inhoud verenigbaar is met zijn eigen algemene voorwaarden. In de verordening (overweging 40) wordt opgemerkt dat meldingen een doeltreffend middel zijn gebleken en beschikbaar moeten blijven naast verwijderingsbevelen.

waarvan de werkzaamheden in 2023 begonnen en in het kader waarvan reeds enkele resultaten zijn behaald bij het verlenen van steun aan kleine ondernemingen met het oog op de naleving van de verordening.

De Commissie leidde inbreukprocedures tegen 22 lidstaten in vanwege het niet aanwijzen van bevoegde autoriteiten op grond van artikel 12, lid 1, van de verordening en het niet naleven van hun verplichtingen op grond van artikel 12, leden 2 en 3, en artikel 18, lid 1, door op 26 januari 2023 **ingebrekestellingen** te versturen[5]. Naar aanleiding van de inleiding van deze inbreukprocedures nam het aantal lidstaten dat de Commissie in kennis stelde van de bevoegde autoriteiten die verantwoordelijk zijn voor het behandelen van verwijderingsbevelen toe, zoals tot uiting kwam in de informatie die in het onlineregister werd gepubliceerd[6]. Daarnaast waren 11 van de in januari 2023 geopende inbreukzaken op 21 december 2023 gesloten[7].

Op basis van de van de lidstaten en Europol ontvangen informatie en de informatie die door aanbieders van hostingdiensten ter beschikking werd gesteld, concludeerde de Commissie dat de toepassing van de verordening een **positieve impact** had op het beperken van de verspreiding van terroristische online-inhoud.

2. ACHTERGROND

De verordening is op 7 juni 2022 in werking getreden. Zij heeft tot doel te zorgen voor de goede werking van de digitale eengemaakte markt, door misbruik van hostingdiensten voor de verspreiding van terroristische online-inhoud onder het publiek tegen te gaan. Zij biedt de lidstaten gerichte instrumenten, in de vorm van verwijderingsbevelen, om de verspreiding van terroristische inhoud online aan te pakken en stelt de lidstaten in staat hostingproviders, ongeacht hun omvang, te verzoeken specifieke maatregelen te nemen om hun diensten te beschermen tegen misbruik door terroristische actoren wanneer zij worden blootgesteld aan terroristische inhoud.

Met de inwerkingtreding van de digitaledienstenverordening op 16 november 2022 wordt het regelgevingslandschap bovendien uitgebreid met horizontale wetgeving met een breed toepassingsgebied die moet zorgen voor een veiligere digitale ruimte voor consumenten, doeltreffende maatregelen om illegale inhoud tegen te gaan en transparantere dienstverleningsvoorwaarden. De digitaledienstenverordening geeft de Commissie ruime toezichts-, onderzoeks- en handhavingsbevoegdheden om acties te ondernemen tegen zeer grote online platforms en zoekmachines. Deze acties omvatten verzoeken om informatie en onderzoeken naar de inhoudsmoderatieacties van bedrijven met de mogelijkheid om boeten op te leggen.

De digitaledienstenverordening maakt het mogelijk om alle vormen van illegale inhoud aan te pakken, waardoor de Commissie platforms kan vragen gegevens te verstrekken om aan te tonen dat zij hun eigen toezeggingen over het verwijderen van inhoud nakomen. Daarnaast biedt de verordening inzake terroristische online-inhoud een nog krachtiger instrument voor deze

[5] Zie persbericht: Terroristische online-inhoud (europa.eu).
[6] Lijst van nationale bevoegde autoriteit(en) en contactpunten (europa.eu). Het onlineregister bevat informatie over de autoriteiten van 23 lidstaten die bevoegd zijn voor het uitvaardigen van verwijderingsbevelen op grond van artikel 12, lid 1, punt a).
[7] Finland, Malta, Tsjechië, Denemarken, Roemenië, Zweden, Letland, Spanje, Litouwen, Oostenrijk en Slowakije.

specifieke vorm van illegale inhoud met een wettelijke verplichting om inhoud te verwijderen binnen een uur na ontvangst van een verwijderingsbevel en effectieve sanctiemechanismen.

Zoals opgemerkt door Europol in de verslagen over de stand van zaken en de tendensen in verband met het terrorisme (TE-SAT-verslagen)[8] die in de afgelopen jaren werden gepubliceerd, maken terroristen uitvoerig gebruik van het internet voor het uitdragen van hun boodschap met het oog op het intimideren, het radicaliseren, het werven, en het faciliteren van terroristische aanslagen. Hoewel vrijwillige maatregelen en niet-bindende aanbevelingen hun vruchten afwierpen wat betreft het beperken van de beschikbaarheid van terroristische online-inhoud, leidden beperkingen, waaronder het kleine aantal aanbieders van hostingdiensten die vrijwillige mechanismen toepasten[9], alsook de versnippering van de procedureregels in de lidstaten, ertoe dat de doeltreffendheid en de efficiëntie van de samenwerking tussen de lidstaten en aanbieders van hostingdiensten werd beperkt, waardoor het nodig werd om regelgeving vast te stellen[10]. De doeltreffende toepassing van de verordening is daarom essentieel voor het aanpakken van de verspreiding van terroristische online-inhoud. De Commissie heeft de nationale bevoegde autoriteiten proactief ondersteund in dit proces.

Overeenkomstig artikel 22 van de verordening was de Commissie verplicht om uiterlijk 7 juni 2023 een verslag over de toepassing van de verordening ("uitvoeringsverslag") in te dienen bij het Europees Parlement en de Raad, voortbouwend op door de lidstaten verstrekte informatie, die weer gedeeltelijk was gebaseerd op informatie die door aanbieders van hostingdiensten werd verstrekt (artikel 21). De vertraging bij de indiening van het uitvoeringsverslag is enerzijds het gevolg van de late toezending aan de Commissie van belangrijke informatie van de lidstaten en aanbieders van hostingdiensten. Anderzijds werd het van belang geacht om in het uitvoeringsverslag het gebruik van PERCI op te nemen, dat op 3 juli 2023 operationeel werd en sindsdien wordt gebruikt voor het verwerken van verwijderingsbevelen overeenkomstig de verordening.

Dit uitvoeringsverslag is er slechts op gericht een feitelijk overzicht te geven van de relevante kwesties in verband met de toepassing van de verordening. Het bevat geen uitleggingen van de verordening, noch enig standpunt met betrekking tot uitleggingen of andere maatregelen die bij de toepassing van de verordening zijn genomen.

Overeenkomstig artikel 21, lid 2, van de verordening moest de Commissie uiterlijk op dezelfde datum (7 juni 2023) een gedetailleerd programma vaststellen voor de monitoring van de outputs, resultaten en effecten van de verordening. Meer specifiek moesten in het monitoringprogramma de indicatoren en middelen worden vermeld waarmee, evenals de tijdstippen waarop de gegevens en ander nodig bewijsmateriaal moesten worden verzameld. Een dergelijk programma is vastgesteld in het begeleidende werkdocument van de diensten van de Commissie. Hierin zijn de maatregelen gespecificeerd die de Commissie en de lidstaten bij het verzamelen en analyseren van

[8] TE-SAT-verslag van Europol 2023 https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2023.pdf en 2022 https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

[9] Europese Commissie, (2018) Impact Assessment accompanying the Proposal for a Regulation on preventing the dissemination of terrorist content online, SWD(2018) 408 final, geraadpleegd op 4.5.2023 op: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN

[10] Zie vorige voetnoot.

de gegevens en ander bewijsmateriaal moeten nemen om de voortgang en de effecten van de verordening te monitoren en om de verordening op grond van artikel 23 te evalueren.

3. DOEL EN METHODE VAN HET VERSLAG

Dit verslag heeft tot doel de toepassing van de verordening en de effecten ervan tot nu toe wat betreft het beperken van de verspreiding van terroristische online-inhoud te beoordelen. Dit omvat door de lidstaten en aanbieders van hostingdiensten getroffen maatregelen, zoals wijzigingen van hun voorwaarden en gemeenschapsrichtlijnen en hun naleving van en reacties op verwijderingsbevelen.

Daartoe heeft de Commissie informatie van de lidstaten, de eenheid voor de melding van internetuitingen van Europol (EU IRU) en aanbieders van hostingdiensten verzameld, met inbegrip van informatie uit de transparantie- en monitoringverslagen op grond van de artikelen 7, 8 en 21 van de verordening. Van 18 lidstaten werd informatie op grond van de artikelen 8 en 21 ontvangen. Informatie over door aanbieders van hostingdiensten getroffen maatregelen werd verzameld aan de hand van hun jaarlijkse transparantieverslagen en via Europol en een rechtstreekse vrijwillige communicatie met de diensten van de Commissie. Dit uitvoeringsverslag bevat informatie die de Commissie tot 31 december 2023 heeft ontvangen.

Monitoring- en transparantieverplichtingen (de artikelen 21, 7 en 8)

Met het oog op het vaststellen van het uitvoeringsverslag moeten de lidstaten overeenkomstig artikel 21, lid 1, van de verordening informatie verzamelen bij hun bevoegde autoriteiten en de onder hun rechtsmacht vallende aanbieders van hostingdiensten en deze elk jaar uiterlijk op 31 maart aan de Commissie zenden. Dit omvat informatie over de acties die zij in overeenstemming met de verordening in het vorige kalenderjaar hebben ondernomen. In artikel 21, lid 1, wordt verwezen naar het soort informatie dat de lidstaten moeten verzamelen met betrekking tot maatregelen die zijn getroffen om de verordening na te leven, zoals gedetailleerde informatie over verwijderingsbevelen, het aantal verzoeken om toegang tot inhoud die is bewaard met het oog op onderzoeken, klachtenprocedures en administratieve of gerechtelijke toetsingsprocedures.

Overeenkomstig artikel 7, lid 1, van de verordening moeten aanbieders van hostingdiensten in hun algemene voorwaarden duidelijk hun beleid voor het tegengaan van de verspreiding van terroristische inhoud vaststellen, met inbegrip van, waar passend, een omstandige toelichting van de werking van specifieke maatregelen.

Daarnaast maakt een aanbieder van hostingdiensten die op grond van deze verordening in een bepaald kalenderjaar maatregelen heeft genomen of heeft moeten nemen om de verspreiding van terroristische inhoud tegen te gaan, op grond van artikel 7, lid 2, van de verordening een transparantieverslag openbaar over de maatregelen die in die periode zijn genomen. Dat verslag moet vóór 1 maart van het volgende jaar worden gepubliceerd.

In artikel 7, lid 3, van de verordening is de informatie uiteengezet die deze transparantieverslagen ten minste moeten bevatten, zoals maatregelen die zijn genomen om terroristische inhoud te

identificeren en de toegang hiertoe te blokkeren, het aantal items dat is verwijderd en/of hersteld en het resultaat van klachten.

Overeenkomstig artikel 8 van de verordening publiceren de aangewezen bevoegde autoriteiten van de lidstaten jaarlijkse transparantieverslagen over hun activiteiten in het kader van de verordening. In artikel 8, lid 1, wordt verwezen naar de informatie die deze verslagen ten minste moeten bevatten[11].

Op 31 december 2023 hadden 18 lidstaten informatie aan de Commissie gezonden over de maatregelen die zij hadden getroffen in overeenstemming met de verordening, terwijl 23 lidstaten (een) autoriteit(en) hebben aangewezen die bevoegd is/zijn voor het uitvaardigen van verwijderingsbevelen, zoals vastgesteld in de verordening.

4. SPECIFIEKE BEOORDELINGSPUNTEN

4.1. VERWIJDERINGSBEVELEN (artikel 3)

De Commissie was op 31 december 2023 in kennis gesteld van ten minste 349 verwijderingsbevelen die door de bevoegde autoriteiten van Spanje, Roemenië, Frankrijk, Duitsland, Oostenrijk en Tsjechië aan Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L, FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net en Catbox werden verstuurd.

62 verwijderingsbevelen werden verstuurd door de Spaanse bevoegde autoriteit — CITCO (*Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*), terwijl de Roemeense bevoegde autoriteit (ANCOM — *Autoritatea Națională pentru Administrare și Reglementare în Comunicații*) 2, en de Franse bevoegde autoriteit (OCLCTIC — *L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication*) 26 verwijderingsbevelen verstuurden. Sinds de terroristische aanslag van Hamas tegen Israël heeft de Duitse bevoegde autoriteit (BKA — *Bundeskriminalamt*) 249 verwijderingsbevelen verstuurd.

De Spaanse bevoegde autoriteit heeft 62 verwijderingsbevelen verstuurd: 18 voorafgaande aan de start van PERCI en 44 via PERCI. De Spaanse bevoegde autoriteit verstrekte een gedetailleerde beschrijving van het versturen en de follow-up van de eerste verwijderingsbevelen, die zeer relevant is om de gevolgen en effecten van de verordening beter te begrijpen.

De eerste twee verwijderingsbevelen werden op 24 april 2023 door de Spaanse bevoegde autoriteit verstuurd[12]. Deze hielden verband met twee items met terroristische inhoud: één met betrekking tot rechts terrorisme en het andere met betrekking tot jihadisme. De inhoud die het voorwerp van het eerste verwijderingsbevel vormde, was een pdf-document dat op Telegram met onbeperkte toegang was gepost, waarin werd gepleit voor terroristisch geweld en waarin rechtse terroristische aanslagen werden verheerlijkt. Het item met terroristische inhoud dat het voorwerp van het tweede verwijderingsbevel vormde, was een video met beelden van jihadstrijders van de terroristische

[11] Zie de tekst van Verordening (EU) 2021/784, artikel 8, lid 1, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32021R0784

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

organisatie Islamitische Staat in gevecht, dat was geüpload op Internet Archive. Deze twee items met inhoud werden in minder dan een uur van beide platforms verwijderd, wat in overeenstemming is met artikel 3, lid 3, van de verordening. In de door de Spaanse bevoegde autoriteit verstrekte beoordeling werd uitgelegd dat zij om twee hoofdredenen de voorkeur had gegeven aan een verwijderingsbevel boven een melding: de naleving van de vereisten van de verordening inzake verwijderingsbevelen en de dringendheid. De Spaanse bevoegde autoriteit heeft vervolgens ettelijke verwijderingsbevelen verstuurd.

De Spaanse autoriteit wees op problemen in verband met het gebruik van een onlineformulier door één aanbieder van hostingdiensten (Meta) voor het ontvangen van verwijderingsbevelen, in plaats van te voorzien in een direct contactpunt. Dit onlineformulier leidde ook tot problemen bij de communicatie met de bevoegde autoriteit van de lidstaat waar zich de hoofdvestiging van de aanbieder van hostingdiensten bevindt.

De Franse bevoegde autoriteit vaardigde haar eerste verwijderingsbevel op 13 juli 2023 uit tegen een uitwisselingsplatform (Justpaste.it), dat de terroristische inhoud binnen een uur verwijderde. De inhoud waarom het ging, was propaganda van Al-Qa'ida, en meer specifiek van het mediaorgaan van deze organisatie, Rikan Ka Mimber, van de Indiase tak, Al Qa'ida Indian Sub continent (AQIS). De volledige verwijdering van de inhoud werd bevestigd op het platform van Europol, PERCI.

De Duitse bevoegde autoriteit vaardigde zes, zestien en vijf verwijderingsbevelen uit op 16, 18 en 24 oktober 2023, die betrekking hadden op respectievelijk propaganda van Hamas en de Palestijnse Islamitische Jihad. De toegang tot de inhoud werd in de EU geblokkeerd in overeenstemming met artikel 3, lid 3, van de verordening. De Duitse bevoegde autoriteit had eerst meldingen verstuurd en vervolgens verwijderingsbevelen uitgevaardigd, omdat niet werd gehandeld naar aanleiding van deze meldingen. Na de aanslag van Hamas op 7 oktober 2023 verstuurde de Duitse bevoegde autoriteit 249 verwijderingsbevelen, voornamelijk aan Telegram[13].

De Tsjechische bevoegde autoriteit en de Oostenrijkse bevoegde autoriteit hebben 2 en 8 verwijderingsbevelen uitgevaardigd, respectievelijk aan X en Telegram.

Wat betreft het gebruik van een onlineformulier voor het ontvangen van verwijderingsbevelen van één aanbieder van hostingdiensten, wezen de Spaanse autoriteiten op twee problemen: 1) in de context van artikel 3, lid 2, van de verordening stelt een onlineformulier de bevoegde autoriteiten van de lidstaten niet in staat om vóór het uitvaardigen van het eerste verwijderingsbevel aan de aanbieder van hostingdiensten informatie over de toepasselijke procedures en termijnen te versturen; 2) in de context van artikel 4, lid 1, maakt een onlineformulier het niet mogelijk om tegelijkertijd een afschrift van het verwijderingsbevel bij de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging heeft, en bij de wettelijke vertegenwoordiger van de aanbieder van hostingdiensten in te dienen.

[13] Volgens de informatie waarover de Commissie beschikt.

4.2. GRENSOVERSCHRIJDENDE VERWIJDERINGSBEVELEN (artikel 4)

Voor de eerste twee verwijderingsbevelen die in april 2023 werden uitgevaardigd, kon de Spaanse bevoegde autoriteit geen afschriften versturen aan de autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging had of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats had, omdat geen van beide aanbieders van hostingdiensten op dat moment zijn hoofdvestiging of een wettelijke vertegenwoordiger in de EU had. Voor de latere verwijderingsbevelen verstuurde de Spaanse bevoegde autoriteit afschriften aan de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging had of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats had.

Het versturen van verwijderingsbevelen aan aanbieders van hostingdiensten in derde landen die hun verplichting tot het aanwijzen van een wettelijk vertegenwoordiger in de EU nog niet zijn nagekomen, werd door de lidstaten als probleem gemeld. De Commissie ondersteunde de lidstaten in dit verband bij het waarborgen dat aanbieders van hostingdiensten hun verplichting tot het aanwijzen van een wettelijk vertegenwoordiger in de EU en het voorzien in een contactpunt (artikel 15, lid 1, van de verordening), zoals een e-mailadres, nakomen, om onmiddellijk optreden te verzekeren. De Commissie heeft aanbieders van hostingdiensten bovendien op verschillende fora, waaronder het EU-Internetforum, aan hun verplichtingen herinnerd.

Volgens de informatie waarover de Commissie beschikt, heeft tot nu toe geen bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging heeft een verwijderingsbevel getoetst op grond van artikel 4 van de verordening om te bepalen of het een ernstige of kennelijke inbreuk op de verordening of op de grondrechten en vrijheden inhoudt, aangezien er nog geen met redenen omkleed verzoek om een toetsing is ingediend. Als gevolg hiervan heeft tot nu toe nog geen autoriteit op deze wijze vastgesteld dat een verwijderingsbevel een inbreuk op deze verordening of op de grondrechten inhoudt.

Tot nu toe heeft geen aanbieder van hostingdiensten de inhoud die voorwerp van een verwijderingsbevel was op grond van een toetsing krachtens artikel 4 van de verordening hersteld of weer toegankelijk gemaakt, omdat dergelijke toetsingen en verzoeken om herstel nog niet hebben plaatsgevonden. Er is derhalve geen informatie beschikbaar over hoe lang het normaal gesproken duurt om inhoud te herstellen of weer toegankelijk te maken of over de “nodige maatregelen” die aanbieders van hostingdiensten nemen om de inhoud te herstellen of weer toegankelijk te maken.

4.3. VOORZIENINGEN IN RECHTE (artikel 9)

Volgens de informatie waarover de Commissie beschikt, hebben aanbieders van hostingdiensten geen verwijderingsbevelen of besluiten op grond van artikel 5, lid 4, voor de desbetreffende rechterlijke instanties betwist. Eén aanbieder van hostingdiensten stelde echter dat het onmogelijk was om een verwijderingsbevel uit te voeren.

Volgens de door de lidstaten verstrekte informatie[14] beschikken ten minste twaalf lidstaten over "doeltreffende procedures" om aanbieders van hostingdiensten en aanbieders van inhoud in staat te stellen een uitgevaardigd verwijderingsbevel en/of een op grond van artikel 4, lid 4, of artikel 5, leden 4, 6 of 7, genomen besluit te betwisten voor de rechterlijke instantie van de lidstaat van de bevoegde autoriteit (artikel 9, leden 1 en 2). In lidstaten waar in deze procedures is voorzien, hebben dergelijke procedures voornamelijk betrekking op rechtszaken. Of deze procedures "doeltreffend" of specifiek voor de verordening zijn, kan echter niet worden vastgesteld op basis van de momenteel van de lidstaten ontvangen informatie, aangezien er tot nu toe geen besluiten zijn betwist.

4.4. SPECIFIEKE MAATREGELEN EN HIERAAN GERELATEERDE TRANSPARANTIE (de artikelen 5 en 7)

Volgens de beschikbare informatie is tot nu toe geen aanbieder van hostingdiensten blootgesteld aan terroristische inhoud in de zin van artikel 5, lid 4, van de verordening. Als gevolg hiervan is de vereiste om de in dat artikel uiteengezette specifieke maatregelen te nemen (nog) niet van toepassing op enige aanbieder van hostingdiensten.

Er kan desalniettemin worden opgemerkt dat verschillende aanbieders van hostingdiensten, volgens de door hen verstrekte transparantieverslagen, maatregelen hebben genomen om het misbruik van hun diensten voor de verspreiding van terroristische inhoud aan te pakken, met name het goedkeuren van specifieke voorwaarden en de toepassing van andere bepalingen en maatregelen om de verspreiding van terroristische inhoud te beperken. Zoals hierboven opgemerkt, moeten aanbieders van hostingdiensten op grond van artikel 7 de transparantie in dit verband niet alleen waarborgen aan de hand van de verslaglegging over de transparantie, maar ook door duidelijke informatie op te nemen in hun algemene voorwaarden.

4.5. ONMIDDELLIJK LEVENSBEDREIGEND GEVAAR (artikel 14, lid 5)

Overeenkomstig artikel 14, lid 5, van de verordening lichten aanbieders van hostingdiensten, indien zij kennis krijgen van terroristische inhoud die een onmiddellijk levensbedreigend gevaar inhoudt, snel de autoriteiten in die in de betrokken lidstaten bevoegd zijn voor het onderzoek en de vervolging van strafbare feiten. Indien het onmogelijk is de betrokken lidstaten te bepalen, geven de aanbieders van hostingdiensten de informatie door aan Europol met het oog op passende follow-up.

Op 31 december 2023 was de Commissie in kennis gesteld van negen gevallen waarin de EU-eenheid voor de melding van internetuitingen van Europol informatie had ontvangen over terroristische inhoud die een onmiddellijk levensbedreigend gevaar inhield. Omdat artikel 14, lid 5, van de verordening niet voorziet in een verplichting om Europol in alle gevallen in te lichten, kan het aantal meldingen hoger zijn. De enige lidstaat die informatie over de toepassing van artikel 14, lid 5, verstrekte, was Spanje. Op 18 april 2023 ontvingen de Spaanse autoriteiten een mededeling van Amazon over een vermoed item met terroristische inhoud die een onmiddellijk

[14] Er moet worden opgemerkt dat de verstrekte informatie niet noodzakelijkerwijs volledig is. Nadere beoordelingen zouden nodig zijn om een volledig en volledig actueel overzicht te verkrijgen van de wijze waarop de lidstaten uitvoering hebben gegeven aan de eis van het waarborgen van de beschikbaarheid van doeltreffende beroepsprocedures.

levensbedreigend gevaar inhield op het videospellenplatform Twitch. Na een beoordeling werd vastgesteld dat de inhoud niet voldeed aan de voorwaarden om te worden aangemerkt als terroristische inhoud die een onmiddellijk levensbedreigend gevaar inhoudt in de zin van de verordening.

4.6. SAMENWERKING TUSSEN AANBIEDERS VAN HOSTINGDIENSTEN, BEVOEGDE AUTORITEITEN EN EUROPOL (artikel 14)

Zoals hierboven opgemerkt, heeft Europol een platform ontwikkeld, met de naam "PERCI", dat de uitvoering van de verordening ondersteunt door **het versturen van verwijderingsbevelen en meldingen** door de lidstaten aan aanbieders van hostingdiensten te centraliseren, te coördineren en te vereenvoudigen. Het platform is sinds 3 juli 2023 operationeel. Voordat PERCI volledig werd uitgevoerd, had Europol voorzien in noodregelingen ter ondersteuning van het handmatige versturen van verwijderingsbevelen, deconflictering van inhoud om inmenging in lopende onderzoeken te vermijden en een crisisrespons in situaties waarin sprake is van een "onmiddellijk levensbedreigend gevaar".

PERCI is een enkel systeem dat de samenwerking tussen bevoegde autoriteiten, aanbieders van hostingdiensten en Europol mogelijk maakt, zoals voorzien in artikel 14 van de verordening met betrekking tot kwesties die onder de verordening vallen. Meer concreet is PERCI:

- een cloudgebaseerde oplossing die is ontworpen om de beveiliging en gegevensbescherming in de cloud te waarborgen;
- één platform voor samenwerking door middel van realtimecommunicatie en coördinatie, dat de snelle verwijdering van terroristische online-inhoud ondersteunt;
- een systeem dat het toetsingsproces voor grensoverschrijdende verwijderingsbevelen vereenvoudigt;
- een systeem dat de deconflictering versterkt, wat van belang is om te voorkomen dat een bevoegde autoriteit van een lidstaat een verwijderingsbevel verstuurt dat gericht is op inhoud die voorwerp is van een lopend onderzoek in een andere lidstaat;
- een systeem dat aanbieders van hostingdiensten in staat stelt om verwijderingsbevelen op uniforme en gestandaardiseerde wijze te ontvangen via één kanaal.

PERCI maakt daarnaast ook het versturen van meldingen mogelijk.

Momenteel vereenvoudigt PERCI, naast de relevantie ervan in verband met meldingen (zie overweging 40 van de verordening), het versturen van verwijderingsbevelen (de artikelen 3 en 4), de verslaglegging door de lidstaten (artikel 8) en de coördinatie, evenals deconflictering in het geval van strijdigheden met lopende onderzoeken naar de inhoud ten aanzien waarvan een verwijderingsbevel wordt beoogd (artikel 14). PERCI wordt op dit moment verder ontwikkeld om

aanvullende taken te ondersteunen die uit de verordening voortvloeien, zoals de toetsing van grensoverschrijdende verwijderingsbevelen (artikel 4)[15].

De lidstaten bevestigden dat, overeenkomstig artikel 14 van de verordening:

- de bevoegde autoriteiten informatie uitwisselen, coördineren en samenwerken met andere bevoegde autoriteiten;
- de bevoegde autoriteiten informatie uitwisselen, coördineren en samenwerken met Europol;
- er mechanismen bestaan om de samenwerking te versterken, terwijl inmenging in onderzoeken die in andere lidstaten worden uitgevoerd, wordt voorkomen;
- de meeste lidstaten PERCI zien als het voorkeursinstrument voor het versturen van verwijderingsbevelen, aanzien het coördinatie en optreden middels deconflictering mogelijk maakt.

4.7. GEVOLGEN VOOR MELDINGEN

Meldingen van terroristische inhoud zijn een vrijwillig middel dat reeds vóór de goedkeuring van de verordening werd gebruikt. Hoewel de verordening geen specifieke regels inzake meldingen bevat, belet, overeenkomstig overweging 40 van de verordening, niets in de verordening de lidstaten en Europol om meldingen te gebruiken als instrument om terroristische online-inhoud tegen te gaan.

Sinds de oprichting ervan in 2015 is de EU-eenheid voor de melding van internetuitingen van Europol actief op het gebied van het identificeren van terroristische online-inhoud en het melden hiervan aan aanbieders van hostingdiensten, alsook op het gebied van het vaststellen van instrumenten (d.w.z. PERCI en daarvoor IRMa[16]) om het versturen van meldingen te vereenvoudigen.

Volgens de aan de Commissie verstrekte informatie gebruiken de autoriteiten van de lidstaten voor bepaalde aanbieders van hostingdiensten nog steeds meldingen, terwijl zij verwijderingsbevelen overwegen ten aanzien van aanbieders van hostingdiensten die niet op meldingen reageren of om andere redenen, zoals de noodzaak van een snelle verwijdering van de inhoud.

---

[15] Meer bepaald: — de artikelen 3 en 4: versturen van verwijderingsbevelen; — artikel 3, leden 6 tot en met 8: feedback van aanbieders van hostingdiensten; — artikel 4, leden 3 tot en met 7: toetsingsmechanisme; — artikel 7: verslaglegging; — artikel 14, lid 1: deconflictering, coördinatie, voorkomen van dubbel werk; — artikel 14, lid 3: veilig communicatiekanaal; — artikel 14, lid 4: gebruik van een speciaal instrument dat is ingesteld door Europol; — artikel 14, lid 5: communicatie over “onmiddellijke levensbedreigende gevaren”; — overweging 40: versturen van meldingen.

[16] Europol ontwikkelde de toepassing voor het beheer van de melding van internetuitingen (IRMa) in 2016 om de melding (markering) van illegale inhoud aan aanbieders van onlinediensten te ondersteunen. IRMa kon in eerste instantie beschikken over personeel van Europol en gespecialiseerde eenheden (IRU’s) in zeven lidstaten. Op 3 juli 2023 werd IRMa vervangen door PERCI.

4.8. STEUN VOOR KLEINERE AANBIEDERS VAN HOSTINGDIENSTEN VOOR DE UITVOERING VAN DE VERORDENING

De verordening bevat verschillende verplichtingen voor aanbieders van hostingdiensten. Terwijl grote aanbieders van hostingdiensten doorgaans over het technische vermogen, de menselijke-verificatiecapaciteit en kennis beschikken om de verordening uit te voeren, hebben kleinere aanbieders van hostingdiensten hiervoor mogelijk beperktere financiële, technische en menselijke middelen en expertise. Kleinere aanbieders van hostingdiensten zijn tegelijkertijd steeds vaker het doelwit van kwaadwillige actoren die hun diensten misbruiken. Dit kan ook het gevolg zijn van de doeltreffende inhoudsmoderatie van grotere aanbieders van hostingdiensten. Hoewel deze trend het succes van maatregelen voor inhoudsmoderatie laat zien, maakt hij ook duidelijk dat kleinere aanbieders van hostingdiensten moeten worden ondersteund bij het uitbreiden van hun capaciteit en kennis om de vereisten van de verordening na te leven.

Om deze uitdaging aan te gaan, publiceerde de Commissie een oproep tot het indienen van voorstellen in het kader van het Fonds voor interne veiligheid om kleinere aanbieders van hostingdiensten te ondersteunen bij het uitvoeren van de verordening[17]. De Commissie selecteerde drie projecten[18] om hen aan de hand van een drieledige benadering te ondersteunen. Ten eerste door te informeren over en het bewustzijn te vergroten van de regels en vereisten van de verordening, ten tweede door instrumenten en kaders te ontwikkelen, uit te voeren en uit te rollen die nodig zijn om de verspreiding van terroristische online-inhoud aan te pakken en ten derde door ervaringen en beste praktijken in de gehele industrie te delen.

De drie projecten begonnen hun werkzaamheden in 2023 en hebben reeds waardevolle resultaten geboekt. In het "mapping report" van het FRISCO-project[19] werd bijvoorbeeld geconstateerd dat micro- en kleine aanbieders van hostingdiensten vaak zeer weinig bewustzijn en kennis van de verordening hebben en werden mogelijke problemen onderstreept waarmee zij te maken zouden kunnen krijgen bij het binnen een uur reageren op verwijderingsbevelen, aangezien zij vaak niet over diensten beschikken die 24 uur per dag beschikbaar zijn. Een gebrek aan middelen is een probleem, net zoals het voorzien in communicatielijnen met rechtshandhavingsinstanties. Meer dan de helft van de door de contractanten ondervraagde aanbieders van hostingdiensten modereert door gebruikers gegenereerde inhoud niet en is nog nooit terroristische inhoud op zijn platform tegengekomen. Deze aanbieders van hostingdiensten nemen waarschijnlijk ad-hocmaatregelen wanneer dergelijke inhoud op hun platform verschijnt.

Aan de hand van deze drie projecten worden kleine aanbieders van hostingdiensten ondersteund bij het leveren van inspanningen om de regels van de verordening na te leven, ook door middel

[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) Op AI gebaseerd kader ter ondersteuning van micro- (en kleine) aanbieders van hostingdiensten bij het melden en verwijderen van terroristische online-inhoud (ALLIES); 2) Fighting terrorist Content Online (FRISCO); en 3) Technology Against Terrorism Europe (TATE). Zie de link voor meer informatie: Funding & tenders (europa.eu).

[19] Verricht gedurende een periode van zes maanden tot mei 2023. Het verslag is gebaseerd op feedback van 48 Europese aanbieders van hostingdiensten, waarvan 33 antwoorden op onze online-enquête en 15 interviews. FRISCO, *D2.1: Mapping Report on needs and barriers for compliance Understanding small and micro HSPs' needs and awareness in relation to implementing the TCO Regulation requirements*, beschikbaar op Deliverables | Frisco (friscoproject.eu).

van het opzetten van contactpunten en het uitvoeren van mechanismen voor klachten van gebruikers.

Daarnaast kan artikel 3, lid 2, van de verordening — dat vereist dat tijdig informatie wordt verstrekt aan aanbieders van hostingdiensten waaraan nog niet eerder een verwijderingsbevel is uitgevaardigd over de toepasselijke procedures en termijnen — met name voor kleinere aanbieders van hostingdiensten relevant zijn.

4.9. WAARBORGEN VOOR DE GRONDRECHTEN

De verordening bevat verschillende waarborgen om de verantwoordingsplicht en transparantie in verband met maatregelen ter verwijdering van terroristische online-inhoud te versterken. In dit verband wordt verwezen naar het bovenstaande, en met name de informatie over voorzieningen in rechte, de verslaglegging en het speciale mechanisme voor grensoverschrijdende verwijderingsbevelen.

Artikel 23 van de verordening vereist bovendien dat de Commissie in het kader van de evaluatie van de verordening verslag uitbrengt over de werking en de doeltreffendheid van de waarborgmechanismen, met name de waarborgmechanismen van artikel 4, lid 4, artikel 6, lid 3, en de artikelen 7 tot en met 11. Dergelijke waarborgen betreffen klachten, voorzieningen in rechte en sanctiemechanismen die zijn goedgekeurd en worden toegepast om het risico op onterechte verwijdering van terroristische online-inhoud te beperken, teneinde aanbieders van inhoud en aanbieders van hostingdiensten te beschermen. De beoordeling van de werking en de doeltreffendheid van de waarborgmechanismen zal derhalve deel uitmaken van de evaluatie op grond van artikel 23.

In dit opzicht is in het monitoringprogramma als bedoeld in artikel 21, lid 2, van de verordening een kader van indicatoren vastgesteld voor de evaluatie van de effecten van de verordening op de grondrechten, dat zal worden meegenomen bij de evaluatie van de verordening.

Het monitoringprogramma zal dienen ter ondersteuning van de beoordeling van de werking en de doeltreffendheid van de waarborgmechanismen die in het kader van de verordening worden toegepast en de gevolgen hiervan voor de grondrechten, die moet worden uitgevoerd als onderdeel van de evaluatie. De impact op dit gebied heeft betrekking op de twee gebieden die in artikel 23 van de verordening worden genoemd: a) de werking en de doeltreffendheid van de waarborgmechanismen, met name de waarborgmechanismen waarin in artikel 4, lid 4, artikel 6, lid 3, en in de artikelen 7 tot en met 11 is voorzien; en b) de impact van de toepassing van deze verordening op de grondrechten, met name de vrijheid van meningsuiting en van informatie, de eerbiediging van het privéleven en de bescherming van persoonsgegevens.

4.10. BEVOEGDE AUTORITEITEN (artikel 13)

Overeenkomstig artikel 13 van de verordening moeten de lidstaten ervoor zorgen dat hun bevoegde autoriteiten over de nodige bevoegdheden en voldoende middelen beschikken om de doelstellingen uit hoofde van de verordening te verwezenlijken en hun verplichtingen uit hoofde van de verordening na te komen. Sommige lidstaten hebben de volgende maatregelen uitgevoerd

om te waarborgen dat de bevoegde autoriteiten over de nodige bevoegdheden en voldoende middelen beschikken:

- de oprichting van nieuwe organen/directoraten;
- de toewijzing van aanvullende middelen en aanvullend personeel; en
- het creëren van nieuwe wetgevingskaders.

5. CONCLUSIE

Het is van het grootste belang dat alle instrumenten en maatregelen op EU-niveau volledig worden geïmplementeerd om de illegale inhoud die online wordt verspreid, snel aan te pakken. Dit is vooral het geval gezien de enorme omvang van dergelijke illegale inhoud, zoals onlangs nog bleek uit de verspreiding van inhoud in verband met de aanval van Hamas op Israël.

De verordening draagt bij tot een grotere openbare veiligheid in de Unie door te voorkomen dat aanbieders van hostingdiensten die op de interne markt actief zijn, door terroristen worden gebruikt voor het uitdragen van hun boodschap met het oog op het intimideren, het radicaliseren, het werven, en het faciliteren van terroristische aanslagen.

Na de inleiding van inbreukprocedures in januari 2023 **is vooruitgang geboekt**. Op 31 december 2023 hadden 23 lidstaten bevoegde autoriteiten aangewezen op grond van artikel 12, lid 1, zoals weerspiegeld in het onlineregister, wat leidde tot een systematischer gebruik van de maatregelen en instrumenten waarin in de verordening is voorzien. Daarnaast waren 11 van de 22 in januari 2023 geopende inbreukzaken op 21 december 2023 gesloten. De Commissie dringt er bij de overige lidstaten op aan de noodzakelijke stappen te nemen om de bevoegde autoriteiten aan te wijzen op grond van artikel 12, lid 1, en hun verplichtingen uit hoofde van artikel 12, leden 2 en 3, en artikel 18, lid 1, na te komen.

Over het algemeen meldden de lidstaten een soepele versturing van verwijderingsbevelen aan aanbieders van hostingdiensten met steun van Europol. Op basis van de van de lidstaten en Europol ontvangen informatie werden sinds de inwerkingtreding van de verordening ten minste 349 **verwijderingsbevelen voor terroristische inhoud** verstuurd. In tien gevallen werd de terroristische inhoud door één aanbieder van hostingdiensten niet binnen het in de verordening vastgestelde maximum van één uur verwijderd/ontoegankelijk gemaakt.

Volgens de van de lidstaten en Europol ontvangen informatie werd er, ondanks het feit dat de verordening geen regels in dit verband bevat, sinds de inwerkingtreding van de verordening vaker gereageerd op meldingen van terroristische inhoud. Europol ontving bovendien in negen gevallen informatie van aanbieders van hostingdiensten over terroristische inhoud die een onmiddellijk levensbedreigend gevaar inhield, op grond van artikel 14, lid 5.

Met name sinds de start van het PERCI-platform op 3 juli 2023 bestaan efficiëntere communicatiekanalen en -procedures, die hebben geleid tot een systematischer benadering van het versturen van verwijderingsbevelen, terwijl PERCI ook wordt gebruikt voor het versturen van een groot aantal meldingen. De lidstaten en Europol verwachten dat het gebruik van PERCI het gebruik van deze instrumenten om terroristische online-inhoud aan te pakken, zal bevorderen.

Op basis hiervan is de Commissie van oordeel dat de verordening over het algemeen een **positieve impact** heeft gehad op het beperken van de verspreiding van terroristische online-inhoud. In 10 van de 349 gevallen werd de in de verordening vastgestelde maximale periode van één uur voor het verwijderen van terroristische inhoud of het blokkeren van de toegang daartoe door de gebruikte aanbieder van hostingdiensten overschreden.

De Commissie steunt de lidstaten en aanbieders van hostingdiensten op proactieve wijze, onder meer door middel van technische workshops die voorafgaande aan en na de inwerkingtreding van de verordening werden georganiseerd. De meest recente workshop vond op 24 november 2023 plaats. De Commissie steunt ook kleinere aanbieders van hostingdiensten bij het waarborgen van een volledige en snelle toepassing van de verordening en het aanpakken van de uitdagingen waarmee zij tot nu toe te maken hebben gekregen.

De Commissie blijft de uitvoering en toepassing van de verordening in het oog houden. De Commissie zal de prestaties van de instrumenten waarin in de verordening is voorzien nauwlettend monitoren aan de hand van het monitoringprogramma, dat zal dienen als input voor de evaluatie van de verordening op grond van artikel 23.