Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

32 317 **JBZ-Raad**

34 843 **Seksuele intimidatie en geweld**

31 015 **Kindermishandeling**

Nr. 979

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID EN VAN DE MINISTER EN STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 25 november 2025

Tijdens het commissiedebat van 24 november jl. is met uw Kamer gesproken over de Verordening ter bestrijding van online seksueel kindermisbruik, ook wel de CSAM-Verordening genoemd. Met deze brief worden de toezeggingen aan uw Kamer zoals gedaan in het commissiedebat gestand gedaan.

Kabinetsstandpunt

In het Deense voorstel dat nu voorligt is verplichte detectie van online seksueel beeldmateriaal van kinderen helemaal uit het voorstel geschrapt en end-to-end-encryptie wordt niet onmogelijk gemaakt. In plaats daarvan wordt voorgesteld de mogelijkheden die bedrijven nu op grond van een tijdelijke derogatieregeling hebben om op eigen initiatief te detecteren, permanent te maken.

Zoals in onze brief van 18 november aangegeven, hebben wij zorgen over het permanent maken van vrijwillige detectie in de CSAM-Verordening.[1] Deze zorgen worden gedeeld binnen het kabinet. De genoemde zorgen zien op de privacy, de grondrechten en de digitale weerbaarheid. Bij het verlengen van de tijdelijke regeling is er telkens een nieuw weegmoment waarbij kan worden gekeken naar deze zorgen en een lidstaat zich desgewenst kan uitspreken. Bij het permanent maken is zo'n periodiek weegmoment er niet meer.

Advies AIVD

Voor de standpuntbepaling van het kabinet voor de CSAM-verordening heeft het kabinet advies ingewonnen bij de AIVD. De AIVD merkt in het advies expliciet op dat cybersecurity slechts één facet van de discussie

[1] Kamerstukken 32 317 en 34 843 en 31 015, nr. 977.

kst-32317-979
ISSN 0921 - 7371
's-Gravenhage 2025

betreft; er zijn ook overwegingen vanuit andere perspectieven (privacy, grondrechten, opsporing) die meegewogen dienen te worden.

Vanuit het perspectief van cybersecurity neemt het nieuwe voorstel de zorgen van de AIVD nog onvoldoende weg. De cybersecurityrisico's van het voorstel moeten worden bezien vanuit het perspectief van een hacker, die misbruik zal proberen te maken van de functionaliteit waarmee CSAM gedetecteerd moet worden. Ondanks dat er cybersecurityeisen worden gesteld aan de technologieën die de providers gebruiken om CSAM te detecteren, blijft er nog altijd sprake van detectietechnologieën die voor hun functionaliteit toegang nodig hebben tot persoonlijke data op mobiele *devices*. Bij een dergelijke functionaliteit komt een omvangrijke en complexe infrastructuur van beheersystemen kijken. Deze combinatie van een groot aantal toegangsrechten met een complexe beheerinfrastructuur, maakt het geheel een interessant potentieel doelwit voor kwaadwillende (statelijke) cyberactoren om potentieel toegang te krijgen tot grote hoeveelheden mobiele gegevens. Hoewel de veiligheid van dergelijke systeem uiteindelijk afhangt van de implementatie, brengt het ontwerp van deze maatregel in beginsel een groter aanvalsoppervlak met zich mee, dat bovendien moeilijk te beheersen is. Dit resulteert in een situatie waarvan de AIVD de risico's voor de digitale weerbaarheid nog altijd als zeer hoog inschat.

Visie Offlimits en Autoriteit online Kinderpornografisch Materiaal

Ook hebben wij uw verzoek de visie van Offlimits en de Autoriteit online Kinderpornografisch Materiaal (ATKM) te vernemen naar deze twee organisaties doorgeleid. Aangezien dit een stichting respectievelijk zelfstandig bestuursorgaan betreft, is met deze partijen besproken dat zij de Kamer zelfstandig kunnen informeren over hun inzichten met betrekking tot de CSAM-Verordening. Offlimits heeft gemeld dat de grootste zorg van Offlimits met de toevoeging van overweging 17a is weggenomen. Deze overweging zou verder versterkt moeten worden door de strekking van de overweging, die benadrukt dat niets in deze Verordening mag leiden tot of opgevat mag worden als een verplichting voor aanbieders om te detecteren, in een artikel van de Verordening op te nemen. Offlimits beschouwt vrijwillige detectie, naast de huidige praktijk, als een morele verplichting voor bedrijven om de veiligheid van hun omgeving te waarborgen. Offlimits pleit er voor dit uitsluitend te doen met bekend beeldmateriaal en niet met betrekking tot grooming (of in een later stadium eventueel audio). De ATKM heeft gemeld Europese wetgeving om de verspreiding van online kinderpornografisch materiaal tegen te gaan onontbeerlijk te achten. De ATKM acht het verder cruciaal voor een effectieve aanpak van de verspreiding van dit materiaal dat vrijwillige detectie mogelijk blijft en is voorstander van deze mogelijkheid.

Tot slot

Cybersecurity is slechts één facet van de discussie. Andere perspectieven zoals privacy, grondrechten en opsporing hebben ook meegewogen bij het bepalen van het huidige kabinetsstandpunt ten aanzien van vrijwillige detectie. Zoals aangegeven in de Kamerbrief van 18 november jl. is de positie die Nederland moet innemen ten aanzien van het huidige voorstel zowel een kwestie van complexe inhoudelijke afwegingen als van strategische belangen in het Europese krachtenveld. Daarbij is van belang dat enerzijds zo veel mogelijk wordt ingezet op het tegengaan van de verspreiding van dit vreselijke materiaal en dat anderzijds recht wordt gedaan aan grondrechtelijke zorgen, de digitale weerbaarheid van de lidstaten en de privacy van gebruikers van internetdiensten.

Het kabinet hoopt dat deze informatie bijdraagt aan een verdere verduidelijking van de kabinetsinzet om zich te onthouden inzake het voorliggende Deense voorstel en behulpzaam is bij het verdere besluitvormingsproces rond de CSAM-Verordening.

De Minister van Justitie en Veiligheid,
F. van Oosten

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
F. Rijkaart

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
E. van Marum