

Vergaderjaar 2025–2026

34 843

Seksuele intimidatie en geweld

Nr. 128

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 november 2025

Online seksueel geweld is een ernstig en groeiend probleem en heeft een verwoestende impact op slachtoffers. De gevolgen van online seksueel geweld worden verergerd door de aanhoudende circulatie van het beeldmateriaal op het internet en de angst voor verdere verspreiding, wat de verwerking belemmert en slachtoffers isoleert. Online seksueel geweld betreft ongewenst seksueel gedrag of een seksuele handeling die via digitale middelen plaatsvindt, zoals websites, sociale media, apps, fora of berichtenservices, waarbij iemand wordt lastiggevalen, bedreigd, geïntimideerd of misbruikt. Deze problematiek heeft onze volledige aandacht en draagt een hoge urgentie.

Op 21 maart 2025 heeft Boekx Advocaten, in samenwerking met Offlimits, Stichting Landelijk Centrum Seksueel Geweld, Privacy First en Fonds Slachtofferhulp, het rapport «Online seksueel geweld» gepubliceerd, zoals meegezonden met deze brief. In dit rapport wordt geconcludeerd dat de huidige aanpak van online seksueel geweld op bepaalde punten, waaronder handhaving en toezicht, tekortschiet en worden aanbevelingen gedaan om de aanpak te versterken. Op 3 april 2025 is tijdens het commissiedebat zeden en (on)veiligheid van vrouwen (Kamerstuk 34 843, nr. 122) toegezegd een beleidsreactie op het rapport naar de Tweede Kamer te sturen. Met deze brief voldoe ik aan deze toezegging. Eveneens wordt de motie van het lid Van Nispen c.s. van 28 mei 2025 om de aanbevelingen uit het rapport over te nemen afgedaan door aan te geven hoe de aanbevelingen worden overgenomen en toe te lichten waarom sommige delen niet overgenomen worden. Ook wordt met deze brief het deel van de motie afgedaan dat verzoekt de uitbreiding van de Autoriteit online Terroristisch en Kinderpornografisch Materiaal te onderzoeken.¹

Met deze brief reageer ik namens het kabinet op het rapport Online seksueel geweld. Ik ga eerst in op de algemene kabinetsinzet en de reeds genomen maatregelen tegen online seksueel geweld (zie onder 1).

¹ Kamerstukken II, 2024–2025, 29 279, nr. 959.

Vervolgens wordt ingegaan op de aanbevelingen uit het rapport (zie onder 2).

Tenslotte wordt aandacht besteed aan de vraag of het mandaat van de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) kan worden uitgebreid naar evident onrechtmatig materiaal van volwassenen (zie onder 3). In de bijlage onderaan deze brief treft uw Kamer een overzicht van de bevoegdheden van de betrokken toezichthouders.

1. Algemene reactie en kabinetsinzet

Het rapport Online seksueel geweld laat zien dat de exponentiële groei van de digitale wereld ook haar schaduwzijden vergroot. Geconstateerd wordt dat het eenvoudig is om online seksueel beeldmateriaal te plaatsen en te verspreiden, terwijl het complex is om dit materiaal weer te verwijderen.² Het rapport erkent de effectieve aanpak van online seksueel kindermisbruik maar benadrukt dat er – ondanks de kabinetsinspanningen – op het gebied van online seksueel geweld nog veel verbetering mogelijk is.³ Volgens het rapport vormen met name het gebrek aan prioriteit bij toezichthouders en handhavers de grootste barrière voor een effectieve aanpak, wat leidt tot langdurig leed bij slachtoffers. Daarnaast signaleert het rapport tekortkomingen in de strafrechtelijke handhaving en de preventieve aanpak van online seksueel geweld.

Inzet kabinet op de bestrijding van online seksueel geweld

Het kabinet dankt de opstellers voor het rapport en voor hun betrokkenheid bij de aanpak van deze ernstige problematiek. Online seksueel geweld is een breed en complex fenomeen dat binnen de Rijksoverheid, politie en het Openbaar Ministerie (hierna: OM) op verschillende niveaus en binnen diverse gespecialiseerde teams wordt behandeld. De bestrijding van online seksueel geweld heeft prioriteit voor het kabinet, mede door de impact van deze delicten op slachtoffers en daarmee op onze maatschappij als geheel. De afgelopen jaren heeft het kabinet ingezet op versterking van de integrale aanpak van deze problematiek waarin niet alleen is ingezet op het versterken van de strafrechtelijke bescherming van slachtoffers, maar ook breed is ingezet op preventie, slachtofferondersteuning en informatievoorziening. Dit wordt hieronder nader toegelicht.

Met de inwerkingtreding van de Wet seksuele misdrijven (hierna: WSM) op 1 juli 2024, is de strafrechtelijke bescherming van slachtoffers tegen seksueel geweld in de digitale dimensie versterkt. Het uitgangspunt is nu dat wat offline strafbaar is, ook online strafbaar is.

Een belangrijk onderdeel van de integrale aanpak van JenV is onder andere de subsidie aan de Stichting Offlimits. Offlimits biedt met haar hulplijnen en meldpunten preventie, hulp en ondersteuning bij online seksueel geweld in vele vormen. Hun hulplijn Helpwanted speelt dan ook een cruciale rol in de bestrijding van dit fenomeen. Een belangrijke ontwikkeling is de toekenning van de formele *trusted flagger* status aan Offlimits door de Autoriteit Consument en Markt (hierna: ACM) op basis van de Digital Services Act (hierna: DSA). Dit betekent dat verwijderverzoeken van Offlimits prioritair en onverwijld door online tussenhandel-

² Paragraaf 2.1 van het rapport

³ De aanpak van seksueel kindermisbruik, een subthema binnen seksueel geweld, is dan ook één van de prioriteiten van het Kabinet, zie: <https://www.rijksoverheid.nl/documenten/publicaties/2024/09/13/regeerprogramma-kabinet-schoof>.

diensten behandeld moeten worden. Offlimits is de eerste organisatie aan wie de ACM een dergelijke status heeft toegekend.

Tevens dragen de Ministeries van JenV en OCW bij aan diverse preventietrajecten, waaronder de recente actualisatie van de «Wegwijzer seksualiteit online». De wegwijzer biedt (onderwijs)professionals praktische handvatten bij incidenten van online seksueel grensoverschrijdend gedrag. Ook geeft de wegwijzer een overzicht van preventieve hulpmiddelen en staan er handreikingen voor docentprofessionalisering, beleidsvorming en ouderbetrokkenheid in. Het Ministerie van JenV onderzoekt, in samenwerking met een consortium met expertorganisaties, politie en OCW, bovendien mogelijke aanvullende gedragsinterventies tegen het onderling doorsturen van schadelijk materiaal (zoals seksueel beeldmateriaal) in besloten online groepsgesprekken op bijvoorbeeld Whatsapp, Snapchat of Telegram.

Daarnaast zet het kabinet met het Nationaal Actieprogramma Aanpak seksueel grensoverschrijdend gedrag en seksueel geweld (hierna: NAP) in een samenwerkingsverband tussen OCW, SZW, VWS en JenV in op de meerjarige brede aanpak om dit maatschappelijke probleem aan te pakken.⁴ Dit met het doel seksueel grensoverschrijdend gedrag en seksueel geweld te voorkomen, te herkennen, aan te pakken en hulp te bieden aan de slachtoffers. Het NAP zet in op een cultuurverandering waarin dergelijk gedrag, ook online, niet wordt getolereerd. Het programma richt zich op preventie, wet- en regelgeving, hulpverlening en onderzoek. Online gedrag krijgt hierin nadrukkelijk aandacht, onder meer via publiekscampagnes, projecten zoals «Seksuele Opvoeding door Ouders» (Rutgers), de alliantie Act4Respect en onderzoek als T@CKLE (Nationale Wetenschapsagenda). Jongeren leren over de impact van online seksueel grensoverschrijdend gedrag en mediawijsheid krijgt een stevigere plek in het onderwijs.

Verder wordt door de bij het NAP betrokken departementen en de regeringscommissaris seksueel grensoverschrijdend gedrag en seksueel geweld verkend hoe omstanders online actiever kunnen worden. Deze inzet sluit aan op bredere Rijksbrede trajecten, zoals het Project Online Content Moderatie (JenV), het netwerk Mediawijsheid (OCW), Richtlijn Gezond Schermgebruik voor opvoeders (VWS)⁵ en het project tegen online discriminatie, racisme en hate speech. Waar mogelijk worden initiatieven met elkaar verbonden.

Nederland beschikt daarnaast over een uitgebreid en onafhankelijk toezichthouderslandschap, bestaande uit verschillende autoriteiten met elk hun eigen expertise waarbij ieder valt onder de verantwoordelijkheid van een departement. Binnen ons toezichthouderslandschap bewaakt de Autoriteit Persoonsgegevens (hierna: AP) (JenV) onze persoonsgegevens, terwijl de ACM (EZ) zorgt voor eerlijke concurrentie en consumentenbescherming online. Het Commissariaat voor de Media (CvdM) (OCW) houdt toezicht op videoplatformdiensten en video-uploaders («influencers»), bevordert betrouwbaar en pluriform media-aanbod en zet zich in voor een veilige online omgeving voor jongeren. Relatief nieuw is de ATKM: een autoriteit waar het Ministerie van Justitie en Veiligheid het initiatief toe heeft genomen om een verschil te maken in de hosting van materiaal van seksueel kindermisbruik in Nederland. De ATKM is gericht op het

⁴ <https://www.rijksoverheid.nl/onderwerpen/aanpak-seksueel-grensoverschrijdend-gedrag-en-seksueel-geweld/nationaal-actieprogramma-aanpak-seksueel-grensoverschrijdend-gedrag-en-seksueel-geweld>.

⁵ De richtlijn gaat niet expliciet over online seksueel geweld, maar er staat wel in wat opvoeders kunnen bespreken met hun kind als er grensoverschrijdend gedrag online plaatsvindt.

detecteren, beoordelen en laten verwijderen van deze specifieke content op basis van haar bestuursrechtelijke bevoegdheden. Hoewel de ATKM enkel kan acteren op materiaal van kinderen, is zij wel een belangrijke speler in handhaving op online seksueel geweld.

De toezichthouders informeren burgers en bedrijven, voeren controles uit en handhaven de regels met waarschuwingen, boetes of andere maatregelen. De toezichthouders werken steeds vaker samen bij online kwesties. Deze samenwerking en hun autonomie zijn cruciaal voor een betrouwbaar en veilig digitaal Nederland. Voor meer details over hun bevoegdheden verwijs ik naar de bijlage onderaan deze brief.

Hoewel deze toezichthouders veelal zelfstandig opereren en een onafhankelijke juridische positie innemen, draagt het kabinet de eindverantwoordelijkheid voor het stelsel van het toezicht in Nederland. Deze verantwoordelijkheid betreft in de eerste plaats het scheppen van de randvoorwaarden waarbinnen toezichthouders hun werk goed kunnen doen. Denk hierbij aan het wettelijk kader, de *governance*, en de financiering. De inhoudelijke oordeelsvorming in individuele toezichtzaken valt echter nadrukkelijk buiten de invloedsfeer van het kabinet. In beginsel moeten toezichthouders hun wettelijke taken onafhankelijk en onpartijdig vervullen; politieke of ambtelijke inmenging in operationele beslissingen is daarbij ongewenst en in strijd met de beginselen van behoorlijk bestuur. Tegelijkertijd blijft het kabinet aanspreekbaar op de werking van het toezichtstelsel als geheel. Indien zich structurele knelpunten of disfunctioneren van een toezichthouder voordoen, wordt van het kabinet verwacht dat het passende maatregelen treft.

2. Reactie op aanbevelingen

Om de in het rapport geschetste problematiek aan te pakken wordt een aantal aanbevelingen gedaan. Hieronder wordt toegelicht op welke wijze invulling wordt gegeven aan de gedane aanbevelingen en uitgelegd waarom niet alle aanbevelingen integraal worden overgenomen, zoals de motie Van Nispen c.s. verzoekt.

a. Prioritering en samenwerking

De opstellers van het rapport bevelen aan dat toezichthouders en handhavende instanties online seksueel geweld per 1 januari 2026 als prioriteit opnemen. Ze zouden hun rol, verwachtingen en behoeftes helder moeten definiëren. Ook dient er een periodiek, niet-vrijblijvend overleg te worden georganiseerd tussen toezichthouders, handhavers en relevante partijen zoals Offlimits. De opstellers van het rapport bevelen daarnaast aan dat toezichthouders en handhavende instanties vanaf 1 januari 2026 jaarlijks rapporteren over hun inspanningen ter bescherming van slachtoffers van online seksueel geweld.

Toezichthouders onderschrijven de aanpak van online seksueel geweld breed en zijn bereid de samenwerking, waar mogelijk, verder te versterken. Toezichthouders werken al effectief samen in verschillende verbanden, zoals de DSA-Kamer en het multilateraal samenwerkingsprotocol.⁶

⁶ Toezichthouders in Nederland werken samen via de DSA-Kamer, opgericht door het Samenwerkingsplatform Digitale Toezichthouders (SDT), met de ACM als voorzitter. Dit samenwerkingsverband bundelt toezicht en handhaving van de DSA op nationaal niveau. Daarnaast is er een multilateraal samenwerkingsprotocol tussen de ACM en elf andere toezichthouders dat afspraken regelt over taakverdeling, informatie-uitwisseling en onderlinge ondersteuning voor effectief en efficiënt DSA-toezicht.

Naar aanleiding van het rapport hebben de betrokken toezichthouders, het OM en de politie het initiatief genomen om te verkennen hoe hun samenwerking verder kan worden verdiept en hoe de beschikbare bevoegdheden optimaal kunnen worden benut voor een sluitende aanpak. Tegelijkertijd moet worden onderkend dat, ook bij maximale inzet, juridische of capacitaire beperkingen kunnen blijven bestaan. Het kabinet benadrukt in dit verband het grote belang van nauwere samenwerking, met inachtneming van ieders wettelijke bevoegdheden en verantwoordelijkheden. Indien de toezichthouders op basis van hun overleggen concrete verzoeken indienen bij het kabinet ter verbetering van hun handhaving, zal hier met prioriteit aandacht aan worden besteed.

Aanvullend is het belangrijk dat concrete en kwalitatief hoogwaardige informatie wordt aangeleverd aan de relevante toezichthouders, zodat zij hun toezichthoudende taken effectief kunnen uitvoeren. Hoewel zij hun focus en prioriteiten zelf zorgvuldig bepalen, kan kwalitatief hoogwaardige en gerichte informatie bijdragen aan het versterken van het toezicht. Zo kunnen concrete meldingen van overtredingen van de Digital Services Act (DSA) voor de ACM bijvoorbeeld aanleiding zijn om prioriteiten te heroverwegen. Voor de ACM ligt de nadruk onder meer op de bescherming van minderjarigen en de aanpak van hosterproblematiek. Deze thema's maken deel uit van de toezichtstrategie *Focus op digitale economie 2025*, waarbij online seksueel geweld een rol kan spelen.⁷ Daarnaast neemt de ACM via de Digitale Dienstenraad deel aan een gezamenlijke actie tegen adult content-platforms, die momenteel in een werkgroep verder wordt uitgewerkt.⁸

Voor de AP geldt dat ze de problematiek rondom online seksueel geweld uiterst serieus nemen en in overleg zijn en blijven met andere toezichthouders om te zien waar ze effectief kunnen optreden en, als blijkt dat ze dat niet kunnen, welk additioneel instrumentarium daarvoor noodzakelijk is.

Het kabinet benadrukt dat deze toezichthouders onafhankelijk zijn. Het is daarom primair aan hen om, binnen de wettelijke kaders en beschikbare middelen, hun prioriteiten te stellen en de wijze van taakuitvoering te bepalen. In het lopende contact is uiteraard ruimte om prioritering knelpunten in de handhaving te bespreken, hetgeen het kabinet ook doet.

Voor de politie en het OM geldt eenzelfde autonomie. Bij de regionale recherches zijn gespecialiseerde teams ingericht, die belast zijn met de opsporing van seksuele misdrijven binnen het werkgebied van de politie-eenheid. De zedenteams behandelen zowel online als offline zaken. De prioriteiten voor hun inzet worden bepaald door het bevoegd gezag binnen de politie-eenheid. Gezien het omvangrijke werkaanbod zijn scherpe keuzes onvermijdelijk. Om hierin te ondersteunen hebben de politie en het OM in 2024 de Handreiking Sturing Seksuele Misdrijven OM-Politie opgesteld. Deze handreiking biedt een sturingsmodel dat ondersteunt in de sturing op zedenzaken en landelijk door de politie en het OM wordt toegepast. Dit betekent dat alle meldingen van seksuele misdrijven die bij de zedenteams binnenkomen, worden voorzien van advies na triage. Daarbij wordt gekeken naar spoedhandelingen, slachtofferbehoeften en passende interventies.

⁷ <https://www.acm.nl/system/files/documents/acm-focus-op-digitale-economie-2025-ned.pdf>.

⁸ De Europese Raad voor digitale diensten (de «raad») bestaat uit de coördinatoren voor digitale diensten van de lidstaten en wordt voorgezeten door de Europese Commissie.

Bij een strafrechtelijk onderzoek worden impact, haalbaarheid en werkvoorraad meegewogen, waarbij zaken met grote impact of spoed voorrang krijgen. Daarnaast heeft de aanpak van online seksuele misdrijven binnen de zedenteams de volle aandacht van de politie. Inspanningen richten zich onder meer op het operationaliseren (verbeteren van het werkproces), de sturing en prioritering, het opdoen van ervaring en de stap naar datagedreven werken.

b. Feitenonderzoek Offlimits

De opstellers van het rapport stellen voor om afspraken te maken met Offlimits, een erkende «trusted flagger», zodat hun feitenonderzoek direct kan dienen als basis voor handhavende maatregelen.

Offlimits levert een hele waardevolle bijdrage aan het signaleren van misstanden, met name waar het slachtoffers betreft die anders buiten beeld blijven. Mede daarom is het Ministerie van Justitie en Veiligheid dan ook de hoofdfinancier van Offlimits. Omdat één melding van Offlimits vaak wijst op een bredere problematiek, geven politie en het OM dergelijke meldingen extra aandacht. Meldingen van Offlimits worden derhalve wel extra serieus opgepakt.

Desalniettemin richten toezichthoudende instanties, politie en OM hun handhavings- en opsporingsactiviteiten onafhankelijk in. Deze onafhankelijkheid is cruciaal voor een integere en effectieve rechtsgang en instanties in staat stelt feiten te verifiëren en zelfstandig te kwalificeren conform de geldende wettelijke kaders, waarbij eigen onderzoek noodzakelijk is voor objectiviteit en rechtsgeldigheid. Deze instanties kunnen daarom geen afspraken maken over het één-op-één overnemen van feitenmateriaal dat door Offlimits wordt aangedragen. Dit is ook niet een taak die past in de rol van een meldpunt. Opsporing kan en mag niet enkel gebruik maken van bewijsmateriaal dat alleen door een derde partij is vergaard zonder dat eigen onderzoek is gedaan.⁹ Uiteraard kunnen de feiten die Offlimits bloot legt wel een begin zijn voor een onderzoek. Voor het OM geldt het opportuniteitsbeginsel: het uitgangspunt dat een officier van justitie zelf beslist of een strafbaar feit wordt vervolgd. Dit biedt de ruimte om, ook wanneer er voldoende bewijs is, in zorgvuldig overwogen gevallen af te zien van vervolging. Het kan ook besluiten om af te zien van vervolging als dat in het algemeen belang of het belang van de rechtshandhaving beter is, bijvoorbeeld bij geringe ernst, onvoldoende maatschappelijke schade, of als andere maatregelen passender zijn.

c. Budgettaire en personele behoeften

De opstellers van het rapport adviseren om de budgettaire en personele behoeften van de betrokken toezichthouders en handhavende instanties te inventariseren om hun taken goed uit te kunnen voeren.

De financiële en personele behoeften van toezichthouders worden periodiek geïnventariseerd binnen hun reguliere financieringscyclus. De betrokken toezichthouders onderzoeken momenteel zelf de lacunes in hun aanpak. Tot dusver is daarbij niet gebleken dat een tekort aan financiële middelen de primaire oorzaak van de signaleerde problematiek rondom seksueel beeldmateriaal dat lastig offline te halen is.

Voor de opsporing geldt dat de formatie van de zedenteams van de politie de afgelopen jaren flink is uitgebreid. Ook is er geïnvesteerd in opleiding en expertise van politiemedewerkers vanwege de inwerkingtreding van de

⁹ Zie ook ECLI:NL:RBROT:2019:8535.

WSM op 1 juli 2024. Hoewel het is gelukt om extra capaciteit voor de zedenteams te werven, zien we dat het door de pensioenuitstroom (relatief veel ervaren politiemedewerkers stromen uit) en de krappe arbeidsmarkt momenteel een uitdaging is om de bezetting op peil te houden. In het halfjaarbericht politie wordt uw Kamer halfjaarlijks geïnformeerd over de situatie omtrent de zedenteams.

3. Uitbreiding ATKM

In de eerder genoemde motie van het lid Van Nispen c.s. is de regering verzocht te bezien of het mandaat van de ATKM kan worden uitgebreid, zodat in de toekomst ook verwijderbevelen kunnen worden afgegeven bij evident onrechtmatig materiaal van volwassenen. Hoewel dit verzoek sympathiek lijkt vanuit het oogpunt van bescherming tegen schadelijk online materiaal, is het op dit moment niet opportuun om het mandaat van de ATKM uit te breiden.

De ATKM is een relatief jonge toezichhouder. Het is belangrijk dat zij de tijd krijgt om verder te groeien om een gezaghebbende autoriteit te worden op het gebied van de bestuursrechtelijke aanpak van online kinderpornografisch materiaal en terroristische online inhoud. Gelet hierop moet de ATKM eerst de ruimte krijgen om zich te richten op haar kerntaken, waarbij het gaat om twee essentiële onderwerpen die direct raken aan de nationale veiligheid en fundamentele mensenrechten; twee van de meest verwerpelijke vormen van online illegale content.

Daarbij merk ik op dat het vaststellen van «evident onrechtmatig materiaal van volwassenen» complexe materie is, waarbij het een andere beoordeling betreft dan de kwalificatie die de ATKM nu uitvoert om haar wettelijke taken te vervullen. Bij het vaststellen van de onrechtmatigheid is de toestemming van de betrokkene een belangrijk gegeven. Daarbij kan het ook noodzakelijk zijn om in contact te staan met de desbetreffende volwassene die is afgebeeld. Gezien de doelstelling van de ATKM – het tegengaan van verspreiding van kinderpornografisch en terroristisch online materiaal – is dit nu nooit het geval. Daarnaast vereist de vaststelling van onrechtmatigheid vaak een belangenafweging waarbij context doorslaggevend is en open normen zoals «schadelijk» of «maatschappelijk onaanvaardbaar» een rol spelen.

Concluderend is het op dit moment niet opportuun en in deze fase niet verstandig om het mandaat van de ATKM uit te breiden naar evident onrechtmatig materiaal van volwassenen. De prioriteit ligt nu bij het zorgvuldig opbouwen van een effectieve en gezaghebbende toezichthouder binnen haar bestaande, wettelijk afgebakende opdracht.

Tot slot

Het vertrouwen in de digitale omgeving – een omgeving die in toeneemende mate cruciaal is voor het functioneren van onze samenleving – staat onder druk door het groeiende misbruik van deze infrastructuur voor uiteenlopende vormen van criminaliteit. Deze ontwikkeling is zorgwekkend en vraagt om een realistische benadering van de mogelijkheden én beperkingen op het gebied van handhaving en opsporing binnen de digitale context.

De verwachtingen van burgers van de overheid bij het aanpakken van maatschappelijke problemen zijn hoog en dat is begrijpelijk. Tegelijkertijd komen die verwachtingen vaak niet overeen met wat de overheid kan waarmaken en is het niet altijd de rol van de overheid: ook bedrijven dienen hun verantwoordelijkheid te nemen bij het tegengaan van online

seksueel geweld. Verder maakt de aard van het internet, waarin anonimiteit en grensoverschrijdend handelen de standaard zijn, het opsporen en vervolgen van daders bijzonder complex. Daarom is het ook van belang om in internationaal verband samen te werken. Technologische hulpmiddelen maken het mogelijk dat kwaadwillenden hun identiteit afschermen en zich vrijwel onvindbaar maken – wat effectieve handhaving vanuit nationale kaders ernstig belemmert. De digitale leefwereld beperkt zich daarnaast niet tot de landsgrenzen en verhoudt zich slecht tot nationale jurisdicties. In de praktijk is digitale criminaliteit vaak lastig op te sporen en vervolgen. Dit staat op gespannen voet met het rechtvaardigheidsgevoel en de normen die we in de fysieke wereld hanteren. Dit is een ongemakkelijke constatering maar alleen door deze realiteit onder ogen te zien, geven we vorm aan realistische en toekomstbestendige oplossingen die zowel de weerbaarheid van onze digitale infrastructuur vergroten als het publieke vertrouwen versterken.

Deze problematiek kan niet door de overheid alleen worden opgelost en daarom is het belangrijk is dat alle actoren in de samenleving samen blijven optrekken, zoals de organisaties die samen hebben gewerkt aan dit rapport, het bedrijfsleven en organisaties die internationaal samen werken. We staan samen aan de lat om de problematiek rondom online seksueel geweld te verbeteren, en zullen ons ook blijven inzetten om slachtoffers te ondersteunen.

De Minister van Justitie en Veiligheid,
F. van Oosten

SAMENVATTING VAN DE BEVOEGDHEDEN VAN DE VERSCHILLENDE TOEZICHTHOUDERS

In het licht van artikel 5:44 Algemene Wet Bestuursrecht (hierna: Awb) kan een toezichthouder die handelt op basis van de Awb, slechts acties ondernemen bij gedragingen die tevens een strafbaar feit zijn, nadat deze zijn voorgelegd bij de Officier van Justitie (hierna: OvJ) (lid 2) en de OvJ heeft aangegeven af te zien van vervolging (lid 3).

Een toezichthouder zal gemiddeld genomen geen prioriteit geven aan zaken die minder kansrijk zijn (datzelfde geldt voor het OM en politie). Voor effectief optreden is een heldere norm nodig die is overschreden, die snel en makkelijk kan worden aangetoond, gevolgd door handhavingsrecht dat ook toelaat dat er snel kan worden gehandhaafd en met de Awb is dat laatste niet (altijd) evident.

Autoriteit Consument & Markt

De ACM is de primaire toezichthouder op de DSA in Nederland en houdt onder andere toezicht op online platforms en webhostingdiensten. De DSA geeft de ACM geen directe bevoegdheid om verwijderbevelen op te leggen. Wel bevat de DSA verplichtingen op grond waarvan de ACM kan handhaven wanneer online platforms stelselmatig of structureel onvoldoende optreden tegen illegale inhoud, bijvoorbeeld naar aanleiding van meldingen van gebruikers en derden dan wel naar aanleiding van eigen onderzoek van de ACM. Tevens kan de ACM organisaties aanwijzen als «trusted flagger». Meldingen van dat soort organisaties moeten door platforms prioritair behandeld moeten worden. De ACM houdt ook toezicht op «trusted flaggers» om bijv. te voorkomen dat zij hun positie misbruiken en daarnaast kan de ACM de jaarlijkse rapportages van trusted flaggers eveneens gebruiken voor hun eigen toezicht.

Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) is belast met het toezicht op de naleving van de gegevensbeschermingswetgeving, zoals onder meer vastgelegd in de Algemene Verordening Gegevensbescherming (AVG). De bevoegdheden van de AP zien op de verwerking van persoonsgegevens. Dit betekent bijvoorbeeld dat als intieme beelden zonder toestemming worden verspreid, de AP kan ingrijpen als deze beelden persoonsgegevens zijn die onrechtmatig verwerkt zijn.

Slachtoffers van online seksueel geweld kunnen ook een klacht indienen bij de AP, waardoor zij een actieve rol vervullen in het signaleren van mogelijke schendingen van het gegevensbeschermingsrecht. Het is daarbij van belang te benadrukken dat de AVG niet van toepassing is op verwerkingen die uitsluitend binnen de huishoudelijke of persoonlijke sfeer plaatsvinden.¹⁰ Dit impliceert dat het maken van seksuele deepfakes voor uitsluitend «eigen gebruik» niet onder de AVG valt.

De AP kan een onderzoek instellen naar personen of organisaties die verantwoordelijk zijn voor het maken en verspreiden van dit soort materiaal. Dit kunnen online platforms zijn, maar ook hostingproviders die de content hosten. De AP heeft een ruim mandaat met uitgebreide bevoegdheden om te onderzoeken of partijen voldoen aan hun verplichtingen uit de AVG. Als uit het onderzoek blijkt dat er overtredingen zijn, kan de AP aanwijzingen geven. Ze kunnen bijvoorbeeld aanbieders van

¹⁰ Artikel 2 lid 2 sub c AVG

online diensten opdragen om het schadelijke maantoegekankelijk te maken (verwerkingsbeperking, waaronder een verwerkingsverbod).

Autoriteit online en Terroristisch Kinderpornografisch Materiaal

De ATKM kon reeds bevelen ter verwijdering of ontoegankelijk maken opleggen aan aanbieders van hostingdiensten bij aangetroffen online terroristisch materiaal en bestuursrechtelijk handhaven wanneer daar geen gehoor aan wordt gegeven. Op basis van de Europese Verordening inzake het tegengaan van de verspreiding van terroristische online-inhoud en bijbehorende nationale Uitvoeringswet. Vanaf 1 juli 2024 is de wet bestuursrechtelijke aanpak online kinderpornografisch materiaal in werking getreden waarmee de ATKM eveneens bevoegdheden heeft verkregen voor kinderpornografisch materiaal. Deze wet regelt onder meer de bevoegdheid voor de ATKM om aanbieders van hostingdiensten en aanbieders van communicatiediensten te verplichten online kinderpornografisch materiaal ontoegankelijk te maken of te verwijderen en bestuursrechtelijk te handhaven wanneer zij dat niet doen. De ATKM verwacht nog dit jaar handhavende maatregelen te kunnen treffen. De ATKM en Offlimits hebben recentelijk samenwerkingsafspraken gemaakt om informatie te kunnen uitwisselen over partijen die niet meewerken. Indien aanbieders van hostingdiensten niet meewerken kan de ATKM een last onder dwangsom of bestuurlijke boete opleggen oplopend tot 10% van de jaarlijkse omzet van de onderneming. Ook kan de ATKM ervoor kiezen om deze sanctiebesluiten openbaar te maken en zal dat in beginsel ook doen, gelet op de diffamerende werking die daarvan uitgaat.

Het Commissariaat voor de Media (CvdM)

Het Commissariaat is de toezichthouder die zich richt op het naleven van de Mediawet binnen Nederland, waarbij de focus ligt op mediakanalen zoals radio, televisie en bepaalde videoplatformdiensten en video-uploaders («influencers») die onder de Mediawet vallen. De taak van het Commissariaat bestaat onder meer uit het waarborgen van pluriformiteit, het beschermen van minderjarigen tegen schadelijke content en het handhaven van de voorschriften omtrent aanstootgevende en schadelijke uitzendingen.

Met betrekking tot online seksueel geweld heeft het Commissariaat een beperkte maar duidelijke rol. In gevallen waarin mediakanalen die onder zijn toezicht vallen uitzendingen of content verspreiden waarin sprake is van seksueel geweld, kan het Commissariaat toezien op de naleving van de geldende regels en indien nodig handhavend optreden. Dit kan resulteren in waarschuwingen, het opleggen van boetes, of andere bestuursrechtelijke maatregelen, zoals het opleggen van een last onder dwangsom. Het Commissariaat beschikt niet over de bevoegdheid om zelfstandig online content te verwijderen of offline te halen buiten zijn regulieringskader. De meerderheid van de online content wordt verspreid via platforms die niet direct onder de Mediawet of het toezicht van het Commissariaat vallen, zoals in het buitenland gevestigde social mediabedrijven, forums en andere websites.