

**22 112 Nieuwe Commissievoorstellen en initiatieven
van de lidstaten van de Europese Unie**

Nr. 4388 Verslag van een schriftelijk overleg
Vastgesteld 19 juni 2026

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de staatssecretaris van Economische Zaken en Klimaat over de brief van 14 november 2025 over Fiche: DSA richtsnoeren betreffende minderjarigen online (Kamerstuk 22 112 nr. 4207).

De vragen en opmerkingen zijn op 19 december 2025 aan de staatssecretaris van Economische Zaken en Klimaat voorgelegd. Bij brief van 19 juni 2026 zijn de vragen beantwoord.

De voorzitter van de commissie,
Dekker

Adjunct-griffier van de commissie,
Muller

Vragen en opmerkingen vanuit de fracties en reactie van de bewindspersoon

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben met interesse kennisgenomen van het Fiche van de DSA-richtsnoeren betreffende minderjarigen online d.d. 18 december. Deze leden onderschrijven het belang van een veilige online omgeving, in het bijzonder voor minderjarigen, maar zien nog onduidelikheden wat betreft de effectiviteit en uitvoerbaarheid van de voorgestelde maatregelen.

Zij constateren dat de eisen in de DSA sterk overlappen met wetgeving uit de aangekondigde Digital Fairness Act (DFA) en de AI Act. De leden van de D66-fractie vragen hoe het kabinet in Europees verband concreet gaat voorkomen dat de verplichtingen uit de DSA, de toekomstige Digital Fairness Act en de AI Act elkaar deels overlappen of zelfs tegenspreken, zodat het ook duidelijk is welk kader leidend is voor handhavers en toezichthouders. Deze leden vragen hoe bij het harmoniseren van deze wetgeving wordt gewaarborgd dat de bescherming van burgers niet wordt afgezwakt ten behoeve van uniformiteit, specifiek in relatie tot de AI Act.

Antwoord:

Bij het verslag van de informele Telecomraad van 9 en 10 oktober 2025 dat op 12 november 2025 aan uw Kamer is verstuurd heeft het kabinet de non-papers bijgevoegd waarin ze haar ideeën voor zowel de Digital Fairness Act als de Digitale Omnibus uiteenzet. Zowel het voorkomen of oplossen van overlap en tegenstrijdige regels, als ook het waarborgen van de bestaande bescherming van burgers maken daarvan deel uit. Zo heeft het kabinet aangegeven dat de Digitale Omnibus geen afbreuk mag doen aan de doelstellingen van de wetgeving die ze voorstelt te wijzigen en moet de Omnibus zich richten op het stroomlijnen van rapportageverplichtingen en definities, het vergroten van duidelijkheid, consistentie en het makkelijker maken van

naleving. Daarnaast moet de governance van wetgeving worden versterkt zodat de wetgeving duidelijk en consistent wordt uitgelegd en geïnterpreteerd, ook over landsgrenzen heen en waar wetgeving overlapt. In het non-paper zijn diverse concrete voorstellen hiertoe gedaan. Een nadere appreciatie en invulling van de Omnibus AI en Omnibus Digitaal heeft het kabinet recent gegeven in het BNC-fiche over deze voorstellen.

Daarnaast is het belangrijk om het verschil in doelstelling en reikwijdte tussen de digitaaldienstenverordening (DSA) en de DFA voor ogen te houden. De DSA richt zich op een specifieke groep ondernemingen, namelijk online tussenhandeldiensten, waaronder platforms. De DFA zal zich, als onderdeel van het consumentenrecht, naar verwachting richten op handelaren. In het non-paper voor de DFA vraagt het kabinet primair om effectieve handhaving van bestaande regelgeving in de digitale economie, zoals de DSA en de AI-verordening. Het kabinet acht het dan ook het meest logisch dat handhaving op het terrein van verslavend ontwerp primair via de DSA verloopt, voor partijen die onder de reikwijdte van de DSA vallen, zoals grote social media platforms. De DFA kan daarnaast van belang zijn voor partijen waarop de regels uit de DSA niet van toepassing zijn, zoals de meeste gamebedrijven. In het non-paper over de DFA heeft het kabinet bovendien concrete voorstellen gedaan om de verhouding tussen onder meer de DSA (als het gaat om dark patterns) en de Audiovisuele Mediadiensten Richtlijn (als het gaat om influencer marketing) te verduidelijken en overlap te voorkomen.

Zij constateren dat de nieuwe richtsnoeren beoogd zijn om platforms 'te ondersteunen'. Denkt de staatssecretaris dat platforms daadwerkelijk actie gaan ondernemen op basis van deze richtsnoeren, gegeven het feit dat bijvoorbeeld verslavende elementen een fundamenteel onderdeel vormen van het verdienmodel van grote techbedrijven?

Antwoord:

Ja, dat is wel de verwachting. Hoewel de richtsnoeren niet wettelijk bindend zijn worden ze beschouwd als een

belangrijke referentie voor het voldoen aan de norm uit artikel 28, eerste lid, DSA. De Europese Commissie heeft laten weten dat ze de richtsnoeren ziet als maatstaf voor handhaving die zij en de digitaledienstencoördinatoren gaan gebruiken om naleving van de DSA te beoordelen. De verwachting is dan ook dat platforms de richtsnoeren zullen toepassen om aan de norm van artikel 28 DSA te voldoen.

De leden van de D66-fractie benadrukken dat privacy en de bescherming van persoonsgegevens kernwaarden zijn en hebben vragen over de uitwerking van de voorstellen voor leeftijdsverificatie en de inzet van de EU Digital Identity Wallet (eIDAS). Met name het feit dat de Europese Commissie voorstelt dat lidstaten zelf mogen bepalen in hoeverre de Wallet toezicht houdt op de informatie wat een afnemende partijen opvraagt. Deze leden vragen welke kwetsbaarheden dit creëert voor de privacy en gegevensbescherming van burgers.

Zij vragen dan ook of het kabinet de zorg deelt van de burgerrechtorganisatie epicenter. works en 14 burgerrechtenorganisaties¹ dat de huidige voorstellen het mogelijk maken voor informatie afnemende partijen om Europese beschermingsmechanismen te omzeilen en onnodig veel data van gebruikers op te vragen.

Antwoord:

Het kabinet volgt de ontwikkeling van verschillende leeftijdsverificatie-instrumenten nauwlettend, en zet zich in voor een handhaafbare Europese minimumleeftijd van 15 jaar voor sociale media, met privacyvriendelijke leeftijdsverificatie voor jongeren. Hierbij wordt goed gekeken naar de proportionaliteit en het voorkomen van privacy inbreuken en praktische problemen voor gebruikers en aanbieders.

¹ EDRI (5 februari 2025), 'Civil Society Demands: European Commission Must Close e-ID loopholes!', geraadpleegd via <https://edri.org/our-work/civil-society-demands-european-commission-must-close-e-id-loopholes/>.

De inzet van EDI-wallets is een van de mogelijkheden voor online leeftijdsverificatie waarnaar gekeken wordt. Daarbij is het van belang dat het gebruik van een EDI-wallet altijd vrijwillig is. Er zullen daarom ook alternatieven moeten zijn voor mensen die geen EDI-wallet willen gebruiken.

Voor wie wél een EDI-wallet wil gebruiken zijn in de Europese kaders voor wallets al veel maatregelen opgenomen om te zorgen dat gebruikers op een veilige en privacyvriendelijke manier kunnen beschikken over hun gegevens.

Organisaties die gegevens vragen moeten zich houden aan de geldende privacyregels, zoals de Algemene Verordening Gegevensbescherming. Om te voorkomen dat partijen niet om meer gegevens vragen dan noodzakelijk om de dienst te kunnen verlenen moeten zij vooraf openbaar maken welke gegevens zij zullen vragen. Deze informatie komt in een openbaar register waardoor iedereen – de burger zelf, maar ook toezichthouders en burgerrechtenorganisaties – kan zien welke gegevens zullen worden gevraagd voor een bepaalde dienst. Wanneer wordt opgemerkt dat de organisatie in de praktijk toch om andere gegevens vraagt, dan kan daartegen worden opgetreden.

Het kabinet zet aanvullend erop in dat er technische beschermingsmaatregelen worden getroffen die er zoveel mogelijk voor zorgen dat Nederlandse partijen niet om andere gegevens kunnen vragen dan zij hebben geregistreerd.

De leden van de D66-fractie willen weten hoe het kabinet zich inzet voor de garantie dat leeftijdsverificatie te allen tijde strikt privacy-vriendelijk wordt ingericht, waarbij minimale data-uitwisseling (zoals 'zero-knowledge proofs') de norm is, in plaats van het delen van volledige identiteitsgegevens.

Antwoord:

Om online platforms te ondersteunen om aan de verplichtingen uit de DSA om minderjarigen online te beschermen te voldoen, heeft de Europese Commissie afgelopen zomer een blauwdruk voor een online leeftijdsverificatie-app gepresenteerd. Dit EU-initiatief heeft tot doel een geharmoniseerde, privacybeschermende en gebruiksvriendelijke aanpak te bieden die in de gehele EU kan worden overgenomen door lidstaten en/of online diensten. Deze EU-blauwdruk app maakt gebruik van Zero Knowledge Proof. Zero Knowledge Proof is een cryptografische methode waarmee kan worden bewezen dat iemand boven een bepaalde leeftijd is, zonder dat de leeftijd of identiteit van een persoon hoeft te worden onthuld. Het idee is dat lidstaten of private partijen deze blauwprint gemakkelijk om kunnen zetten naar de nationale context. Dit kan door middel van een aparte (standalone) app voor leeftijdsverificatie óf door de leeftijdsverificatie-functie zoals technisch beschreven in de blauwprint te integreren in een andere nationale app (bijvoorbeeld een EUDI Wallet).

TNO is gevraagd om te kijken naar de organisatorische, juridische, technische en financiële haalbaarheid van nationale implementatie van een losse 'standalone' leeftijdsverificatie-app in Nederland. Hierbij kijkt TNO ook naar de impact op belangrijke waarden, zoals privacy, betrouwbaarheid, veiligheid en toegankelijkheid. Het rapport van TNO is eind januari ontvangen. In maart heeft een expertsessie plaats gevonden om de bevindingen te appreciëren en vervolgens te vertalen naar een beleidsvoorstel waarover uw Kamer zal worden geïnformeerd.

Deze leden vragen hoe de inzet op verplichte ouderlijke toestemming of strikte leeftijdsgrenzen zich verhoudt tot het recht van kinderen op toegang tot informatie en vragen of het kabinet het risico erkent dat kwetsbare jongeren, bijvoorbeeld LHBTIQ+-jongeren, hierdoor worden afgesneden van essentiële online hulpverlening. Zij vernemen graag welke specifieke waarborgen het kabinet wil inbouwen op Europees niveau om te voorkomen dat

beschermende maatregelen onbedoeld leiden tot digitale uitsluiting van deze kwetsbare groepen.

Antwoord:

Het kabinet realiseert zich dat er onder kinderen (extra) kwetsbare groepen zijn. Het is niet de bedoeling kinderen of groepen kinderen uit te sluiten van het gebruik van alle digitale diensten of het gebruik daarvan zomaar te beperken. Deze diensten bieden kinderen immers ook kansen. In het coalitieakkoord is het voornemen geuit voor een Europese minimumleeftijd van 15 jaar voor sociale media, zolang deze onvoldoende veilig zijn. Het coalitieakkoord richt zich met name op het gebruik van onveilige digitale diensten, zoals bepaalde categorieën van sociale media. Het kabinet vindt het hierbij van belang dat kinderen toegang houden tot informatie en online hulpverlening.

Het uitgangspunt van het kabinetsbeleid is daarom niet om alle digitale diensten te verbieden maar om de digitale wereld veiliger te maken voor kinderen. Tegelijkertijd ontwikkelt die wereld zich snel en doemen nieuwe risico's op. Het kabinet vindt het daarom ook verstandig ouders en verzorgers handvatten mee te geven om het gesprek met hun kind aan te gaan over het gebruik van digitale diensten. Dit is ook wat experts adviseren.

De leden van de D66-fractie delen de zorg van het kabinet dat risico's die voortkomen uit algoritmen nu onvoldoende worden vastgesteld of gecorrigeerd en dat handhaving onmogelijk is zonder toegang tot data, documentatie en testresultaten. Deze leden vragen hoe het kabinet erop inzet dat op Europees niveau toezichthouders zo snel mogelijk daadwerkelijk toegang krijgen tot de informatie die nodig is om aanbevelingssystemen te controleren en welke sancties of dwangmiddelen de toezichthouders ter beschikking staan als platforms weigeren deze data te delen. Zij vragen of de huidige bevoegdheden toereikend zijn om niet alleen reactief, maar ook proactief 'black box'-algoritmes te controleren op discriminatie of schadelijke sturing.

Antwoord:

De DSA geeft de Europese Commissie de bevoegdheid om, ter uitvoering van haar toezichtstaken, inlichtingen te vorderen van zeer grote online platforms en zeer grote online zoekmachines (artikel 67 van de DSA). Daarnaast beschikken zowel de Autoriteit Consument en Markt als digitaledienstencoördinator, en de Autoriteit Persoonsgegevens als bevoegde autoriteit, over de bevoegdheid om controles uit te voeren, informatie te vorderen, en werknemers van aanbieders van tussenhandeldiensten te vragen om uitleg te geven (artikel 51 van de DSA). Bovendien zijn aanbieders van zeer grote onlineplatforms of van zeer grote onlinezoekmachines verplicht om de Europese Commissie en de digitaledienstencoördinator van de lidstaat waar zij gevestigd zijn toegang te geven tot gegevens die nodig zijn om naleving te monitoren en te beoordelen. Dit omvat ook de verplichting om toelichting te geven op het ontwerp, de logica, de werking en het testen van algoritmische systemen, waaronder aanbevelingssystemen (artikel 40, eerste t/m derde lid van de DSA). Indien platforms weigeren om de gevraagde data te delen, kunnen de Europese Commissie en de digitaledienstencoördinator voorlopige maatregelen, dwangsommen of geldboeten opleggen.

Ik heb geen signalen dat deze bestaande bevoegdheden ontoereikend zijn voor de toezichthouders.

De leden van de D66-fractie constateren dat er een structureel gat blijft bestaan tussen content die evident illegaal is en content die weliswaar legaal, maar zeer schadelijk is (de zogenaamde 'grijze zone'), waarbij platforms zich vaak verschuilen achter het argument dat de inhoud formeel niet verboden is. Deze leden vragen of het kabinet bereid is om in EU-verband te pleiten voor aanvullende normen of gedragscodes die specifiek gericht zijn op deze 'borderline-content' en welke mogelijkheden het kabinet ziet om platforms aan te spreken op hun verantwoordelijkheid voor moderatie. Zij vragen daarnaast hoe het kabinet ervoor zorgt dat platforms kindvriendelijke meldmechanismen om schadelijke content te rapporteren

niet alleen op papier beloven, maar ook daadwerkelijk en laagdrempelig invoeren.

Antwoord:

Ik deel de zorg dat zowel illegale als niet-illegale content ernstige gevolgen kunnen hebben en aandacht behoeven. Tegelijkertijd is het belangrijk om uiterst voorzichtig te zijn met niet-illegale content, die in beginsel wordt beschermd door het grondrecht op vrijheid van meningsuiting. Dat grondrecht is ook verankerd in het Handvest van de EU en internationale verdragen waaraan Nederland zich heeft gebonden. Bovendien is het feit dat dergelijke content niet als illegaal is aangemerkt door de wetgever een teken dat er in het parlement geen overeenstemming is over de toelaatbaarheid van dergelijke content. Terughoudendheid is daarom op zijn plaats.

Dit is ook terug te zien in de regels in de DSA voor niet-illegale, doch schadelijke content. Zo zijn zeer grote online platforms en zoekmachines verplicht om tenminste jaarlijks te onderzoeken of hun diensten vatbaar zijn voor zogenaamde systeemrisico's, zoals gebruik van hun diensten voor het ondermijnen van verkiezingsprocessen of ernstige negatieve gevolgen voor het lichamelijk en geestelijke welzijn van personen. Indien dergelijke systeemrisico's bestaan dan moeten zij daar maatregelen tegen nemen. De DSA bepaalt nadrukkelijk niet dat dit moet leiden tot het verwijderen van content om te voorkomen dat het recht op vrijheid van meningsuiting onnodig wordt ingeperkt. Andere maatregelen zijn meer passend, zoals het aanpassen van aanbevelingsalgoritmes om te voorkomen dat dit soort content erdoor wordt versterkt en verder verspreid.

In dit kader is ook relevant dat de DSA regels bevat voor het opstellen van gedragscodes ten behoeve van de naleving. Gedragscodes kunnen partijen helpen verbintenissen aan te nemen die bijdragen tot het minimaliseren van risico's onder de DSA. Zo is de praktijkcode inzake desinformatie in februari 2025 in de DSA geïntegreerd als gedragscode in de zin van artikel 45 DSA. De code heeft tot doel de risico's voortvloeiend uit desinformatie te bestrijden, maar ook de

vrijheid van meningsuiting te beschermen. Ook de Gedragscode voor de bestrijding van illegale haatzaaiende uitlatingen online is via deze weg in de DSA geïntegreerd.

Ondertussen zit het kabinet ook niet stil. Zo ziet het kabinet bijvoorbeeld dat extremistische content kan bijdragen aan gewelddadig extremisme en terrorisme. Daarom heeft de minister van Justitie en Veiligheid afgelopen najaar in samenwerking met Duitsland en Frankrijk een non-paper aan de Europese Commissie gestuurd met voorstellen hieromtrent. Uw Kamer is daarover geïnformeerd bij brief van 17 december 2025.² Teneinde de vrijheid van meningsuiting te beschermen en eventuele wet- of regelgeving over dit thema uitvoerbaar te maken voor bedrijven en toezichthouders zal Nederland eraan werken om tot een werkbare definitie van 'extremistische content' te komen, zoals door de Kamer ook is verzocht in de motie van het lid Michon-Derkzen.³

Zij vragen daarnaast hoe het kabinet ervoor zorgt dat platforms kindvriendelijke meldmechanismen om schadelijke content te rapporteren niet alleen op papier beloven, maar ook daadwerkelijk en laagdrempelig invoeren.

Antwoord:

De DSA verplicht platforms die zich richten op minderjarigen of overwegend door hen worden gebruikt om de gebruiksvoorwaarden uit te leggen op een manier die minderjarigen kunnen begrijpen (artikel 14, derde lid DSA). Dit omvat informatie over beleidsmaatregelen, procedures, maatregelen en instrumenten die worden ingezet voor inhoudsmoderatie en procedurevoorschriften. Het is nu aan de onafhankelijk toezichthouders op de DSA om hier toezicht op te houden en zo nodig te handhaven.

De leden van de D66-fractie maken zich tot slot zorgen over de uitvoerbaarheid, en vragen hoe het kabinet in EU-verband gaat aandringen op een effectieve en uniforme handhaving

² Kamerstukken II 2025-26, 29754, nr. 773.

³ Kamerstukken II 2025-26, 29754, nr. 758.

van de DSA door de Commissie om versnippering van toezicht te voorkomen.

Antwoord:

Juist omwille van een effectieve en uniforme handhaving van de DSA is een deel van het toezicht exclusief belegd bij de Europese Commissie, namelijk het toezicht op en de handhaving van de verplichtingen die gelden voor zeer grote online platforms- en zoekmachines. Er is geen reden om te veronderstellen dat de Commissie dit niet op effectieve en uniforme wijze doet. Het kabinet heeft op diverse momenten laten blijken dat zij de Europese Commissie steunt in het handhaven van de DSA.

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met interesse kennisgenomen van het Fiche: DSA richtsnoeren betreffende minderjarigen online. Deze leden benadrukken het belang van het nemen van maatregelen om de privacy, veiligheid en beveiliging van minderjarigen online te waarborgen en steunen de Nederlandse positie ten aanzien van het voorstel. Zij stellen nog enige vragen.

De leden van de VVD-fractie lezen dat het kabinet positief staat tegenover de maatregelen in de richtsnoeren die zien op het verbeteren van moderatie-, rapportage- en klachtafhandelingsprocessen zodat zowel minderjarigen als ouders over voldoende duidelijke en laagdrempelige hulpmiddelen beschikken om illegale of schadelijke inhoud te melden en klachten te kunnen neerleggen over moderatiebeslissingen van platforms. Deze leden vragen welke rapportageverplichtingen de platformen hebben over het aantal en het soort gemelde schadelijke berichten op hun platformen. Hebben platformen daarbij bovendien de plicht om van berichten met illegale inhoud op hun platformen direct aangifte te doen bij de politie? En is er over het algemeen voldoende uitwisseling van gegevens tussen

sociale platformen en de opsporings- en inlichtingendiensten?

Antwoord:

Op grond van de DSA zijn zeer grote online platforms ('very large online platforms', of VLOP's) verplicht tot het publiceren van een halfjaarlijks transparantieverslag. Hierin staat het aantal en het type contentmoderatieberispingen en moeten zij onder meer inzage geven in het aantal ontvangen bevelen van autoriteiten, meldingen van gebruikers, verwijderde accounts, samenwerking met trusted flaggers en uitkomsten van interne klachtenprocedures (artikelen 15, 24 en 42). Hierbij wordt wel inzicht gegeven in het aantal en soort contentmoderatieberispingen, maar zijn deze doorgaans niet te herleiden naar de specifieke content waar die beslissing over genomen is.

Daarnaast hebben VLOP's onder de DSA de verplichting tot een jaarlijkse risicobeoordelingsrapportage. Hierin moeten ze systeemrisico's identificeren. Waar de verspreiding van illegale inhoud en de bescherming van minderjarigen een specifiek onderdeel van zijn.

In het kader van de DSA moeten platforms dus gedetailleerd rapporteren over de aard en omvang van moderatie, maar er is geen algemene verplichting om aangifte te doen bij politie wanneer er illegale content wordt geïdentificeerd. De DSA stelt alleen een specifieke meldingsplicht voor ernstige feiten die levensbedreigend kunnen zijn, denk aan terroristische misdrijven, seksueel misbruik van kinderen en mensenhandel (Artikel 18 DSA).

Los van de DSA bestaat in het strafrecht de mogelijkheid voor de Officier van Justitie om, in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, van het Wetboek van Strafvordering (Sv), met een machtiging van de rechter-commissaris, een aanbieder van een communicatiedienst te bevelen om gegevens ontoegankelijk te maken als het noodzakelijk is ter beëindiging van het

strafbare feit of ter voorkoming van nieuwe strafbare feiten (artikel 125p Sv).

Zij noteren dat de onlinewereld risico's met zich meebrengt voor kinderen en jongeren, zoals 'blootgesteld worden aan online content die kan leiden tot radicalisering dan wel extremisme'. De richtsnoeren van de Commissie hebben het over 'geweld, radicalisering, gewelddadig extremisme en terrorisme'. Daarnaast wil de Commissie ook discriminerende en radicaliserende inhoud tegengaan in artikel 65 (h) van de richtsnoeren. Hoe zorgt het kabinet ervoor dat maatregelen die online gericht zijn op het tegengaan van radicalisering en extremisme niet onnodig ingrijpen in de vrijheid van meningsuiting en legitieme politieke discussie?

Antwoord:

Het tegengaan van online radicalisering, extremisme en terrorisme omvat een breed palet aan maatregelen. Een deel daarvan richt zich op illegale online inhoud, zoals terroristisch materiaal. Dergelijke inhoud is verboden en kan op basis van een verwijderbevel van de Autoriteit online Kinderpornografisch en Terroristisch Materiaal (ATKM) worden verwijderd of ontoegankelijk worden gemaakt. Extremistische content is niet per definitie illegaal. Voor dit type inhoud bestaan daarom geen overeenkomstige bevoegdheden, (mede) in verband met fundamentele rechten, zoals de vrijheid van meningsuiting. Tegelijkertijd kan extremistische content bijdragen aan radicalisering, gewelddadig extremisme en terrorisme. Gelet hierop wordt het (meer) inzetten op verwijderverzoeken onderzocht, in het kader van de evaluatie van de verordening Uitvoeringswet Terroristische Online-Inhoud. In het coalitieakkoord is opgenomen dat onderzoek wordt gedaan naar het verbieden en verwijderen van content die mistrijven toont, behalve in journalistieke verslaglegging. Hiervan kan sprake zijn bij gewelddadig extremistische content. Het beschermen van fundamentele rechten, zoals de vrijheid van meningsuiting,

wordt in acht genomen bij de inspanningen om extremisme en terrorisme te bestrijden. Hiermee wordt een ongerechtvaardigde inbreuk op deze rechten in principe tegengegaan. Ter bescherming van de vrijheid van meningsuiting zal Nederland zich bijvoorbeeld inzetten voor het komen tot een werkbare definitie van 'extremistische content', conform het verzoek van uw Kamer, zoals verwoord in de motie van het lid Michon-Derkzen. Een dergelijke definitie kan bijdragen aan een meer gedeeld beeld van dit type content en de risico's die het met zich meebrengt. Om de online dreiging tegen te gaan, heeft de minister van Justitie en Veiligheid afgelopen najaar, in samenwerking met Duitsland en Frankrijk, ook een non-paper aan de Europese Commissie gestuurd met inhoudelijke voorstellen. Deze voorstellen zijn overigens niet specifiek gericht op het verwijderen van extremistische content. In plaats daarvan hebben deze voorstellen betrekking op onder andere het delen van signalen van online radicalisering en het tegengaan van zogeheten platformmigratie. Uw Kamer is hierover geïnformeerd bij brief van 17 december 2025. Zoals bepleit in dit non-paper verwijst de nieuwe EU-agenda om terrorisme te voorkomen en te bestrijden expliciet naar de mogelijkheid om een gedragscode voor platformen op te zetten.

Ook lezen de leden van de VVD-fractie in artikel 57 (b) (v) en 58 (f) van C/2025/5519 dat onlineplatforms voor alle minderjarigen moeten zorgen dat in de accountinstellingen de toegang tot foto's en de camerafunctie is uitgeschakeld of dat tijdens een actieve sessie wordt aangegeven dat deze functies zijn ingeschakeld. Acht het kabinet een technisch verbod op foto- en cameratoegang in de standaardinstellingen en het tonen van de status tijdens een actieve sessie in de praktijk haalbaar voor socialmediaplatforms? Heeft de Commissie reeds consultaties met platforms of technische leveranciers gehouden over de technische en operationele uitvoerbaarheid van dergelijke instellingen?

Antwoord:

De Europese Commissie heeft bij de totstandkoming van deze richtsnoeren verschillende stappen gezet om input op te halen over de uitvoerbaarheid en proportionaliteit van maatregelen ter bescherming van minderjarigen. In 2025 heeft de Commissie een openbare consultatie georganiseerd over de concept-richtsnoeren, waarop onder meer onlineplatforms en andere betrokken partijen hebben gereageerd. Het kabinet beschikt niet over gedetailleerde informatie over de inhoud van bilaterale gesprekken die de Commissie mogelijk met individuele platforms of technische leveranciers heeft gevoerd, noch over de vraag of daarin specifiek is gesproken over deze concrete instellingen. Dergelijke gesprekken en de inhoud daarvan worden door de Commissie niet structureel met lidstaten gedeeld.

De Europese Commissie heeft daarnaast nadere informatie gepubliceerd over het consultatieproces. Zo zijn er samenvattende rapporten verschenen van zowel de openbare consultatie als de call for evidence, waarin reacties van onder meer platforms en andere stakeholders zijn verwerkt. Hoewel geen volledige lijst van individuele bijdragen is gepubliceerd, geven deze rapporten inzicht in de breedte van de opgehaalde input.⁴⁵

Daarnaast zijn alle ingediende reacties openbaar toegankelijk gemaakt via het “Have Your Say”-portaal van de Commissie.⁶ Ook heeft de Commissie gedurende het proces workshops georganiseerd met een brede groep stakeholders, waaronder zeer grote onlineplatforms (VLOPs) en kleinere

⁴ <https://digital-strategy.ec.europa.eu/en/library/digital-services-act-summary-report-targeted-public-consultation-protection-minors-guidelines>

⁵ <https://digital-strategy.ec.europa.eu/en/library/digital-services-act-summary-report-call-evidence-protection-minors-guidelines>

⁶ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines_en

platforms. Verdere toelichting op het proces is beschikbaar via de publicatiepagina van de richtsnoeren.⁷

Deze leden lezen verder dat de effectiviteit van de richtsnoeren onder andere valt of staat met de bereidheid van de platformen om de maatregelen daadwerkelijk uit te voeren. Zij vragen of het kabinet mogelijkheden ziet om deze bereidheid richting de platformen te stimuleren.

Antwoord:

De Europese Commissie heeft laten weten dat ze de richtsnoeren ziet als maatstaf voor handhaving die zij en de digitaledienstencoördinatoren gaan gebruiken om naleving van de DSA te beoordelen. Het kabinet zal deze toepassing van de richtsnoeren met aandacht volgen.

De leden van de VVD-fractie lezen tot slot in het Fiche dat de inzet van leeftijdsverificatie eerder te rechtvaardigen is naarmate de risico's in specifieke situaties voor jongeren groter zijn en er tevens wettelijke leeftijdsgrenzen zijn. Hoe kijkt het kabinet naar het stellen van zo'n wettelijke leeftijdsgrens voor sociale media?

Antwoord:

Op dit moment geldt er geen wettelijke minimumleeftijd voor sociale media. In het Coalitieakkoord is opgenomen dat er een handhaafbare Europese minimumleeftijd van 15 jaar voor sociale media moet komen met privacy vriendelijke leeftijdsverificatie, zolang sociale media onvoldoende veilig zijn. Momenteel wordt onderzocht langs welke juridische weg dit is te bereiken.

⁷ <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>

Deze leden constateren dat in resolutie 2025/2060(INI) van het Europees Parlement, d.d. 26 november 2025, wordt gepleit voor een geharmoniseerd leeftijdslimiet van 16 jaar voor toegang tot social media. De brief van de bewindspersoon is opgesteld voordat deze resolutie werd aangenomen, waardoor de positie van het Europees Parlement destijds onbekend was. Gezien dit standpunt van het Europees Parlement vragen zij of het kabinet of het van oordeel is dat een geharmoniseerd leeftijdslimiet van 16 jaar de online veiligheid van minderjarigen beter waarborgt, of dat het de voorkeur geeft aan de risico-gebaseerde aanpak zoals geformuleerd in de richtsnoeren van de Commissie.

Antwoord:

Inmiddels is er een Coalitieakkoord waarin is opgenomen dat er een handhaafbare Europese minimumleeftijd van 15 jaar voor sociale media moet komen met privacyvriendelijke leeftijdsverificatie, zolang sociale media onvoldoende veilig zijn. Momenteel wordt onderzocht langs welke juridische weg dit is te bereiken.

Voorts vragen de leden van de VVD-fractie wanneer de resultaten van het onderzoek van TNO over de juridische, financiële en technische haalbaarheid van de implementatie van een Nederlandse leeftijdsverificatie-app met de Kamer kan worden gedeeld?

Antwoord:

Het rapport van TNO is eind januari jl. ontvangen. In maart heeft een expertsessie plaatsgevonden om de bevindingen te appreciëren en vervolgens te vertalen naar een beleidsvoorstel waarover uw Kamer zal worden geïnformeerd. Naar verwachting zal dit in het voorjaar plaatsvinden.

Vragen en opmerkingen van de leden van de GL-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de richtsnoeren minderjarigen online en de reactie van het kabinet. Deze leden steunen een strenge aanpak van grote techbedrijven die willens en wetens de online wereld een verslavende en giftige plek maken. Echter hebben zij zorgen, vragen en opmerkingen bij de Europese richtsnoeren. Deze zullen de leden van de GroenLinks-PvdA-fractie nader toelichten.

Deze leden zijn van mening dat jongeren online altijd veilig en vrij moeten zijn. Zij roepen op om vergaande maatregelen te nemen die gebruikers beschermen tegen de manipulatieve trucs van grote techbedrijven én het ongepaste gedrag van kwaadwillenden. Zo moet gevaarlijke content duidelijk geclassificeerd worden zodat gebruikers dit kunnen weren en afschermen, moeten AI-chatbots in populaire apps geweerd worden zodat jongeren hier niet door worden misleid, is er een preventieve aanpak nodig voor 'grooming' waar veelal jongeren slachtoffer van worden, en moeten de risico's op verslaving en te hoge schermtijd worden weggenomen. Wat is de rol van EU-regulering hierin volgens de staatssecretaris, en hoeveel kan op nationaal niveau worden ondernomen op het gebied van mediawijsheid en preventie? Deelt de staatssecretaris de mening dat er nog bij lange na niet genoeg gebeurt om de giftige elementen van sociale media te reguleren?

Antwoord:

Onder artikel 34 en 35 van de DSA hebben VLOPs de verplichting om systeemrisico's te analyseren en mitigeren. Onder deze systeemrisico's vallen ook negatieve effecten op het welzijn van kinderen. Hierbij worden VLOPs geacht om 'redelijke, proportionele en effectieve' maatregelen te nemen om deze risico's te mitigeren. In de richtsnoeren worden verschillende aanbevelingen gedaan op welke manier hier betekenis aan kan worden gegeven. Hierbij kijken we ook

naar de evaluatie van de DSA in 2027 hoe de rol van de DSA hierin precies is geweest.

Op nationaal niveau wordt al veel ondernomen op het gebied van mediawijsheid en preventie, waaronder de publiekscampagne 'Blijf in Beeld' en ondersteuning van Netwerk Mediawijsheid vanuit OCW. Het kabinet ziet in toenemende mate risico's bij het gebruik van sociale media door kinderen. Daarom zet zij nu al in op een minimumleeftijd voor sociale media. Tegelijkertijd is het kabinet geïnteresseerd in de evaluatie van de DSA waarbij wordt gekeken hoe de effectiviteit van deze wetgeving kan worden ondersteund. En naar mogelijkheden binnen de DFA die de zelfbeschikking van gebruikers bevorderen.

De leden van de GroenLinks-PvdA-fractie zijn van mening dat grote techbedrijven veel steviger aangepakt moeten worden. Het is onacceptabel dat de macht en invloed over het maatschappelijke debat en de informatievoorziening ligt bij een handjevol techgiganten die hun geld verdienen door ophef te belonen, gerichte advertenties op te dringen en gebruikersdata te stelen en verkopen. Door de noodzakelijke aanpassingen van sociale media alleen voor minderjarigen in te richten, worden de techbedrijven maar in een klein deel van hun inkomsten geraakt. Deelt de staatssecretaris de opvatting van deze leden dat grote techbedrijven juist baat hebben bij het maken van een scheiding tussen minderjarige en meerderjarige gebruikers, omdat het hen ontslaat van de plicht om ook voor volwassenen hun platforms gezonder te maken? Hoe beoordeelt de staatssecretaris in dit licht de positieve houding van zowel Google als Meta richting het voorstel om dit onderscheid tussen gebruikers te maken?

Antwoord:

De onlinewereld moet voor een ieder die daartoe toegang heeft, veilig zijn. Extra aandacht is nodig waar het gaat om kwetsbare groepen zoals kinderen. Daarom ook zijn in bijvoorbeeld de DSA en de AVG speciaal voor kinderen bepalingen opgenomen in het kader van hun online-bescherming. Waar het zeer grote platforms betreft houdt de

Europese Commissie toezicht, zoals op TikTok waarover de Commissie (voorlopig) oordeelde dat TikTok in strijd met de DSA handelde vanwege het verslavend ontwerp van de dienst. De meeste bepalingen uit genoemde wetgeving gelden overigens ook voor volwassenen. Het maken van onderscheid tussen minder- en meerderjarigen ontslaat normadressanten zoals Google en Meta niet van hun verplichtingen.

Volgens de leden van de GroenLinks-PvdA-fractie roept het maken van onderscheid tussen jong en oud de fundamentele kwestie op over de inzet van leeftijdsverificatie. Hierover hebben deze leden zorgen en vragen.

Zij stellen dat leeftijdsborging en het verplichten van verificatie raakt aan de basis van internetvrijheid. De anonimiteit die noodzakelijk is om gebruikers te beschermen, hun cyberveiligheid te garanderen, en de vrije toegang tot informatie te verzekeren komt mogelijk in het geding. De leden van de GroenLinks-PvdA-fractie zullen hun zorgen één-voor-één toelichten en vragen om een reactie. De eerste zorg van deze leden is het verschuiven van verantwoordelijkheid en macht naar het bedrijfsleven. Enkele methoden voor leeftijdsborging, zoals ID-verificatie, foto-ID-matching en een leeftijdsschatting maken, verplichten dat grote techbedrijven gevoelige persoonsgegevens opvragen en verwerken. Hiermee komt de privacy en cyberveiligheid van gebruikers in het geding. Zij verwijzen bijvoorbeeld naar de hack op communicatieplatform Discord, waar ID-gegevens buitgemaakt zijn.⁸ Hoe kijkt de staatssecretaris naar vormen van leeftijdsverificatie die de verantwoordelijkheid voor verwerking bij bedrijven neerleggen? Deelt hij de zorgen van deze leden over de cyberveiligheid, en druist dit niet in tegen het principe van dataminimalisatie? Welke bijdrage zou het

⁸ Tweakers (4 oktober 2025), 'Discord meldt diefstal ID-bewijzen bij handmatige leeftijdsverificatie', <https://tweakers.net/nieuws/239968/discord-meldt-diefstal-id-bewijzen-bij-handmatige-leeftijdsverificatie.html>.

ontwikkelen van een Nederlandse verificatiemethode, met privacybescherming als uitgangspunt, kunnen bijdragen aan het bevorderen van de keuzevrijheid voor internetgebruikers en de onafhankelijkheid van de betrokken techbedrijven? Hoe duur is het om zo'n methode te ontwikkelen?

Antwoord:

Het kabinet deelt de zorg van deze Kamerleden. De Europese Commissie heeft een blauwdruk voor een online leeftijdsverificatie-app gepresenteerd. Dit EU-initiatief heeft tot doel een geharmoniseerde, privacybeschermende en gebruiksvriendelijke aanpak te bieden die in de gehele EU kan worden overgenomen door lidstaten en/of online diensten. Deze EU-blauwdruk app maakt gebruik van Zero Knowledge Proof. Zero Knowledge Proof is een cryptografische methode waarmee kan worden bewezen dat iemand boven een bepaalde leeftijd is, zonder dat de leeftijd of identiteit van een persoon hoeft te worden onthuld. Het idee is dat lidstaten of private partijen deze blauwprint gemakkelijk om kunnen zetten naar de nationale context. Dit kan door middel van een aparte (standalone) app voor leeftijdsverificatie óf door de leeftijdsverificatie-functie zoals technisch beschreven in de blauwprint te integreren in een andere nationale app (bijvoorbeeld een EUDI Wallet).

Aan TNO is gevraagd om te kijken naar de organisatorische, juridische, technische en financiële haalbaarheid van nationale implementatie van een losse 'standalone' leeftijdsverificatie-app in Nederland. De resultaten van dit onderzoek zijn eind januari ontvangen. In maart heeft een expertsessie plaatsgevonden om de bevindingen te appreciëren en vervolgens te vertalen naar een beleidsvoorstel waarover uw Kamer zal worden geïnformeerd.

Tevens zijn zij benieuwd naar de zienswijze van de staatssecretaris op de European Wallet, waar middels

'tokens' beperkte verificatie kan plaatsvinden in uitzonderlijke situaties. Doet Nederland mee aan pilots met de Wallet? Is de staatssecretaris bereid om deze Wallet te toetsen op het gebied van privacybescherming?

Antwoord:

Zoals aangegeven in de reactie op de vragen van de leden van D66, houdt het kabinet zicht op de ontwikkelingen rondom leeftijdsverificatie-instrumenten en op het gebruik van EDI-wallets. Burgers die een EDI-wallet willen gebruiken, zouden daarmee mogelijk een bewijs kunnen delen met dienstverleners dat zij de benodigde leeftijd hebben bereikt, zonder hun specifieke leeftijd of andere persoonsgegevens te hoeven delen. Daarbij is het van belang dat het gebruik van een EDI-wallet altijd vrijwillig is. Er zullen daarom ook alternatieven moeten zijn voor mensen die geen EDI-wallet willen gebruiken. Er wordt gewerkt aan een stelsel voor EDI-wallets, inclusief een publieke wallet, waarbij privacy hoog in het vaandel staat.

De tweede zorg van de leden van de GroenLinks-PvdA-fractie is dat verplichte verificatie mogelijk een beperking van internetvrijheid kan betekenen doordat het online anonimiteit onmogelijk maakt. Deze leden noemen het voorbeeld van LHBTI-jongeren die opgroeien in een omgeving waarin zij niet worden geaccepteerd. Deze jongeren willen lotgenoten ontmoeten en hebben recht op vrije toegang tot informatie die helpt bij hun ontwikkeling. Het verplichten van verificatie voor deze jongeren kan een serieuze drempel zijn om deel uit te maken van online gemeenschappen die hen juist helpen, omdat hun persoonsgegevens technisch gezien te achterhalen zijn. Hoe reageert de staatssecretaris op deze zorgen? Hoe garandeert hij de communicatieplatforms en websites waar minderheidsgroepen elkaar kunnen ontmoeten niet achter slot en grendel gaan voor jongeren die dit keihard nodig hebben?

Antwoord:

Ook deze zorg deelt het kabinet. Het kabinet ziet dat sociale media kansen voor jongeren biedt, maar ziet ook dat de huidige online omgeving onvoldoende veilig is voor kinderen en jongeren vanwege verslavende en polariserende algoritmes en schadelijke content. Een belangrijk uitgangspunt van het kabinet is daarom dat digitale diensten veilig worden voor kinderen en jongeren, omdat zij het recht hebben om veilig gebruik te maken van digitale diensten. Daarom heeft het kabinet de afgelopen jaren ingezet op het tegengaan van online onveiligheid via onder andere de DSA. Als digitale diensten niet veilig zijn voor kinderen en jongeren, kijkt het kabinet of het proportioneel is om een leeftijdsgrens in te stellen en online leeftijdsverificatie in te zetten om hen te beschermen. Hierbij is het essentieel dat jongeren altijd toegang moeten kunnen hebben tot informatie die hen helpt bij hun ontwikkeling.

De derde zorg van deze leden is het risico op een glijdende schaal. Zodra bepaalde online diensten leeftijdsverificatie gaan verplichten, bestaat de kans dat 'mission creep' optreedt en dat verificatie breder wordt getrokken dan alleen de diensten die onder de Digital Services Act worden gereguleerd. Dit betekent dat nog meer delen van het internet mogelijk begrensd worden en er minder vrije toegang tot informatie en platforms is voor gebruikers. In het ergste geval kunnen lidstaten, zodra er acceptabele methoden voor leeftijdsborging zijn voorgesteld, ook politieke content of LHBTI-onderwerpen als 'ongepast voor kinderen' worden aangemerkt. Is het risico op mission creep volgens de staatssecretaris gegrond? Welke afspraken zijn er in Europees verband gemaakt om te voorkomen dat leeftijdsverificatie wordt ingezet door lidstaten om niet-illegale of politieke content te begrenzen of af te schermen?

Antwoord:

Bij het inrichten van een leeftijdsverificatiesysteem moet aandacht worden besteed aan verschillende aspecten. Naast

onder meer privacy, moet ook aandacht worden besteed aan deze zorg.

De online publieke ruimte moet veilig, toegankelijk en inclusief zijn. Discriminatie en uitsluiting is niet toegestaan en gelijke gevallen dienen gelijk behandeld te worden. Het stelselmatig onevenredig uitsluiten van (content van) bepaalde groepen online op basis van specifieke gronden, is in strijd met de fundamentele vrijheden en rechten zoals in het Handvest verankerd dat aan de basis ligt van de DSA. De DSA ziet toe op volledige harmonisatie van de regels voor online platforms.

De vierde zorg van de leden van de GroenLinks-PvdA-fractie is het risico op een waterbedeffect. Het afschermen van bepaalde content en websites voor jongeren, kan betekenen dat ze naar nog slechter gereguleerde platforms overstappen die geen leeftijdsverificatie vereisen. Dit kan leiden tot een verplaatsing van jongeren naar schimmige online omgevingen met nog minder toezicht. Deelt de staatssecretaris deze zorg met de leden, en neemt hij dit mee in zijn beoordeling of de inzet van leeftijdsverificatie proportioneel is?

Antwoord:

Ja, deze zorg wordt gedeeld en past in de beoordeling naar passendheid van het instrument. Tegelijkertijd is de inzet van het kabinet erop gericht digitale diensten veiliger te maken. Daarnaast is het een taak van ouders en verzorgers in gesprek te gaan met kinderen over zaken als schermtijd en het gebruik van apps.

De vijfde zorg deze leden is het gemak waarmee verificatiemethoden kunnen worden omzeild. Zo kunnen minderjarigen makkelijk een VPN (Virtual Private Network) gebruiken om hun locatie virtueel te veranderen naar een

plek zonder verificatieplicht op online platforms. Daarmee wordt het voor gebruikers die de verificatie willen omzeilen makkelijk om dat te doen, en raakt verificatie vooral gebruikers die wél hun echte locatie opgeven. Kan de staatssecretaris toelichten of de landen waar reeds met leeftijdsverificatie wordt gewerkt, ook een toename zien in het VPN-gebruik onder internetgebruikers? Hoe staat hij tegenover het gebruik van VPN's, ook door volwassenen die de verificatie willen omzeilen wegens privacy- of cyberveiligheidsbezwaren? Weegt hij dit mee in zijn beoordeling of verificatie proportioneel is?

Antwoord:

Ja, het is een bekend gegeven dat verificatiemethoden kunnen worden omzeild. Dat is te zien in Australië waar een verbod op sociale media voor de leeftijdscategorie tot zestien jaar van kracht is geworden. In het TNO-rapport zal aan dit verschijnsel van omzeiling aandacht worden besteed.

Zij vragen de staatssecretaris tevens om helder te maken in welke gevallen verschillende methoden van leeftijdsborging proportioneel en passend zijn. Kan hij dit met praktische voorbeelden toelichten? Is het voor lidstaten ook mogelijk om nationaal te bepalen dat voor bepaalde diensten juist géén verificatie nodig is, als de staatssecretaris samen met experts oordeelt dat een voorgestelde toepassing disproportioneel is?

Antwoord:

Nee, dit is niet op voorhand aan te geven. Zoals eerder beschreven zal per situatie moeten worden beoordeeld of leeftijdsverificatie een passend instrument is. Voorstelbaar is dat in een situatie waarin sprake is van een kwetsbare groep of een wettelijke leeftijdseis, passendheid eerder wordt aangenomen.

De leden van de GroenLinks-PvdA-fractie steunen de inzet van het kabinet op het bekender maken van de richtlijn

gezond schermgebruik. Deze leden vragen om dit ook op een begrijpelijke wijze onder de aandacht te brengen op plekken waar veel kinderen en opvoeders komen, zoals scholen, verenigingen of supermarkten. Wat doet de staatssecretaris om deze richtlijn met de verschillende adviesleeftijden breed te communiceren? Kan hij tevens een update geven over de ontwikkeling van een Digitale Kijkwijzer op basis van wetenschappelijk onderzoek, in samenwerking met het NICAM, n.a.v. de motie-Kathmann en Van der Werf (Kamerstuk 36600 VII, nr. 71)?

Antwoord:

Met de publicatie van de richtlijn gezond scherm- en sociale mediagebruik is een belangrijke stap gezet om gezond scherm- en sociale media gebruik door kinderen te stimuleren en te ondersteunen en kinderen digitaal weerbaarder te maken en mentaal gezond te houden. Minstens zo belangrijk is dat de adviezen nu goed worden geïmplementeerd.

Samen met o.a. de wetenschap, het Nederlands Jeugdinstituut (NJI), het Trimbos Instituut en Netwerk Mediawijsheid werkt het ministerie van VWS aan een implementatieplan: wat is er nodig om ervoor te zorgen dat alle opvoeders en professionals dezelfde adviezen en normen gaan uitdragen en nastreven?

Waar mogelijk worden bestaande kanalen en tools benut, zoals bijvoorbeeld de jeugdgezondheidszorg (jgz), de kinderopvang, het onderwijs en de MediaDiamant. Ook ben ik in gesprek met het opgavenetwerk Opvoeding in Digitale Balans over hoe het netwerk en de verbonden partijen de implementatie van de richtlijn kunnen versterken. Binnen dit opgavenetwerk wordt verschillende expertise rondom mediaopvoeding samengebracht: wetenschap/onderzoek, praktijkervaring professionals, beleidskennis en de stem van ouders, kinderen en jongeren zelf.

In december is in opdracht van VWS de vernieuwde versie van de MediaDiamant gelanceerd. Deze bekende en veelgebruikte tool voor opvoeders en professionals helpt hen te ondersteunen bij (het gesprek over) mediaopvoeding en is beschikbaar in meerdere talen.

In september 2025 is vanuit het ministerie van BZK ook de publiekscampagne 'Blijf in beeld' gestart met praktische tips en informatie om het online leven van kinderen veiliger te maken. Deze publiekscampagne wordt in de zomer van 2026 vervolgd. Op de bijbehorende website, Jouwkindonline.nl, is de richtlijn gezond schermgebruik verwerkt.

Een praktische suggestie uit het onderzoek naar de richtlijn is het ontwikkelen van een digitale Kijkwijzer. Eerder is hier door de leden Kathmann (GL-PvdA) en van der Werf (D66) ook een motie over ingediend. Na overleg tussen de verschillende betrokken ministeries is de uitvoering van deze motie overgedragen aan de ministeries van OCW en VWS. OCW is betrokken vanuit mediaregulering en is primair accounthouder van NICAM. VWS is betrokken vanuit het dossier (mentaal) gezond opgroeien en opvoeden van kinderen en jongeren. Het NICAM heeft een eerste plan opgeleverd voor de uitvoering van de motie, alleen ontbreekt het nog aan financiële middelen voor de uitvoering hiervan. De beide ministeries (OCW en VWS) bekijken nu de mogelijkheden om het plan van NICAM ten uitvoer te kunnen brengen.

Ondanks dat de leden van de GroenLinks-PvdA-fractie het belang van online veiligheid voor jongeren onderschrijven, wijzen ze er wel op dat de eenzijdige focus op minderjarigen een te beperkt beeld geeft van de problemen op online platforms. Bedrijven als X en Meta maken hun sociale media voor iedereen verslavend en polariserend; dat is hun verdienmodel. Maatregelen om dit te bestrijden, zoals het standaard aan hebben staan van de meest

privacyvriendelijke instellingen, het verbieden van manipulerende ontwerpstrucjes en het voorkomen van informatiefuiken via aanbevelingsalgoritmen, zouden voor álle gebruikers moeten gelden. Deelt de staatssecretaris de mening dat álle gebruikers van sociale media platforms een gelijke en grote mate van bescherming en keuzevrijheid verdienen? Deze leden vinden het ongeloofwaardig dat minderjarige gebruikers deze bescherming wel zouden verdienen, maar vanaf dat ze meerderjarig zijn wél opeens toegang krijgen tot een ongezondere en verslavende online-ervaring. Zij verwijzen bijvoorbeeld naar het bericht van de Autoriteit Persoonsgegevens dat TikTok gebruikersdata deelt met China⁹, een risico voor zowel jonge als oude gebruikers. Hoe wil de staatssecretaris ervoor zorgen dat álle gebruikers beschermd zijn tegen dit soort illegale praktijken?

Antwoord:

Ik deel uw mening dat de onlinewereld veilig en transparant dient te zijn voor iedereen, niet alleen voor minderjarigen. Dat minderjarigen gelden als een kwetsbare groep die extra risico's loopt in de digitale omgeving, neemt niet weg dat volwassen ook onderhevig zijn aan dezelfde risico's.

De DSA bevat grondslagen die gebruikers beschermen tegen de risico's die worden genoemd in de vraag. Zo mogen platforms hun online-interfaces niet zodanig ontwerpen, organiseren of beheren dat zij gebruikers misleiden of manipuleren, of hun vermogen om vrije en geïnformeerde beslissingen te nemen op een andere manier wezenlijk verstoren of ondermijnen (artikel 25 DSA). Daarnaast zijn VLOP's verplicht jaarlijks te beoordelen of het ontwerp en de werking van hun diensten negatieve effecten hebben op de openbare veiligheid, democratische processen, volksgezondheid en het lichamelijke en geestelijke welzijn (artikel 34). Indien dergelijke risico's worden vastgesteld, moet het platform het ontwerp of de werking van de dienst

⁹ NU.nl (16 december 2025), TikTok deelt gebruikersdata volgens privacywaakhond nog steeds met China, geraadpleegd via <https://www.nu.nl/economie/6379666/tiktok-deelt-gebruikersdata-volgens-privacywaakhond-nog-steeds-met-china.html>.

aanpassen om deze effecten te minimaliseren (artikel 35). Ten slotte moeten platforms in hun algemene voorwaarden in duidelijke taal uitleggen welke parameters zij gebruiken om informatie aan te bevelen en hoe gebruikers deze kunnen beïnvloeden (artikel 27), en moeten ze VLOPs gebruikers ten minste één optie bieden voor een aanbevelingssysteem dat niet gebaseerd is op profilering.

Bij niet naleving kan de Europese Commissie, als toezichthouder van de DSA, dwangsommen van de gemiddelde dagomzet en geldboetes opleggen ter hoogte van 6% van de wereldwijde omzet van de aanbieder die in overtreding is. Daarnaast kunnen personen en organisaties gebruik maken van de mogelijkheden om de zaak voor te leggen aan een onafhankelijke geschilbeslechtscommissie, of via de civiele rechter online platforms dagen voor overtredingen van de DSA. Er zijn inmiddels al een aantal voorbeelden waarbij Nederlandse organisaties en personen platforms voor de rechter hebben gedaagd wegens overtreding van de DSA, en dat hebben gewonnen.¹⁰

De DSA is ontworpen om de grondrechten van mensen in de onlinewereld te bestendigen en ik vind het belangrijk binnen de kaders van de wet te blijven handelen. De DSA is een relatief nieuwe wet en het vereist tijd om inzicht te krijgen of de geboden kaders en maatregelen werken zoals bedoeld. In 2027 evalueert de Europese Commissie de wet en wordt deze evaluatie voorgelegd aan het Europees Parlement, de Raad en het Europees Economisch en Sociaal Comité. Tijdens deze evaluatie is er ook de mogelijkheid om namens Nederland input te geven.

De leden van de GroenLinks-PvdA-fractie pleiten voor een ambitieuze en strenge uitwerking van de Digital Fairness Act

¹⁰ [ECLI:NL:RBAMS:2025:7253](https://ecli.nl:RBAMS:2025:7253), [Rechtbank Amsterdam, C/13/774725 / KG ZA 25-687 MK/JD](https://rechtspraak.amsterdam/C/13/774725/KG_ZA_25-687_MK/JD)

(DFA), die álle gebruikers meer keuzevrijheid geeft en hun rechten beter beschermt tegen de manipulatieve praktijken van grote techbedrijven. Kan de staatssecretaris het rapport van 4 november 2025 van het Europees Parlement over minderjarigen online appreciëren?¹¹ Welke maatregelen moeten volgens de staatssecretaris sowieso in de DFA worden opgenomen? Bepleit hij hier ook de breedgedragen oproep van de Kamer, verwoord in de motie-Kathmann en Timmermans (Kamerstuk 21501-33, nr. 1158), voor een volledig Europees verbod op radicaliserende algoritmes op basis van tracking en interactie? Wat gaat hij doen om zich hiervoor in te zetten?

Antwoord:

Ja, ik kan het rapport van het Europees Parlement appreciëren.

Algoritmen gebaseerd op tracking en interactie zorgen ervoor dat gebruikers ‘geprefereerde’ content zien. Dit heeft in de eerste instantie een commercieel doel: hoe langer gebruikers op een platform blijven, hoe meer geld er verdiend kan worden. Deze ontwerpkeuzes zijn primair gericht op het maximaliseren van betrokkenheid en schermtijd, en worden in het publieke debat regelmatig aangeduid als ‘verslavend ontwerp’. Maar ook aan de beperkte werking van platformmoderatie op basis van gebruikersmeldingen: wanneer je steeds geprefereerde content te zien krijgt, ben je minder geneigd het te melden als in strijd met platformbeleid. Dit zijn redenen om in te zetten op het verder mitigeren van de risico’s van algoritmen gebaseerd op tracking en interactie en tot beleid te komen ten aanzien van de negatieve effecten van deze algoritmen.

Daarnaast, zoals gesteld in de beantwoording van de Kamervragen over Tiktok algoritmes en extremisme, is radicalisering ‘een complex proces waarbij verschillende

¹¹ Europees Parlement (4 november 2025), REPORT on the protection of minors online | A10-0213/2025, geraadpleegd via [REPORT on the protection of minors online | A10-0213/2025 | European Parliament](#).

factoren een rol spelen'.¹² Aanbevelingsalgoritmes hebben hierin een versterkende rol. Algoritmes zijn dus geen directe oorzaak van radicalisering, maar kunnen wel bijdragen aan een versnelde toegang tot extremistische content en een grotere hoeveelheid van die content. Dit kan het proces van radicalisering versnellen of versterken, vooral bij kwetsbare gebruikers. De minister van Justitie en Veiligheid vraagt daarom in de dialoog met de internetsector expliciet aandacht voor de rol van aanbevelingsalgoritmes bij de verspreiding van extreme online content. Hiermee zal de aandacht voor de rol van deze algoritmes in het bestrijden van extremisme en terrorisme onverminderd doorgezet worden.

Tot slot wijzen deze leden erop dat beleid voor jongeren online altijd met jongeren aan tafel moet worden ontwikkeld. Zij wijzen op het recente onderzoek van HackShield, Offlimits, ESET NL en het COPS team naar het online gedrag van kinderen.¹³ Hiermee hebben zij 85.000 reacties rechtstreeks van kinderen opgehaald over wat zij online meemaken. Is de staatssecretaris bereid om dit onderzoek te betrekken bij zijn inzet voor een veiligere online omgeving voor minderjarigen? Is de staatssecretaris bereid om in gesprek te gaan met de initiatiefnemers van het onderzoek en te bezien of er vervolgonderzoeken kunnen worden gedaan, waar mogelijk ook relevante vragen kunnen worden uitgezet die waardevol zijn voor het ontwikkelen van online jongerenbeleid? Welke andere acties neemt de staatssecretaris om ervoor te zorgen dat de stem van jongeren luid en duidelijk wordt gehoord in het beleid? Is de betrokkenheid van jongeren voldoende geborgd?

Antwoord:

Het kabinetsbeleid online kinderrechten is er mede op gericht de stem van jongeren te vangen ten behoeve van

¹² Aanhangsel handelingen II, 2025/26, nr. 606.

¹³ HackShield (5 december 2025), "1 op de 3 kinderen praat met onbekenden in games", <https://nl.joinhackshield.com/nl/nieuws/401>.

ontwikkeling en bijstelling van beleid. De staatssecretaris van EZK praat voor het derde jaar op rij met jongeren uit de Jongerenraad Digitalisering die speciaal voor dit doel is opgezet in samenwerking met UNICEF. De raad wisselt regelmatig van samenstelling om telkens andere jongeren de gelegenheid te geven te vertellen wat hen bezighoudt in de digitale wereld; wat zij er leuk aan vinden maar ook waar zij risico's zien en wat naar hun idee daarvoor een oplossing zou kunnen zijn.

Daarnaast heeft de staatssecretaris van BZK in september 2025 een strategiebrieftje online kinderrechten aan uw Kamer gezonden. Deze strategie is tot stand gekomen in nauwe samenwerking met andere departementen, het maatschappelijk middenveld (waaronder Offlimits en Hackshield), de wetenschap, toezicht en ontwikkelaars van digitale diensten. Voor dit jaar voorziet de staatssecretaris van BZK een actualisering van deze strategie, opnieuw in samenwerking met genoemde partijen.

In zijn algemeenheid geldt dat de staatssecretaris van EZK relevante stakeholders betreft bij het vormgeven van beleid. Zij spreekt daarom met verschillende partijen en neemt kennis van (wetenschappelijke) literatuur en onderzoeken. Waar nodig worden onderzoeken en opdrachten uitgezet. De staatssecretaris volgt daarbij de regels die gelden voor aanbesteding en subsidieverlening.

Vragen en opmerkingen van de leden van de CDA-fractie

De leden van de CDA-fractie hebben kennisgenomen van het Fiche inzake DSA richtsnoeren betreffende minderjarigen online en danken het kabinet hiervoor. Deze leden maken graag van de gelegenheid gebruik om enkele vragen aan het kabinet te stellen hierover.

Zij constateren dat de richtsnoeren zowel inzetten op een risicogebaseerde aanpak als op het beperken van schadelijke ontwerpkeuzes en aanbevelingssystemen. De leden van de CDA-fractie vragen hoe het kabinet gaat borgen dat platforms deze maatregelen in de praktijk daadwerkelijk en zorgvuldig toepassen en hoe de uitvoerbaarheid en handhaafbaarheid hiervan wordt gegarandeerd, zodat minderjarigen niet langer worden blootgesteld aan schadelijke of manipulatieve online prikkels en zich bewust worden van het feit dat (niet-Europese) Big Tech bedrijven en landen mogelijk over hun (privacygevoelige) data beschikken indien zij actief zijn op het internet of bepaalde platforms.

Antwoord:

De Europese Commissie heeft laten weten dat ze de richtsnoeren als maatstaf ziet voor handhaving. Dat is een belangrijke stimulans voor platforms om er uitvoering aan te geven. Ik heb geen signalen om eraan te twifelen dat de richtsnoeren uitvoerbaar en handhaafbaar zijn. Indien dit de komende tijd toch niet het geval blijkt, dan heeft de Europese Commissie de mogelijkheid om de richtsnoeren na raadpleging van de digitale dienstencoördinatoren te wijzigen.

Deze leden vragen verder hoe het kabinet gaat waarborgen dat alle betrokken partijen, en met name de grote online platforms, hun verantwoordelijkheid daadwerkelijk nemen om hardnekkige risico's zoals cyberpesten, uitbuiting, schadelijke content en online misbruik te verkleinen, en hoe wordt voorkomen dat schadelijke maar niet-illegale "borderline"-inhoud buiten beeld blijft bij moderatie en toezicht. Is het kabinet bereid om in Europees verband draagvlak te verkrijgen om harder op te treden tegen cyberpesten?

Antwoord:

Zoals is geantwoord op eerdere vragen over borderline en schadelijke content wordt er gewerkt aan een Europese aanpak van extremistische content. Online platformen stellen daarnaast veelal zelf voorwaarden aan het gebruik van hun diensten, op basis waarvan ze moderatie verrichten. In die voorwaarden worden ook vaak regels gesteld voor niet-illegale inhoud, zoals 'borderline content'. Zij zijn verplicht om die voorwaarden te handhaven. Doe ze dan niet, dan kunnen toezichthouders daar onderzoek naar verrichten en desnoods handhavend optreden.

Wat betreft cyberpesten geldt dat scholen een zorgplicht hebben voor een veilig schoolklimaat. Met het wetsvoorstel vrij en veilig onderwijs dat momenteel in uw Kamer ligt scherpt het kabinet die zorgplicht aan. Onder andere door vertrouwenspersonen te verplichten op elke school, en incidenten te registreren, en te melden als het ernstige incidenten betreft. OCW subsidieert Stichting School en Veiligheid om scholen hierin te ondersteunen. Stichting School en Veiligheid heeft ook specifieke handreikingen over cyberpesten.

Aanvullend hierop zet het kabinet via het Nederlandse Safer Internet Centre in op de preventie en aanpak van cyberpesten en ander schadelijk online gedrag. Het Safer Internet Centre Nederland wordt gecoördineerd door Offlimits en geeft uitvoering aan de Better Internet for Kids-strategie van de Europese Commissie.

Offlimits vervult binnen dit samenwerkingsverband de rol van meldpunt, hulplijn en jongerenpanel. Via de hulplijn kunnen kinderen en jongeren laagdrempelig ondersteuning krijgen bij online grensoverschrijdend gedrag, waaronder cyberpesten. Daarnaast draagt het Safer Internet Centre actief bij aan de Europese beleidsontwikkeling, onder meer op het Europese actieplan tegen cyberpesten. In 2026 ligt

binnen het Safer Internet Centre bovendien een nadrukkelijke focus op zogenoemde “harmful but lawful”-problematiek, waaronder cyberpesten. Daarmee wordt niet alleen ingezet op het bestrijden van strafbare feiten, maar ook op het tegengaan van schadelijk gedrag dat binnen de grenzen van de wet blijft, onder meer door dialoog met platforms, ondersteuning van gebruikers en versterking van online weerbaarheid.

De leden van de CDA-fractie steunen de risicogebaseerde aanpak. Echter, deze leden vragen wel hoe het kabinet beoordeelt of de ingezette maatregelen, zoals safety-by-design, leeftijdsverificatie en het versterken van digitale weerbaarheid, voldoende ambitieus zijn om het tempo en de schaal van online risico's bij te benen, en hoe wordt geborgd dat deze initiatieven daadwerkelijk leiden tot merkbaar veiliger online gedrag van kinderen.

Antwoord:

De vraag van deze leden is terecht. Het kabinet voert een robuust online kinderrechtenbeleid en wil daarmee de gewenste effecten bereiken. Tegelijkertijd is duidelijk dat ontwikkelingen in de digitale wereld snel gaan. Het kabinet wil langs verschillende wegen borgen dat zij bijblijft maar ook resultaten ziet van het ingezette beleid. Met de verzamelbrief digitalisering van december 2025¹⁴ heb ik u geïnformeerd over de forecast die ik heb laten uitvoeren om tijdig zicht te krijgen op de impact van nieuwe technologieën op de samenleving. Daarbij heeft TNO op mijn verzoek expliciet oog gehad voor de doelgroep minderjarigen. Op dit moment wordt de forecast onder de aandacht gebracht van verschillende overheden om samen met hen te beoordelen wat er - naast al bestaand beleid - nodig is zodat mensen en bedrijven deze technologieën op een verantwoorde manier gebruiken. Ook breng ik de kennis die in Nederland wordt opgedaan over de impact van technologie op de samenleving

¹⁴ Kamerstukken II, 2025/2026, 26643, nr. 1450

in bij de Europese Commissie en de relevante raads werkgroepen.

Daarnaast worden evaluaties van verschillende beleidsinstrumenten uitgevoerd. In dit voorjaar wordt het resultaat verwacht van een aantal van die evaluaties. Op basis daarvan zal waar nodig beleid wordt bijgesteld. Tenslotte is een online kinderrechtenstrategie ontwikkeld (hierboven al beschreven) die jaarlijks wordt geactualiseerd op basis van nieuwe inzichten, nieuwe input van onder meer de jongeren uit de Jongerenraad Digitalisering, uitkomsten van de inzet van beleidsinstrumenten zoals de kinderrechten impact assessments en gesprekken met maatschappelijk middenveld, toezicht, wetenschap en ontwikkelaars van digitale diensten.

Zij vragen ook hoe het kabinet ervoor zorgt dat de richtsnoeren als handhavingsbenchmark worden toegepast in de EU, hoe platforms worden gestimuleerd de Kinderrechtenimpactassessment (KIA) te gebruiken, hoe transparantie over aanbevelingssystemen wordt afgedwongen en hoe versnippering met de Digital Fairness Act wordt voorkomen, zodat schadelijke ontwerptechnieken, algoritmes en moderatielacunes structureel en Europees breed worden aangepakt. In het Fiche staat hierover het volgende: "Platforms moeten daarnaast voorkomen dat het gebrek aan commerciële geletterdheid van kinderen wordt uitgebuit" (Kamerstuk 22112, nr. 4207).

Antwoord:

De Europese Commissie heeft reeds aangegeven de richtsnoeren te zullen gebruiken als benchmark voor haar toezicht, en dat van de digitaledienstencoördinatoren. Verdere maatregelen daartoe van het kabinet zijn daarom op dit moment niet nodig. De richtsnoeren verduidelijken verder dat het verrichten van een Kinderrechtenimpactassessment (KIA) één van de mogelijke instrumenten is waarmee online

platforms uitvoering kunnen geven aan de verplichtingen van artikel 28 DSA. Net als vergelijkbare instrumenten van UNICEF en CEN-CENELEC. Gegeven het belang van de richtsnoeren zal dit online platforms uitnodigen om te onderzoeken of zij een Kinderechtenimpactassessment of vergelijkbaar instrument moeten inzetten om ervoor te zorgen dat zij artikel 28 DSA naleven. Om het nut en de toegevoegde waarde van KIAs onder de aandacht te brengen heeft het kabinet het instrument in het verleden gepresenteerd aan de Europese Commissie en diverse lidstaten.

De DSA bevat in artikel 27 regels over de transparantie van aanbevelingssystemen. Dit artikel verplicht aanbieders van online platforms die gebruikmaken van aanbevelingssystemen om in hun algemene voorwaarden in duidelijke en begrijpelijke taal de belangrijkste parameters te vermelden die in hun aanbevelingssystemen worden gebruikt. Zij moeten daarin ook beschrijven welke opties afnemers van de dienst hebben om deze belangrijkste parameters te wijzigen of te beïnvloeden. Aanbieders van zeer grote online platforms en zoekmachines zijn op grond van artikel 38 DSA verplicht om afnemers ten minste een optie te bieden van een aanbevelingssysteem dat niet gebaseerd is op profilering. Dat draagt ook bij aan transparantie over aanbevelingssystemen omdat afnemers na het (tijdelijk) uitzetten of gebruiken van het online platform zonder de invloed van zo'n systeem kunnen zien hoe het er dan uit ziet, en welke content ze dan te zien krijgen.

Voor de vraag hoe versnippering met de DFA wordt voorkomen, verwijs ik naar mijn antwoord op de vraag van de D66-fractie over het tegengaan van overlap van de DSA en de DFA.

Ook maken de leden van de CDA-fractie zich zorgen over de prikkels via social media om allerlei aankopen te doen, soms

ook met buy-now-pay-later opties (met schulden onder jongeren tot gevolg). Hoe kunnen we deze zaken beperken via aangescherpte regelgeving van de DSA? Is het kabinet bereid om daarover nader in gesprek te gaan in Europa?

Antwoord:

De DSA is pas relatief recent van kracht geworden en het toezicht erop door de Europese Commissie en autoriteiten in de lidstaten begint nu op gang te komen. Het is op dit moment nog te vroeg om de DSA aan te gaan scherpen. Indien dit noodzakelijk of wenselijk is, dan is daar voor het eerst gelegenheid voor na de evaluatie ervan eind 2027.

Daarnaast vragen deze leden hoe het kabinet gaat borgen dat platforms hun moderatie- en klachtenprocedures verbeteren, dat kinderen beter worden beschermd tegen schadelijke maar niet-illegale inhoud, en dat leeftijdsverificatie alleen zorgvuldig, proportioneel en privacybeschermend wordt ingezet, inclusief duidelijkheid over de mogelijke ontwikkeling van een Nederlandse verificatie-app.

Antwoord:

Er zijn sinds de inwerkingtreding van de uitvoeringswet van de DSA meerdere zogeheten betrouwbare flaggers aangewezen door de ACM als digitaaldienstencoördinator. Betrouwbare flaggers zijn organisaties die een speciale status genieten bij het melden van illegale inhoud. Hun meldingen moeten door online platforms met voorrang en onverwijld worden behandeld. Zo is er Meld Online Discriminatie voor online discriminatie en Offlimits voor online misbruik. Daarnaast wordt er in 2026 samengewerkt met Offlimits om handelingsperspectieven te ontwikkelen voor een breder pallet van schadelijke maar legale content. Voor wat betreft leeftijdsverificatie verwijs ik u graag naar het antwoord dat hiervoor is gegeven op vragen van leden van de D66-fractie en hieronder aan leden van de BBB-

fractie. We zetten in op bewijsvoering door middel van onderzoek, standaardisering van transparantierapportages en impact assessments. Daarnaast willen we een portaal maken om toegang tot gerechtelijke instanties makkelijker te maken. En mensen bewuster maken van hun digitale rechten en handelingsperspectief.

Zij vragen verder hoe het kabinet de brede Europese steun voor de richtsnoeren, waaronder de Jutland-verklaring, gaat benutten om platformverplichtingen verder te concretiseren en een effectieve, uniforme handhaving in alle lidstaten te waarborgen, en hoe zij het huidige Europese krachtenveld beoordeelt, inclusief de oproep van de IMCO-commissie (Internal Markt and Consumer Protection) om verslavende ontwerptechnieken te verbieden, met het oog op een actieve Nederlandse inzet voor verdere Europese stappen om schadelijke digitale prikkels voor minderjarigen tegen te gaan.

Antwoord:

Verdere concretisering en effectieve, uniforme handhaving, is nu aan de onafhankelijk toezichthouders. Uiteraard zal ik hen daarbij ondersteunen of faciliteren als ze daarom vragen of daar waar lidstaten een rol hebben. Zoals bijvoorbeeld bij het vaststellen van uitvoeringshandelingen en gedelegeerde handelingen door de Europese Commissie. In het non-paper over de DFA roept het kabinet op tot een verdere Europese aanpak tegen verslavende ontwerptechnieken. Met name via een verbod op verslavende ontwerptechnieken die het welzijn van consumenten schaden, zoals technieken die leiden tot overmatig gebruik.

Het voorkomen van deze negatieve impact op minderjarigen vraagt ook om goede voorlichting, bewustwording en mogelijkheden voor ouders en scholen om hier mee om te gaan. Ziet het kabinet kans om maatschappelijke organisaties hierbij te consulteren? Denk aan het Nederlands

Jeugdinstituut dat ook nadenkt over de positieve en negatieve gevolgen van mediagebruik door jongeren¹⁵.

Antwoord:

Ja. Het kabinet ziet nadrukkelijk ruimte om maatschappelijke organisaties te consulteren bij voorlichting en bewustwording over de impact van (digitale) media op minderjarigen. Organisaties zoals het Nederlands Jeugdinstituut beschikken over waardevolle expertise over zowel de risico's als de kansen van mediagebruik door jongeren. Zij worden al betrokken bij de publiekscampagne van BZK. Deze kennis wordt benut voor onder meer de inzet op de publiekscampagne 'Blijf in beeld', die ouders en opvoeders ondersteunt met toegankelijke informatie en handelingsperspectief. Hiermee wordt ingezet op samenhang tussen beleid, praktijkkennis en publieksvoorlichting.

De leden van de fractie-CDA vragen het kabinet welke waarborgen zij (additioneel) wil regelen op nationaal niveau, naast deze Europese wetgeving. Op welk niveau wordt de handhaving vanuit de overheid (waaronder het uitdelen van boetes) uitgevoerd en zijn hier personele middelen voor beschikbaar?

Antwoord:

De DSA vormt maximumharmonisatie van de verplichtingen voor aanbieders van tussenhandeldiensten binnen het toepassingsgebied van de verordening zoals bepaald in artikel 2 DSA. De ruimte die er daardoor nog bestaat voor lidstaten om nationaal aanvullende regels te stellen is beperkt. Gegeven het veelal grensoverschrijdende karakter van deze diensten acht ik het effectiever om eventuele aanvullende regels op EU-niveau te stellen om zo een gelijk

¹⁵ Nederlands Jeugdinstituut (2025), 'Mediagebruik van ouders', geraadpleegd via <https://www.nji.nl/kennis/mediaopvoeding/mediagebruik-door-pubers#:~:text=Voelen%20en%20emoties-.In%20het%20kort,om%20hun%20identiteit%20te%20verkennen.>

speelveld te waarborgen en te voorkomen dat er een 'waterbedeffect' optreedt waarbij dienstverleners zich verplaatsen naar de lidstaat die geen of het minste aanvullende regels stelt ten opzichte van de DSA.

Deze leden verwijzen naar het recente bericht van het Europees Parlement waarin wordt voorgesteld dat kinderen pas vanaf 16 jaar toegang zouden moeten krijgen tot sociale mediaplatforms¹⁶. Zij vragen hoe het kabinet dit voorstel beoordeelt, welke gevolgen dit zou hebben voor Nederland en of de staatssecretaris bereid is de Kamer te informeren over de wenselijkheid, haalbaarheid en mogelijke beleidsalternatieven rondom een dergelijke minimumleeftijd in de Nederlandse context.

Antwoord:

Inmiddels is in het Coalitieakkoord opgenomen dat er een handhaafbare Europese minimumleeftijd van 15 jaar voor sociale media moet komen met privacyvriendelijke leeftijdsverificatie, zolang sociale media onvoldoende veilig zijn. Momenteel wordt onderzocht langs welke juridische weg dit is te bereiken.

Dit neemt niet weg dat bij de ontwikkelaars van digitale diensten de verantwoordelijkheid voor veiligheid ligt in de vorm van onder meer verplichtingen uit de DSA. Het kabinet en (Europese) toezichthouders houden dat nauwlettend in de gaten.

De leden van de CDA-fractie vragen hoe het kabinet de verwachte positieve effecten van de richtsnoeren op regeldruk, toezicht en rechtszekerheid beoordeelt, en op

¹⁶ Europarl (26 november 2025), 'Children should be at least 16 to access social media, say MEPs', geraadpleegd via <https://www.europarl.europa.eu/news/en/press-room/20251120IPR31496/children-should-be-at-least-16-to-access-social-media-say-meps>.

welke wijze zij gaat voorkomen dat de vrijwillige maatregelen die mogelijk extra uitvoeringslasten met zich meebrengen alsnog leiden tot onduidelijkheid of ongelijkheid tussen bedrijven, terwijl tegelijk wordt gewaarborgd dat ook grote niet-EU-platforms deze richtsnoeren effectief toepassen ondanks het uitblijven van directe geopolitieke gevolgen.

Antwoord:

De richtsnoeren helpen bedrijven om uitvoering te geven aan de bestaande verplichting uit artikel 28 DSA door te verduidelijken wat er van hen verwacht wordt. Dit is naar verwachting positief voor de regeldruk omdat het onduidelijkheid vermindert. Doordat de richtsnoeren als maatstaf fungeren voor de Europese Commissie en de digitaledienstencoördinatoren wordt bovendien hun toezicht vergemakkelijkt en de kans op ongelijke behandeling van bedrijven in verschillende lidstaten verkleind, ongeacht hun vestigingsplaats.

De DSA is van toepassing op alle tussenhandeldiensten die in de EU worden aangeboden. Aanbieders van tussenhandeldiensten die geen vestiging in de EU hebben, dienen een wettelijk vertegenwoordiger in een lidstaat aan te wijzen die kan worden geraadpleegd door de autoriteiten en die in voorkomende gevallen zelfs aansprakelijk kan worden gesteld voor niet-naleving van de DSA (artikel 13 DSA). Daarmee is het mogelijk om ook naleving van ondernemingen die hun voornaamste vestiging niet in de EU hebben te verzekeren. Dat handhaving van de DSA geopolitieke gevolgen kan hebben is wellicht waar, maar dat moet volgens het kabinet geen reden zijn om daarvan af te zien. De EU en haar lidstaten zijn soeverein in het stellen van de regels voor tussenhandeldiensten zoals die worden aangeboden op de interne markt.

Vragen en opmerkingen van de leden van de BBB-fractie

De leden van de BBB-fractie hebben het Fiche met belangstelling gelezen. Deze leden delen de mening van het kabinet dat onze kinderen en jongeren opgroeien in een wereld waarin schermtijd, sociale media en online contacten een groot deel van hun leven vormen. Tegelijk zien zij ook het aantal risico's toenemen: identiteitsfraude, online pesten, verslaving, misinformatie, deepfakes en ongewenste beïnvloeding zijn reële bedreigingen. Jongeren, maar ook ouderen en andere kwetsbare groepen, verdienen extra bescherming én goede voorlichting om weerbaar te blijven. Daarbij zijn de leden van de BBB-fractie van mening dat niet het schermgebruik doorslaggevend is, maar vooral wát jongeren online doen, welke content zij zien, met wie zij contact hebben en in welke omstandigheden dat gebeurt. Daarnaast wegen factoren zoals schoolstress, prestatiedruk en sociale ongelijkheid minstens zo zwaar. Bovendien zijn offline en online voor jongeren nauw met elkaar verweven. De digitale omgeving brengt risico's met zich mee, zoals cyberpesten, maar biedt óók kansen op het gebied van sociale verbondenheid, creativiteit en leren.

In dit licht zien deze leden het belang van duidelijke leeftijdsgrenzen, maar ook van een bredere, integrale aanpak. Mediawijsheid, samenwerking met platforms en goede ondersteuning aan ouders, professionals en zorgverleners zijn noodzakelijk om jongeren veilig en gezond te laten opgroeien. De leden van de BBB-fractie zijn daarom van mening dat Nederland binnen de EU inzet moet tonen voor een uniform en privacyvriendelijk systeem voor leeftijdsverificatie, dat ook voor sociale-media-apps geldt. Dat biedt duidelijkheid aan gebruikers en versterkt de bescherming van minderjarigen online.

Tegen deze achtergrond hebben deze leden een aantal vragen over de DSA-richtsnoeren betreffende minderjarigen online. Allereerst: de richtsnoeren zijn van toepassing op alle online platforms, behalve op micro- en kleine ondernemingen. Kan de staatssecretaris toelichten waarom er voor deze uitzondering is gekozen? Welke overwegingen liggen hieraan ten grondslag?

Deelt de staatssecretaris de mening dat ook kleine online platforms risico's voor minderjarigen kunnen creëren, bijvoorbeeld doordat zij vergelijkbare functies aanbieden (chat, beeldmateriaal, aanbevelingssystemen)? Zo ja, hoe wordt voorkomen dat risico's ontstaan doordat minderjarigen uitwijken naar kleinere aanbieders die niet onder deze richtsnoeren vallen? Kan de staatssecretaris uitleggen vanaf welke omvang of omzet een onderneming niet langer als micro- of klein wordt aangemerkt? En op basis van welke EU-normen of criteria wordt deze grens bepaald?

Antwoord:

De DSA bevat een fors aantal verplichtingen voor aanbieders van tussenhandeldiensten. Deze zijn bedoeld om een veilige, voorspelbare en betrouwbare onlineomgeving te creëren. Naarmate de invloed van deze diensten op de maatschappij en economie groter is, schrijft de DSA zwaardere verplichtingen voor. Zo zijn de zwaarste verplichtingen van toepassing op online platforms en zoekmachines die gemiddeld meer dan 45 miljoen maandelijks actieve gebruikers in de Unie hebben. Zogenaamde 'zeer grote online platforms' en 'zeer grote online zoekmachines'.

Naleving van de DSA kan een toetredingsdrempel voor nieuwe tussenhandeldiensten vormen terwijl de risico's niet per se (direct) groot zijn als een tussenhandeldienst nog maar een micro- of kleinbedrijf is. Daarom is ervoor gekozen om zogenaamde micro- en kleine bedrijven uit te zonderen

van een deel van de verplichtingen uit de DSA.¹⁷ Zo wordt onnodige regeldruk voorkomen, blijven toetredingsdrempels laag, wordt innovatie niet belemmerd en wordt rekening gehouden met de beperkte risico's van micro- en kleine ondernemingen.

De definitie van micro- en kleine ondernemingen is gegeven in Aanbeveling 2003/361/EG. Een "kleine onderneming" is een onderneming waar minder dan 50 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal 10 miljoen EUR niet overschrijdt. Een "micro-onderneming" is een onderneming waar minder dan 10 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal 2 miljoen EUR niet overschrijdt.

Om te voorkomen dat een onderneming de verplichtingen uit de DSA tracht te ontwijken is overigens geregeld dat de verplichtingen voor zeer grote online platforms en zoekmachines ook van toepassing zijn op online platforms en zoekmachines die onder de grens van het micro- of kleinbedrijf blijven, maar wel gemiddeld wel meer dan 45 miljoen maandelijks actieve gebruikers hebben (artikel 19, tweede lid, DSA).

Dat minderjarigen uitwijken naar aanbieders van tussenhandeldiensten die onder de uitzonderingen van de DSA vallen, kan niet worden voorkomen, maar dit betekent niet automatisch dat minderjarigen daar grotere risico's lopen. Ook deze diensten moeten immers nog altijd voldoen aan diverse verplichtingen uit de DSA. Zo moeten zij over kennisgevings- en actiemechanismen beschikken zodat gebruikers mogelijke illegale inhoud kunnen melden (artikel 16 DSA) en moeten zij een motivering geven voor opgelegde beperkingen, zoals het schorsen van een account of de verwijdering van een post (artikel 17 DSA). Voor zover er

¹⁷ Zie voor de definities van het micro- en kleinbedrijf Aanbeveling 2003/361/EG.

toch risico's bestaan, is het belangrijk dat minderjarigen en ouders zich daar bewust van zijn.

Naast de verplichtingen uit de DSA zet het kabinet in op flankerend beleid om risico's voor minderjarigen in de onlineomgeving te beperken en hun digitale weerbaarheid te versterken. Zo biedt de Richtlijn Gezond en Verantwoord Schermgebruik ouders, opvoeders en professionals concrete handvatten voor bewust en evenwichtig schermgebruik. Daarnaast draagt de publiekscampagne 'Blijf in beeld' bij aan bewustwording bij ouders en jongeren over online risico's en het belang van betrokken digitaal opvoeden.

Verder voert het ministerie van EZK Kinderrechtenimpactanalyses (KIA's) uit om inzichtelijk te maken welke risico's en kansen deze platforms met zich meebrengen voor kinderen en hun rechten. De uitkomsten hiervan worden benut om beleid beter te onderbouwen en waar nodig aanvullende maatregelen te verkennen. Hiermee wordt invulling gegeven aan een bredere aanpak waarin bescherming van minderjarigen niet uitsluitend leunt op verplichtingen voor aanbieders, maar wordt ondersteund door preventie, bewustwording en beleidsmatige borging van online kinderrechten.

Verder constateren zij dat de richtsnoeren zich richten op aanbieders van online platforms. Hoe definieert de staatssecretaris een 'online platform' in de context van de DSA? Valt een dienst als Wordfeud, waar gebruikers ook met elkaar kunnen chatten, bijvoorbeeld onder deze definitie? Zo ja, wat betekent dit voor vergelijkbare spellen en apps?

Antwoord:

De definitie van een 'online platform' wordt in artikel 3, onderdeel i, van de DSA gegeven: *“een hostingdienst¹⁸ die, op verzoek van een afnemer van de dienst, informatie opslaat en verspreidt bij het publiek, tenzij die activiteit een klein of een louter bijkomend kenmerk van een andere dienst of een kleine functionaliteit van de hoofddienst uitmaakt en om objectieve en technische redenen niet kan worden gebruikt zonder die andere dienst, en de integratie van het kenmerk of de functionaliteit in de andere dienst geen manier is om de toepasbaarheid van deze verordening te omzeilen”*.

Doorslaggevend in deze definitie is met name dat een online platform op verzoek van een afnemer informatie verspreidt bij het publiek. Wat verspreiding bij het publiek is wordt gedefinieerd in artikel 3, onderdeel k: *“het op verzoek van de informatieverstrekende afnemer van de dienst beschikbaar stellen van informatie aan een mogelijk onbeperkt aantal derden”*. Hieruit, en uit overweging 14, wordt duidelijk dat een dienst die chatten tussen een beperkt aantal personen mogelijk maakt, maar niet het delen van informatie met een mogelijk onbeperkt aantal derden, niet onder de definitie van een 'online platform' valt.

De leden van de BBB-fractie lezen dat de richtsnoeren risicogebaseerde aanpak hanteren: hoe hoger het risico, hoe zwaarder de maatregelen. Hoe worden deze risico's in de praktijk ingeschat? Op basis van welke indicatoren, criteria of instrumenten (zoals het Kinderrechtenimpactassessment) wordt bepaald of een platform een hoog, middelmatig of laag risico vormt voor minderjarigen?

Antwoord:

De inschatting van risico's wordt in de eerste plaats verricht door de platforms zelf. Op grond van artikel 34 van de DSA

¹⁸ De definitie van een hostingdienst wordt in artikel 3, onderdeel g, onder iii, gegeven: *een “hosting”-dienst, die bestaat in de opslag van de door een afnemer van de dienst verstrekte informatie, op diens verzoek.*

zijn aanbieders van zeer grote online platforms en zoekmachines verplicht om jaarlijks een risicoanalyse uit te voeren. Daarbij brengen zij systemische risico's in kaart, waaronder risico's voor de bescherming van minderjarigen, zoals blootstelling aan schadelijke content, ontwerpkeuzes die verslavend kunnen werken en risico's voor privacy en welzijn.

De ernst en waarschijnlijkheid van deze risico's bepalen in hoeverre zwaardere risicobeperkende maatregelen nodig zijn. Richtsnoeren hanteren hierbij een risicogebaseerde aanpak: hoe groter het vastgestelde risico, hoe ingrijpender de maatregelen die van platforms worden verwacht.

Instrumenten zoals een KIA kunnen hierbij aanvullend worden ingezet om risico's voor minderjarigen systematisch en vanuit kinderrechtenperspectief in kaart te brengen, maar vervangen de wettelijke verplichtingen van platforms onder de DSA niet.

Deze leden zien dat volgens de richtsnoeren de leeftijdsverificatie in verschillende situaties een passende en evenredige maatregel is, onder meer wanneer nationale regels minimumleeftijden voorschrijven. Bestaan er in Nederland al nationale leeftijdsgrenzen die onder deze categorie vallen voor sociale platformen? Zo nee, vindt de staatssecretaris leeftijdsverificatie dan alsnog passend en evenredig wanneer risico's hoog zijn? En welke vorm van leeftijdsverificatie heeft daarbij de voorkeur?

Antwoord:

Het kabinet wil inzetten op een handhaafbare Europese minimumleeftijd van 15 jaar voor sociale media, zolang sociale media onveilig zijn. Ook andere digitale diensten vragen om online leeftijdsverificatie. Door verschillende betrokken ministeries wordt momenteel gewerkt aan de wettelijke borging van adequate leeftijdsverificatie bij wettelijke leeftijdsvereisten of is reeds wetgeving van toepassing. In de Alcoholwet is de leeftijdsgrens op 18 jaar gesteld en is het hebben van een leeftijdscontrolesysteem verplicht bij de online verkoop van alcohol. Sinds de legalisering van online gokken per 1 oktober 2021 is online gokken enkel voor meerderjarigen toegestaan. Deze wetgeving bevat sindsdien ook de verplichting voor dienstenaanbieders om vast te stellen dat de speler 18 jaar of ouder is. Het Ministerie van Financiën werkt aan een wettelijk verbod voor het aanbieden van Buy Now Pay Later diensten aan minderjarigen en de wettelijke verplichting voor de aanbieder om de leeftijd van de consument te verifiëren.

Het kabinet kijkt of het proportioneel is om een leeftijdsgrens te stellen en leeftijdsverificatie in te zetten als handhavingsmiddel om kinderen en jongeren te beschermen als sociale media niet veilig zijn voor hen. Ook wordt gekeken naar de gevolgen voor de grondrechten. Bij deze verkenning wordt rekening gehouden met de Europese kaders en publieke waarden als toegankelijkheid, proportionaliteit, transparantie en handhaafbaarheid.

Om te voorkomen dat jongeren uitwijken naar minder gereguleerde platforms, is een uniform systeem nodig. Hoe borgt het kabinet dat alle online platforms die door jongeren worden gebruikt - ook minder voor de hand liggende diensten - onder dezelfde kaders voor leeftijdsverificatie en ouderlijke toestemming vallen? Op welke manier voorkomt het kabinet dat jongeren kunnen uitwijken naar alternatieve, minder veilige of niet-goedgekeurde platforms? Welke lessen

trekt het kabinet uit voorbeelden in andere landen (zoals Australië) waar gefragmenteerde wetgeving ertoe heeft geleid dat jongeren massaal uitwijken naar minder veilige apps?

Antwoord:

Een algemeen leeftijdsverificatiesysteem voor alle situaties is niet mogelijk. Zoals eerder omschreven is TNO gevraagd om te kijken naar de organisatorische, juridische, technische en financiële haalbaarheid van nationale implementatie van een losse 'standalone' leeftijdsverificatie-app in Nederland. Hierbij kijkt TNO ook naar de impact op belangrijke waarden, zoals privacy, betrouwbaarheid, veiligheid en toegankelijkheid. Op basis daarvan zal ik uw Kamer informeren over de gekozen richting. In het online kinderrechtenbeleid is de inzet van het kabinet erop gericht digitale diensten veiliger te maken. Daarnaast is het een taak van ouders en verzorgers in gesprek te gaan met kinderen over zaken als schermtijd en het gebruik van apps.

Jongere kinderen en oudere tieners hebben andere ontwikkelingsniveaus en kwetsbaarheden. Deelt de staatssecretaris de mening van de leden van de BBB-fractie dat een 10-jarige andere bescherming verdient dan een 16-jarige? Hoe wordt dit onderscheid gemaakt binnen de toepassing van de richtsnoeren? Welke factoren worden in deze afweging betrokken?

Antwoord:

Ja, deze mening deel ik. In de richtsnoeren worden de maatregelen beschreven die aanbieders van voor minderjarigen toegankelijke onlineplatforms volgens de Commissie moeten nemen om een hoog niveau van privacy, veiligheid en bescherming van minderjarigen online te waarborgen, overeenkomstig artikel 28, lid 1, van Verordening (EU) 2022/2065. De richtsnoeren maken geen

onderscheid in te nemen maatregelen naar leeftijd. Deze inschatting ligt bij de aanbieders zelf. Er is op Europees niveau of nationaal niveau vooralsnog geen minimumleeftijd vastgelegd in Unierecht of nationaal recht voor toegang tot specifiek gedefinieerde categorieën onlinediensten voor sociale media. In het coalitieakkoord wordt ingezet op een handhaafbare Europese minimumleeftijd van 15 jaar voor sociale media met privacyvriendelijke leeftijdsverificatie voor jongeren, zolang sociale media onvoldoende veilig zijn en strenger toezicht.

In het advies richtlijn gezond scherm- en sociale mediagebruik is deze differentiatie wel aangebracht. In de richtlijn zijn leeftijdsadviezen opgenomen voor schermtijd, alsmede gebruik van sociale interactie platforms en sociale media platforms. Dit vanuit de gedachte dat kinderen bewust, veilig en gezond, onder begeleiding van opvoeders stapsgewijs moeten leren omgaan met sociale media. Ondersteunende tools zoals de Mediadiamant en de toolbox Mediaopvoeding (NJI) maken ook onderscheid in leeftijd en bieden handelingsperspectief per leeftijdscategorie. Hiernaast verkennen de ministeries OCW en VWS de ontwikkeling van een Digitale Kijkwijzer. Een eventuele online Kijkwijzer informeert ouders en opvoeders tot welke leeftijd diensten schadelijk zijn voor kinderen.

De Jutland-verklaring roept expliciet op tot strengere, uniforme maatregelen om kinderen online te beschermen, zo constateren deze leden. Hoe verhoudt de voorzichtige Nederlandse appreciatie van leeftijdsverificatie zich tot deze politieke verplichting die Nederland zelf onderschreven heeft?

Kan de staatssecretaris toelichten op welke wijze leeftijdsverificatie, mits privacyvriendelijk ingericht, wél proportioneel kan zijn? Erkent hij dat de huidige formulering in het Fiche onterecht de indruk wekt dat leeftijdsverificatie per definitie disproportioneel is?

Antwoord:

Het uitgangspunt van het Nederlandse beleid is 'safety-by-design': digitale diensten moeten vanaf het begin veilig zijn voor minderjarigen. Bedrijven moeten schadelijke ontwerpstechnieken vermijden, schadelijke content weren en zorgvuldig omgaan met persoonsgegevens van kinderen. Omdat veel diensten niet volledig veilig zijn, kunnen aanvullende maatregelen zoals leeftijdsverificatie en ouderlijk toezicht nodig zijn, maar deze ontslaan bedrijven niet van hun voortdurende verantwoordelijkheid om hun diensten zo veilig mogelijk te maken. Deze maatregelen zijn hulpmiddelen, geen doel op zich. Ten aanzien van effectieve en privacy vriendelijke leeftijdsverificatie op sociale media en andere relevante digitale diensten die een risico vormen voor kinderen is de Nederlandse inzet als volgt. Het gebruik van leeftijdsverificatie kan, in combinatie met andere maatregelen, kinderen online beter beschermen. Daarom is het belangrijk om leeftijdsverificatie op een robuuste en betrouwbare manier mogelijk te maken, waarbij fundamentele rechten zoals privacy, gegevensbescherming en non-discriminatie worden gewaarborgd. Daarnaast moeten verschillende methoden voor leeftijdsverificatie beschikbaar zijn om inclusiviteit te bevorderen en te voorkomen dat gebruikers gedwongen worden een specifieke methode te gebruiken.

Vragen en opmerkingen van de leden van de SGP-fractie

De leden van de SGP-fractie hebben kennisgenomen van de op 10 oktober 2025 door de Europese Commissie gepubliceerde richtsnoeren bij artikel 28 van de Digital Services Act (DSA) inzake de bescherming van minderjarigen online. Deze leden onderschrijven het belang van een veilige digitale omgeving voor kinderen en jongeren, waarin zij

beschermd worden tegen schadelijke content, misbruik en verslavende ontwerpkeuzes.

Zij lezen dat de richtsnoeren een niet-uitputtende set maatregelen bevatten om de online veiligheid van minderjarigen te versterken, waaronder leeftijdsverificatie, verantwoord ontwerp en bescherming tegen misbruik. De leden van de SGP-fractie constateren echter dat de richtsnoeren geen eenduidige verplichting bevatten om de leeftijd van gebruikers daadwerkelijk vast te stellen, terwijl veel beschermingsmaatregelen hier in de praktijk wel van afhankelijk zijn. Deze leden vragen wat de kabinetsinzet hierop zal zijn.

Antwoord:

Zie het antwoord bij de vorige vraag.

De leden van de SGP-fractie vragen het kabinet of zij deelt dat effectieve bescherming van minderjarigen online in belangrijke mate afhankelijk is van het daadwerkelijk kunnen vaststellen of een gebruiker minderjarig is.

Antwoord:

Effectieve bescherming van minderjarigen online is afhankelijk van een aantal factoren. Een daarvan is het kunnen vaststellen of een gebruiker minderjarig is. Bescherming is ook een rol voor de ontwikkelaars van digitale diensten die normadressant zijn van verplichtingen uit onder meer de DSA. Ook ouders en verzorgers spelen een rol bij het beschermen van hun kinderen in de digitale wereld door bijvoorbeeld met hen daarover in gesprek te gaan. Het kabinet faciliteert dit door middel van een richtlijn en een publiekscampagne.

Deze leden lezen dat het kabinet in zijn appreciatie het belang en de urgentie van leeftijdsverificatie erkent, maar deze tegelijkertijd kwalificeert als een “zwaar middel dat grondrechten raakt en proportioneel moet worden ingezet”. Zij constateren dat deze kwalificatie suggereert dat leeftijdsverificatie per definitie privacy-onvriendelijk of disproportioneel zou zijn.

Antwoord:

Nee, deze constatering is niet juist. Het kabinet ziet leeftijdsverificatie als een van de instrumenten om kinderen online beter te beschermen.

De leden van de SGP-fractie constateren dat er Europese consensus is over bescherming van minderjarigen, maar dat nog onduidelijk is hoe leeftijdsverificatie moet worden vormgegeven. Deze leden vragen het kabinet wat hierin de door het kabinet beoogde rol van Europa wordt. Zij vragen het kabinet te voorkomen dat de terechte zorgen over impact van sociale media op jongeren misbruikt wordt om een Europese Digitale Identiteit uiteindelijk als onvermijdelijk te presenteren. De leden van de SGP-fractie vragen het kabinet te bevestigen dat dit ook haar inzet zal blijven en de Europese Digitale Identiteit niet te hanteren om leeftijdsverificatie toe te passen, maar te kijken naar de bestaande mogelijkheden zoals leeftijdsverificatie op appstore-niveau en daarbij aandacht te hebben voor de waarborgen ten aanzien van de privacy van gebruikers en de rechten van ouders. Is het kabinet bereid zich in te zetten voor regelgeving die ouders nadrukkelijk ondersteunt en faciliteert in het nemen van beslissingen passend bij hun gezinssituatie?

Antwoord:

Het kabinet onderschrijft het belang van bescherming van minderjarigen online en zet zich in Europa in voor een

zorgvuldige en proportionele invulling van leeftijdsverificatie.

In Europese wetgeving is vastgelegd dat het gebruik van een EDI-wallet vrijwillig is en dat de toegang tot publieke en private diensten niet mag worden beperkt of belemmerd voor mensen die die wallets niet gebruiken. Wanneer onlinediensten leeftijdverificatie vereisen, moeten zij dus ook andere geschikte leeftijdverificatie-instrumenten dan EDI-wallets toestaan.

Deze leden vragen het kabinet of zij kan toelichten welke grondrechten volgens haar concreet worden geraakt indien er concreet wordt gekozen om de bestaande systematiek dat bij het installeren van een telefoon om de leeftijd wordt gevraagd en dat dit enkel wordt uitgebreid door het verplicht stellen van verificatie hiervan.

Antwoord:

Dit is afhankelijk van de systematiek van leeftijdverificatie. Fundamentele rechten die kunnen worden geraakt zijn het recht op privacy omdat leeftijdverificatie om het delen of verwerken van persoonsgegevens kan vragen. Ook kan het recht op bescherming van persoonsgegevens aan de orde zijn in verband met bijvoorbeeld opslagduur en hergebruik van gegevens. Het recht op menselijke waardigheid speelt een rol bij een systematiek van leeftijdverificatie die is gebaseerd op gezichtsherkenning. Gebruik van leeftijdverificatie raakt het recht op toegang tot bepaalde diensten en maatschappelijke participatie. Dat is alleen aanvaardbaar als leeftijdverificatie proportioneel is.

Zij vragen het kabinet voorts waarom zij leeftijdverificatie als zwaar middel beschouwt, terwijl bij het instellen van een smartphone reeds standaard naar de leeftijd wordt gevraagd,

zonder dat dit als problematisch wordt aangemerkt vanuit grondrechtelijk perspectief.

Antwoord:

Bij het instellen van een smartphone kan het vragen naar leeftijd gemakkelijk worden omzeild. Kinderen doen dat omdat zij zich niet bewust zijn van de risico's en graag de telefoon in gebruik nemen. In dergelijke gevallen wordt het beoogde doel van het vragen naar leeftijd niet bereikt, nl. juist beschermen tegen die risico's. Dat is wel het geval bij een robuust systeem van leeftijdsverificatie. Daar zitten evenwel de eerder omschreven consequenties over fundamentele rechten aan. Het is daarom dat de inzet van leeftijdsverificatie bij elke situatie moet worden overwogen.

De leden van de SGP-fractie vragen of het kabinet bereid is te erkennen dat leeftijdsverificatie, mits zorgvuldig vormgegeven, juist kan bijdragen aan de bescherming van grondrechten van minderjarigen. Deze leden vragen tevens of zij bereid is zich in te zetten en samen met gelijkgestemde landen te pleiten voor een Europese digitale meerderjarigheidsleeftijd met centrale leeftijdsverificatie en ouderlijke goedkeuring als norm voor alle onlinediensten zoals games? Hoe waarborgt het kabinet dat alle apps en digitale diensten die door jongeren worden gebruikt, onder dezelfde regels voor leeftijdsverificatie en ouderlijke goedkeuring vallen, zodat er geen uitwijkmogelijkheid is naar minder veilige alternatieven?

Antwoord:

Leeftijdsverificatie kan, mits voldaan aan het proportionaliteitsvereiste, bijdragen aan bescherming van grondrechten. Het kabinet zal op basis van het TNO-rapport bekijken welke richting kan worden gekozen voor wat betreft leeftijdsverificatie.

Inmiddels is in het Coalitieakkoord opgenomen dat er een handhaafbare Europese minimumleeftijd van 15 jaar voor sociale media moet komen met privacyvriendelijke leeftijdsverificatie, zolang sociale media onvoldoende veilig zijn. Momenteel wordt onderzocht langs welke juridische weg dit is te bereiken.

De focus ligt daarnaast op het ondersteunen van ouders met richtlijnen en leeftijdsadviezen zoals dat inmiddels is gedaan met de richtlijn over gezond schermgebruik van het ministerie van VWS. Ouders kunnen dan zelf beslissen wat passend is voor hun kind. Ouderlijke toezichtsinstrumenten kunnen bijdragen aan online veiligheid, maar ontslaan tegelijkertijd platforms niet van hun verantwoordelijkheid zorg te dragen voor veilige digitale diensten. Ouders en verzorgers worden ook ondersteund door middel van de publiekscampagne “Blijf in beeld” en de website “Jouw kind online”. De Nederlandse inzet ziet op het verder reguleren van de verslavende ontwerptechnieken in digitale diensten en mogelijk het verbieden van de meest schadelijke technieken. Nederland en ook andere lidstaten volgen daarom nauwgezet de ontwikkeling in het voorstel van de Europese Commissie tot een DFA.

Zij vragen het kabinet of zij deelt dat het beperken van leeftijdsverificatie tot hoog-risico diensten uitwijkgedrag naar minder veilige alternatieven in de hand kan werken. De leden van de SGP-fractie vragen het kabinet ook of zij deelt dat leeftijdsverificatie en ouderlijke goedkeuring onderdeel moeten zijn van een bredere, integrale aanpak voor de bescherming van minderjarigen online.

Antwoord:

Het kabinet ziet het vooral als taak van ouders en verzorgers om samen met kinderen te bespreken van welke digitale diensten wel en niet gebruik mag worden gemaakt. Daarbij kunnen ouderlijke toezichtsinstrumenten helpen. Het kabinet

ondersteunt dit door middel van richtlijnen en leeftijdsadviezen en door middel van een publiekscampagne. Het kabinet zet verder in op het veiliger maken van digitale diensten door aanbieders daarvan te wijzen op hun verantwoordelijkheid, bijvoorbeeld door middel van het uitvoeren van kinderrechten impact assessments die, behalve de kansen, ook de risico's van een digitale dienst in kaart brengen. Daarnaast overweegt het ministerie van OCW de ontwikkeling van een Digitale Kijkwijzer mogelijk te maken, conform de al eerder genoemde motie Kathmann/Van der Werf, die gebruikers met behulp van icoontjes moet informeren over de risico's van die dienst.

Deze leden lezen dat technische mogelijkheden bestaan om leeftijdsverificatie en ouderlijke goedkeuring op besturingssysteemniveau te organiseren, waardoor leeftijd slechts eenmaal hoeft te worden geverifieerd. Zij zien hierin voordelen op het gebied van gebruiksgemak, gegevensbescherming en uitvoerbaarheid. De leden van de SGP-fractie vragen het kabinet of zij bereid is zich in te zetten voor een systeem waarin leeftijdsverificatie en ouderlijke goedkeuring centraal en op besturingssysteemniveau worden vormgegeven.

Antwoord:

Het kabinet is hier geen voorstander van en providers evenmin. Het verlegt immers de verantwoordelijkheid voor veilige digitale diensten van ontwikkelaars (als normadressanten) daarvan naar de providers. Ook ziet het kabinet een sterkere afhankelijkheid van een zeer beperkt aantal providers ontstaan. Zij is daar geen voorstander van.

Deze leden vragen het kabinet of zij bereid is expliciet te erkennen dat ouders primair verantwoordelijk zijn voor de opvoeding van hun kinderen, ook in de digitale omgeving, en dat regelgeving deze verantwoordelijkheid dient te ondersteunen in plaats van te bemoeilijken.

Antwoord:

Ja, ouders zijn primair verantwoordelijk voor de opvoeding van kinderen, ook als het gaat om de digitale omgeving. Zoals hierboven al omschreven ondersteunt het kabinet ouders en verzorgers op verschillende manieren hierbij en richt het kabinetsbeleid zich ook op verantwoordelijkheid van ontwikkelaars van digitale diensten.

Zij lezen dat het kabinet fragmentatie van regelgeving en extra regeldruk wil voorkomen en een gelijk speelveld binnen de Europese Unie nastreeft. Tegelijkertijd constateren de leden van de SGP-fractie dat het kabinet positief staat tegenover de komst van de Digital Fairness Act (DFA). Deze leden vragen het kabinet hoe zij voorkomt dat de DFA leidt tot overlap, onduidelijkheid en vertraging bij de implementatie van bestaande verplichtingen uit de DSA en de bijbehorende richtsnoeren. Zij vragen het kabinet of zij bereid is zich in Brussel actief in te zetten voor heldere, uniforme en Europees geharmoniseerde regels ter bescherming van minderjarigen online, zodat handhaving effectief en uitvoerbaar blijft.

Antwoord:

Zoals eerder is aangegeven in de antwoorden op de vragen van de D66 fractie, heeft het kabinet een non-paper verstuurd over de inzet op de DFA. Een belangrijk onderdeel van de inzet is het creëren van meer samenhang tussen het consumentenrecht enerzijds en regelgeving zoals de DSA anderzijds. Een voorbeeld hiervan is het overnemen van het verbod op dark patterns uit de DSA in het consumentenrecht. Hierdoor ontstaat een Europees geharmoniseerd kader en kan inconsistentie en verdere fragmentatie worden tegengegaan. Naast de inzet op duidelijke consistente wetgeving, staat de bescherming van consumenten en met name minderjarigen centraal. Zo signaleert het kabinet in de non-paper een aantal schadelijke online handelspraktijken waar het huidige kader van wet- en

regelgeving onvoldoende bescherming tegen biedt. Het kabinet roept daarom op om de DFA als gerichte maatregel te gebruiken om deze handelspraktijken aan te pakken, om zo lacunes in de huidige wetgeving te vullen.

De leden van de SGP-fractie lezen dat in verschillende lidstaten en onder maatschappelijke organisaties wordt gepleit voor een Europese digitale meerderjarigheidsleeftijd, met robuuste leeftijdsverificatie en ouderlijke goedkeuring als uitgangspunt. Deze leden vragen het kabinet of zij bereid is zich, samen met gelijkgestemde lidstaten, in te zetten voor een dergelijke Europese norm voor alle online diensten.

Antwoord:

Inmiddels is in het Coalitieakkoord opgenomen dat er een handhaafbare Europese minimumleeftijd van 15 jaar voor sociale media moet komen met privacyvriendelijke leeftijdsverificatie, zolang sociale media onvoldoende veilig zijn. Momenteel wordt onderzocht langs welke juridische weg dit is te bereiken.

De focus ligt daarnaast op het ondersteunen van ouders met richtlijnen en leeftijdsadviezen zoals dat inmiddels is gedaan met de richtlijn over gezond schermgebruik van het ministerie van VWS. Ouders kunnen dan zelf beslissen wat passend is voor hun kind. Ouderlijke toezichtsinstrumenten kunnen bijdragen aan online veiligheid, maar ontslaan tegelijkertijd platforms niet van hun verantwoordelijkheid zorg te dragen voor veilige digitale diensten. Ouders en verzorgers worden ook ondersteund door middel van de publiekscampagne “Blijf in beeld” en de website “Jouw kind online”. De Nederlandse inzet ziet op het verder reguleren van de verslavende ontwerpstechnieken in digitale diensten en mogelijk het verbieden van de meest schadelijke technieken. Nederland en ook andere lidstaten volgen daarom nauwgezet de ontwikkeling in het voorstel van de Europese Commissie tot een DFA.

kabinet zich op een bredere en voortdurend groeiende wetenschappelijke basis.

Ten aanzien van ondersteuning van ouders zet het kabinet in op het versterken van digitale opvoedvaardigheden. Via de publiekscampagne “Blijf in Beeld” worden ouders praktische handvatten geboden om hun kinderen te begeleiden bij het gebruik van digitale media, in samenwerking met o.a. Netwerk Mediawijsheid.

Vragen en opmerkingen van de leden van de CU-fractie

De leden van de ChristenUnie-fractie hebben met interesse kennisgenomen van het Fiche over de DSA richtsnoeren betreffende minderjarigen online. Deze leden hebben nog enkele vragen.

Zij zijn blij om te lezen dat het kabinet aan de Commissie heeft gevraagd om een verbod op loot boxes. Hoe heeft de Commissie op die vraag gereageerd? Ziet het kabinet ook bij andere lidstaten draagvlak voor een dergelijk verbod?

Antwoord:

In aanloop naar het wetgevend voorstel voor de DFA (verwacht in het vierde kwartaal van 2026) onderzoekt de Commissie verschillende beleidsopties voor schadelijke online handelspraktijken, waaronder die in games. Of de Commissie een generiek verbod op loot boxes zal voorstellen is op dit moment niet duidelijk. Ook de positie van de verschillende lidstaten op de mogelijke onderdelen uit de DFA is nog niet bekend. In algemene zin lijkt er een zekere mate van steun te zijn voor het reguleren van handelspraktijken in games, zoals het gebruik van digitale munten en loot boxes, met name met het doel om kinderen en jongeren beter te beschermen.

De leden van de ChristenUnie-fractie zijn verbaasd over de terughoudendheid van het kabinet als het gaat over leeftijdsverificatie, mede gezien de expliciete wens van de Kamer om leeftijdsverificatie in te voeren. Zo wijzen deze leden op de motie van de leden Ceder en Six Dijkstra over het wettelijk borgen van privacyvriendelijke en betrouwbare leeftijdsverificatie voor online gokken en pornografische content (Kamerstuk 36531, nr. 20) en de motie van de leden Ceder en Six Dijkstra over een interdepartementale taskforce leeftijdsverificatie oprichten (Kamerstuk 21501-33, nr. 1154). Zij vragen hoe het kabinetsstandpunt zich verhoudt tot deze aangenomen moties. Ook vragen de leden van de CU-fractie hoe het standpunt zich verhoudt tot de Jutlandverklaring, die Nederland heeft ondertekend. Erkent het kabinet dat deze verklaring stelt dat er een noodzaak is voor leeftijdsverificatie voor sociale media? Deze leden vragen ook om een stand van zaken te geven van de opvolging van bovenstaande moties. Hierbij vragen zij in het bijzonder om een stand van zaken van de oprichting van de taskforce leeftijdsverificatie en wanneer zij het tijdpad voor (nationale) wettelijke verankering van leeftijdsverificatie kunnen verwachten. Ook vragen de leden van de CU-fractie op welke gebieden het kabinet voornemens is leeftijdsverificatie in te voeren.

Antwoord:

Het gebruik van leeftijdsverificatie kan, in combinatie met andere maatregelen, kinderen online beter beschermen. Daarom is het belangrijk om leeftijdsverificatie op een robuuste en betrouwbare manier mogelijk te maken, waarbij fundamentele rechten zoals privacy, gegevensbescherming en non-discriminatie worden gewaarborgd. Daarnaast moeten verschillende methoden voor leeftijdsverificatie beschikbaar zijn om inclusiviteit te bevorderen en te voorkomen dat gebruikers gedwongen worden een specifieke methode te gebruiken.

Ook de Jutlandverklaring ziet leeftijdsverificatie als één van de mogelijke instrumenten.

Deze leden vragen tot slot aan het kabinet of hij ook het risico ziet dat, als leeftijdsverificatie beperkt wordt ingevoerd, minderjarigen hun toevlucht zoeken tot andere apps, die wellicht nog minder veilig zijn. In Australië leek dit namelijk te gebeuren toen het socialmediaverbod eraan kwam. Hoe wil het kabinet leeftijdsverificatie op zo'n manier invoeren, dat dergelijke risico's worden ondervangen?

Antwoord:

Het kabinet ziet dit waterbedeffect ook als een mogelijk risico. Hier is niet een éénduidige oplossing voor. Onderzocht moet worden tot welke digitale diensten kinderen hun toevlucht zoeken. Mogelijk leidt dat bij een bepaalde dienst ook tot het invoeren van leeftijdsverificatie. Verder spelen ook ouders en verzorgers een belangrijke rol. Zij moeten met hun kinderen in gesprek over het gebruik van digitale diensten, ook in het geval kinderen op zoek gaan alternatieven. Het kabinet richt zich structureel tot ontwikkelaars van digitale diensten door hen erop te wijzen, onder meer door het uitvoeren van kinderrechten impact assessments, wat hun verantwoordelijkheid is op het terrein van veiligheid en bescherming van kinderen. Het kabinet zet daarnaast in op ondersteuning van Europese wetgeving zoals de DFA. Daarnaast zet het kabinet in op een Europese aanpak bij het instellen van een minimumleeftijd voor sociale media, zolang die onvoldoende veilig zijn. Het is hierbij van belang om goed te onderzoeken voor welk type sociale mediadiensten een leeftijds grens moet gelden, zodat het waterbedeffect zoveel mogelijk kan worden voorkomen. Het uitgangspunt hierbij is dat kinderen geen toegang moeten hebben tot onveilige sociale media.