

A4 - Online radicalisering, extremisme en terrorisme

Wat is het probleem?

Online radicalisering neemt toe. Extremisten misbruiken vooral sociale media en gamingplatforms om hun ideologie te verspreiden, jongeren te rekruteren en aanslagen voor te bereiden. Zowel jihadistische als rechtsextremistische groepen bereiken jongeren steeds eerder, en het radicaliseringsproces verloopt sneller. Recente arrestaties laten zien dat (steeds jonger wordende) jongeren kwetsbaar zijn voor deze online propaganda, wat kan leiden tot deelname aan extremistische netwerken en het plannen van aanslagen en wat een zorgelijk en groeiend risico vormt voor de nationale veiligheid en de democratische rechtsstaat.

NB. Dit A4 gaat in op online content m.b.t. terrorisme, extremisme en radicalisering. Er bestaan daarnaast veel andere vormen van onwenselijke en/of illegale online content, zoals het online aanbieden van illegale producten (drugs, wapens), de verspreiding van kinderpornografisch beeldmateriaal, het online aanjagen van openbare-ordeverstoringen en het verspreiden van desinformatie. Ook de Digitale Dienstenverordening (DSA) is breed toepasbaar op allerlei vormen van illegale content.

Welke ervaring is er met contentmoderatie op grond van de DSA?

Online platformen hebben een cruciale rol in het tegengaan van online materiaal dat extremistisch en terroristisch gedachtegoed verspreidt. Op basis van de Verordening Terroristische Online Inhoud (TOI) is in Nederland sinds 2024 een onafhankelijke autoriteit operationeel die terroristisch materiaal kan laten verwijderen dan wel ontoegankelijk kan laten maken. Deze Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) stuurt wekelijks verwijderbevelen aan de platformen. De DSA is een bestuursrechtelijk middel om online contentmoderatie door tussenhandeldiensten (zoals hostingdiensten, websites en online platformen) beter af te kunnen dwingen, bijvoorbeeld door middel van het opleggen van boetes. In Nederland is de Autoriteit Consument en Markt aangewezen als handhaver voor de DSA. De DSA is sinds februari 2024 van toepassing op tussenhandeldiensten en bevat diverse bepalingen voor contentmoderatie. De DSA en de TOI-verordening vormen daarmee een belangrijke basis voor het tegengaan van illegale en terroristische content.

Hoewel de wetgeving van recente datum is, is wel duidelijk dat de nadruk vooral ligt op het verwijderen van content en de technische inrichting van online tussenhandeldiensten. Zo gaat het gaat bij de DSA om contentmoderatie op het *openbare* internet. Tussenhandeldiensten, met name online platforms, wordt een aantal verplichtingen opgelegd waar ze aan moeten voldoen om op de Nederlandse en Europese markt te mogen opereren. Interpersoonlijke communicatiediensten (zoals Whatsapp/Signal) en besloten chatgroepen vallen buiten de definitie van een online platform; veel verplichtingen in de DSA zijn op hen niet van toepassing.

De DSA biedt de regels waar tussenhandeldiensten zich aan moeten houden in hun ontwerp en hoe zij moeten handelen richting gebruikers van hun diensten en nationale autoriteiten. De DSA bepaalt niet zelf wat illegale inhoud is. In de DSA wordt daarvoor verwezen naar wat nationaal of Europees verboden is.

Daarnaast is de ervaring tot nu toe dat de DSA, die slechts een deel van de aanpak bestrijkt, niet toereikend is in de bestrijding van online radicalisering omdat de verspreiders van illegale en terroristische content steeds behendiger worden in het laveren binnen de grenzen van de regelgeving. Ondanks de huidige online contentmoderatie, onder de DSA (waarbij tussenhandeldiensten vooral leunen op geautomatiseerde contentmoderatie), zijn er met slechts een paar klikken nog steeds talloze beelden op het internet te vinden van onder andere onthoofdingen, naziverheerlijking en jihadistische propaganda.

Tot slot verplicht de DSA op dit moment geen proactieve contentmoderatie aan tussenhandeldiensten. Zij hebben geen plicht om zich aan de voorkant al zoveel als mogelijk te verzekeren dat hun dienst of platform geen illegale inhoud bevat of verspreidt. Tussenhandeldiensten hebben onder de DSA ook geen zorgplicht ten aanzien van hun gebruikers.

Welke maatregelen?

Een effectieve bestrijding vraagt om meer bewustwording, strikter normeren en vaker/snelser ingrijpen. Er is een verscheidenheid aan partners betrokken (publiek, privaat, nationaal en internationaal). De inzet is gebaat bij een meer gecoördineerde aanpak. In het online domein is het van belang extra maatregelen te treffen:

- Normerende dialoog met de internetsector en concrete samenwerkingen met platformen, bijvoorbeeld in de vorm van pilots, zoals toepassing van de Re-Direct-methode met Meta.¹ Het voornemen is om hiervoor in 2026 een nieuwe gespreksronde op te zetten. Deze gesprekken zijn onderdeel van een bredere inzet vanuit het rijk op publiek-private samenwerking met de internetsector.
- Extra inzet op Europees niveau:
 - In samenspraak met de online platformen komen tot maatregelen voor een betere bescherming van gebruikers, het delen van signalen van online radicalisering en het tegengaan van zogeheten 'platform migratie', waarbij platformen een ingang vormen naar besloten chatgroepen op problematische platformen.

¹ De ReDirect-methode is een functie waarbij mensen die online zoeken naar extremistische of terroristische content in aanraking komen met een informatieveld waarbij zij worden doorgestuurd naar online hulp (LSE).

Deze trapsgewijze benadering is een fundamenteel element van het rekruteringsproces. Idealiter in de vorm van een *gedragscode* op EU-niveau, zoals voorgesteld in een recent NL-Duits-Frans non-paper.²

- Middels een *zorgplicht* kunnen online platformen worden verplicht om meer proactief verantwoordelijkheid te nemen en maatregelen te nemen ten aanzien van de verspreiding van illegale content. Nederland heeft in de onderhandelingen voor de DSA het opnemen van een zorgplicht bepleit. Nederland heeft vanwege de uitstekende digitale infrastructuur een grote hosting- en online platformmarkt, maar dat zorgt ook voor relatief veel illegale inhoud op Nederlandse servers. Denk hierbij aan de grote hoeveelheid aan kinderpornografisch materiaal op Nederlandse servers. Een zorgplicht zou voor de Nederlandse handhavingspraktijk enorm helpen, omdat hostingbedrijven en online platforms dan zelf meer maatregelen nemen om te voorkomen dat ze worden misbruikt voor illegale doeleinden. Helaas was er bij andere EU-lidstaten toen geen meerderheid voor een zorgplicht. In 2027 zal de DSA worden geëvalueerd; dat moment biedt mogelijk kansen voor – het opnieuw bepleiten van – het invoeren van een zorgplicht. Een dergelijke zorgplicht is reeds van kracht in het Verenigd Koninkrijk.
- Inzetten op een *werkbare definitie van (gewelddadige) extremistische content* als opmaat naar terrorisme.
- *Uitbreiding instrumentarium* van de ATKM en meer inzet op verwijderverzoeken (referrals) voor (gewelddadige) extremistische content ter aanvulling op verwijderbevelen voor terroristische content.
- Lokaal vergroten van digitale weerbaarheid (in het bijzonder onder jongeren), trainen van lokale professionals in herkennen van online radicalisering en het inbedden van het *online domein binnen de lokale aanpak*. Inclusief meer mogelijkheden voor zicht op online signalen en het betrekken van de signalen.
- *Sterkere coördinatie* op aanpak voor het bewaken van onderlinge samenhang en synergie om versnippering te voorkomen. Vanuit de Tweede Kamer zijn wensen geuit om in te zetten op een gecoördineerde aanpak op online, met hierin een (mogelijke) rol voor de NCTV.
- *Versteving wettelijk instrumentarium*: bij de evaluatie van de DSA in 2027 zal Nederland inzetten op verdere aanscherping waar nodig en het belang van effectieve contentmoderatie en een zorgplicht benadrukken.

Wat is ervoor nodig?

De samenwerking met de online platformen én behoud van commitment onder de stakeholders en internationale partners heeft prioriteit. Voor maatregelen, zoals een gedragscode en zorgplicht, (innovatieve) initiatieven met online platformen, een gecoördineerde aanpak, een nieuwe EU-brede terrorismebestrijdingsagenda, zijn extra financiële middelen en capaciteitsinzet benodigd. Additionele kosten hiervoor bedragen naar verwachting (ten minste) 2 mln. euro per jaar. Het gaat hier om extra inzet gericht op online radicalisering, extremisme en terrorisme, maar deze inzet zal, bijvoorbeeld met de inzet op de voornoemde zorgplicht, ook gedeeltelijk effect hebben op het bredere maatschappelijke probleem van kwetsbare groepen die in aanraking komen met schadelijke online content of met personen die gebruik maken van internet om schade toe te brengen.

² <https://www.rijksoverheid.nl/documenten/kamerstukken/2025/12/17/tk-non-paper-online-radicalisering-gewelddadig-extremisme-en-terrorisme>