

Brussel, 12.9.2018
SWD(2018) 409 final

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN DE EFFECTBEOORDELING

bij

**Voorstel voor een verordening van het Europees Parlement en de Raad
ter voorkoming van de verspreiding van terroristische online-inhoud**

{COM(2018) 640 final} - {SEC(2018) 397 final} - {SWD(2018) 408 final}

Samenvatting
Effectbeoordeling over de voorkoming van de verspreiding van terroristische online-inhoud
A. Behoeftte aan actie
Waarom? Wat is het probleem?
De verspreiding van terroristische online-inhoud blijft een groot en dringend maatschappelijk en politiek probleem. Ondanks een aantal niet-regelgevende maatregelen worden onlinehostingdiensten nog altijd gebruikt voor de verspreiding van terroristische inhoud.
Wat moet met dit initiatief worden bereikt?
Dit initiatief wil een groter vertrouwen in de onlineomgeving in de digitale eengemaakte markt bewerkstelligen door de beschikbaarheid van terroristische online-inhoud te beperken, en tegelijkertijd de EU-burgers een hoog veiligheidsniveau te garanderen. Specifiek wil het de maatregelen voor het opsporen en verwijderen van terroristische inhoud doeltreffender maken en de transparantie en verantwoordingsplicht van aanbieders van hostingdiensten vergroten. De maatregel wil ook de betrokken autoriteiten beter in staat stellen om tegen terroristische online-inhoud op te treden, waarborgen bieden tegen het risico van onterechte verwijdering van legale inhoud en voorzien in een passende bescherming van de grondrechten.
Wat is de meerwaarde van maatregelen op EU-niveau?
De meeste onlineplatforms zijn grensoverschrijdend actief en maken inhoud toegankelijk, ongeacht waar de gebruikers of de aanbieders van inhoud zich bevinden. De lidstaten hebben wetgeving aangenomen op het gebied van de verwijdering van illegale online-inhoud, maar er moet een evenwicht worden gevonden tussen het feit dat de openbare veiligheid op nationaal niveau moet worden gegarandeerd, en de fundamentele vrijheid van dienstverlening en vrijheid van vestiging op grond van de regels inzake de eengemaakte markt. Er ontstaat een onsamenhangend kader van nationale regels dat steeds groter dreigt te worden, wat een doeltreffende uitoefening van de vrijheid van vestiging en de vrijheid van dienstverlening in de EU in gevaar zou brengen, terwijl ook de strijd tegen terroristische online-inhoud minder doeltreffend wordt, omdat het bedrijfsleven met hogere nalevingskosten zou worden geconfronteerd. Het optreden van de lidstaten alleen kan niet op doeltreffende wijze de beschikbaarheid van illegale online-inhoud beperken, gelet op de aard van de betrokken diensten en de toenemende versnippering van de interne markt.
B. Oplossingen
Welke wetgevende en niet-wetgevende beleidsmaatregelen zijn overwogen? Heeft een bepaalde optie de voorkeur? Waarom?
De effectbeoordeling heeft naast het basisscenario drie opties in overweging genomen, die uitgaan van dezelfde logica voor het optreden maar een verschillende intensiteit hebben qua doeltreffendheid en gevolgen voor de grondrechten. De opties kunnen volgende onderdelen omvatten: Bepalingen voor de harmonisatie van de procedures om terroristische inhoud te verwijderen of ontoegankelijk te maken na een verwijderingsbevel van een nationale autoriteit. Om de procedures mogelijk te maken, omvat harmonisatie verder een gemeenschappelijke definitie van terroristische online-inhoud (elk van de drie opties voorziet in een andere definitie), alsook duidelijkheid over de rechtsmiddelen die aanbieders van hostingdiensten en aanbieders van inhoud kunnen instellen tegen verwijderingsbevelen (gemeenschappelijk element van alle opties). Bepalingen om te zorgen voor transparante processen en rapportage aan de autoriteiten en aan de Commissie (dezelfde in alle opties) zouden de verantwoordingsplicht en het vertrouwen in het proces van het modereren van inhoud vergroten, en zouden beleidsmakers en nationale autoriteiten ondersteunen in hun strijd tegen terroristische inhoud. Daarnaast zouden gebruikers beter kunnen begrijpen hoe aanbieders van hostingdiensten hun contentmanagementbeleid toepassen.

Samenwerking tussen nationale autoriteiten en Europol (met een verschillende intensiteit naargelang de optie) zou hen beter in staat stellen om collectief op te treden tegen terroristische inhoud en dubbel werk te voorkomen, en zou de interactie van aanbieders van hostingdiensten die hun diensten over de grenzen heen aanbieden, met nationale autoriteiten minder complex maken en de kosten daarvan verminderen.

Daarnaast zijn er bepalingen om te garanderen dat aanbieders van hostingdiensten **passende en evenredige maatregelen nemen om proactief terroristische inhoud op te sporen** ingeval ondernemingen aan terroristische inhoud zijn blootgesteld (verschillende vereisten naargelang de optie).

Waarborgen (gemeenschappelijk element van alle opties) en bepalingen om te garanderen dat de maatregelen om terroristische inhoud op te sporen en te verwijderen, niet tot onterechte verwijdering van legale inhoud leiden en de grondrechten eerbiedigen.

Bepalingen **om te garanderen dat maatregelen kunnen worden gehandhaafd** (gemeenschappelijk element van alle opties), waaronder de aanwijzing van wettelijke vertegenwoordigers voor ondernemingen van buiten de EU, de aanwijzing van contactpunten en het verzekeren dat de lidstaten over een coherente reeks sancties beschikken.

Het verslag presenteert een combinatie van de maatregelen die volgens de beoordeling het meest doeltreffend zijn in de strijd tegen terroristische online-inhoud. Het presenteert ook een evaluatie van de voordelen van de verschillende onderdelen qua doeltreffendheid.

De effectbeoordeling concludeert dat het opnemen van maatregelen zoals een ruime definitie van terroristische inhoud, de verplichting gemelde inhoud binnen één uur te verwijderen door middel van verwijderingsbevelen, de toetsing van doorverwijzingen door Europol en de lidstaten, alsook de verplichting voor aanbieders van hostingdiensten die aan terroristische inhoud zijn blootgesteld, om proactieve maatregelen te nemen om nieuwe terroristische inhoud op te sporen en te voorkomen dat bekend materiaal opnieuw wordt geüpload, en een solide reeks waarborgen tegen onterechte verwijdering van legale inhoud en transparantieverplichtingen, doeltreffender zou zijn om de beleidsdoelstellingen te verwezenlijken.

Wie steunt welke optie?

Aanbieders van hostingdiensten zijn doorgaans voorstander van het basisscenario, omdat zij van oordeel zijn dat de volledige effecten van niet-regelgevende inspanningen eerst moeten worden geëvalueerd. Als een rechtsinstrument wordt aangenomen, zijn zij voorstander van een gerichte interventie met betrekking tot specifieke kwesties die van bijzondere openbare waarde zijn.

De lidstaten erkennen dat er verdere ondersteunende maatregelen moeten worden genomen (d.w.z. voortgezette ontwikkeling van het basisscenario) en ondersteunen een interventie tegen terroristische inhoud. De lidstaten wijzen meer bepaald op de noodzaak van een gemeenschappelijke definitie van terroristische inhoud, de verplichting tot het ondernemen van actie na doorverwijzingen, proactieve maatregelen en transparantie en maatregelen om ervoor te zorgen dat verwijderde inhoud toegankelijk is voor rechtshandavingsdoeleinden. De Europese Raad heeft de Commissie opgeroepen "een wetgevingsvoorstel in te dienen ter verbetering van het opsporen en verwijderen van inhoud die tot haat en terreurdaden aanzet".

Maatschappelijke organisaties op het gebied van digitale rechten en academici zijn voorstander van de ontwikkeling van het basisscenario. Zij waarschuwen voor sommige onderdelen van de regelgevende opties, meer bepaald wat de proactieve maatregelen en de gevolgen voor de grondrechten betreft. Ook particulieren tonen zich hierover bezorgd in hun antwoorden op de openbare raadpleging: een representatieve steekproef van burgers in een speciale Eurobarometer was voorstander van aanvullende maatregelen op EU-niveau ter bestrijding van illegale online-inhoud.

C. Kosten en voordelen van de voorkeursoptie

Deze effectbeoordeling geeft een gedetailleerde beschrijving van de kosten en voordelen voor de maatregelen waarin de verschillende opties voorzien. De conclusie luidt dat optie 3 het doeltreffendst is. De beleidsoptie zou aanzienlijk bijdragen aan de verwezenlijking van de beleidsdoelstellingen en zou de meeste voordelen

opleveren in verhouding tot de omvang en draagwijdte van het probleem. De derde optie heeft naar verwachting het grootste economische effect met betrekking tot de verwachte kosten en extra administratieve lasten, maar zou ook de grootste voordelen opleveren.

D. Opvolging

Wanneer wordt dit beleid geëvalueerd?

Er zal een gedetailleerd programma worden vastgesteld voor de monitoring van de outputs, resultaten en effecten van de wetgeving, zodat die in de evaluatie daarvan kunnen worden meegenomen. De monitoring zal in de eerste plaats gebaseerd zijn op informatie van de lidstaten die door de bevoegde autoriteiten is verzameld in de uitvoering van hun taken, aangevuld met de openbare transparantieverslagen. Andere gegevens, met name over de proactieve maatregelen, zullen worden verstrekt door aanbieders van hostingdiensten in het kader van hun rapportageverplichtingen. Deze monitoring zal in alle opties worden aangevuld met onderzoek dat wordt verricht om de verspreiding van illegale online-inhoud beter te begrijpen en de technologische evolutie op het gebied van automatische instrumenten voor de verwijdering van illegale inhoud in kaart te brengen.