

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

31

Vragen van het lid **Ceder** (ChristenUnie) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (Koninkrijksrelaties en Digitalisering) over *het bericht «Dure reclamecampagne blijkt flop: nauwelijks «ouderlijk toezicht» op Instagram»* (ingezonden 19 juli 2024).

Antwoord van Staatssecretaris **Szabó** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Staatssecretaris van Justitie en Veiligheid (ontvangen 20 september 2024).

Vraag 1

Bent u bekend met het artikel «Dure reclamefilmpje blijkt flop: nauwelijks «ouderlijk toezicht» op Instagram»?¹

Antwoord 1

Ja, ik ben hiermee bekend.

Vraag 2

Kunt u aangeven wat de wettelijke verplichtingen zijn ten aanzien van social mediagebruik onder 16 jaar? In hoeverre voldoen social mediabedrijven, en specifiek META, hieraan? Acht u deze aanpak voldoende?

Antwoord 2

Rechtmatige verwerking van persoonsgegevens bij online diensten, zoals Meta, van kinderen die de leeftijd van 16 jaar nog niet hebben bereikt mogen volgens de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) alleen met toestemming van de ouders of de wettelijke vertegenwoordiger worden verwerkt. Dit betekent dat een kind jonger dan zestien jaar enkel een account mag aanmaken als hiervoor door de ouder of wettelijke vertegenwoordiger toestemming is gegeven. Bedrijven die online persoonsgegevens van kinderen verwerken zijn volgens de AVG verplicht een redelijke inspanning te leveren om te controleren of er daadwerkelijk toestemming is gegeven. Naast deze wettelijke verplichting kiezen diverse sociale mediaplatforms, waaronder Instagram, ervoor om kinderen jonger dan 13 jaar in elk geval niet toe te laten tot hun platform. Deze regel volgt echter niet uit een wettelijke vereiste. Uit onderzoek van Ofcom, de Britse mediatoezichthouder,

¹ BNR, 18 juli 2024 (www.bnr.nl/nieuws/tech-innovatie/10552636/dure-reclamecampagne-blijkt-flop-nauwelijks-ouderlijk-toezicht-op-instagram).

blijkt dat 60% van de kinderen tussen de 8 en 12 jaar een sociale media-account hebben. Hoewel dit onderzoek specifiek ziet op Britse kinderen is het aannemelijk dat deze aantallen in Nederland vergelijkbaar zijn. Dit zijn zorgelijke aantallen en het is belangrijk dat dit wordt teruggebracht en dat sociale media platforms aan de wetgeving (ouderlijke toestemming onder de 16 jaar) en aan hun eigen beleid (veelal geen account onder de dertien jaar) voldoen.

Het is aan de Europese toezichthouders (in Nederland is dit de Autoriteit Persoonsgegevens (AP)) dan wel aan de toezichthoudende autoriteit van de hoofdvestiging in een andere lidstaat, om als onafhankelijke toezichthouder toe te zien op de naleving van de AVG en waar nodig handhavend op te treden voor zover de toezichthouder daar de competentie toe heeft.

De Digitaal dienstenverordening (DSA), die in februari van dit jaar volledig van toepassing is geworden, verplicht bovendien onlineplatforms die toegankelijk zijn voor minderjarigen om passende en evenredige maatregelen te nemen om een hoog niveau van privacy, veiligheid en bescherming van minderjarigen binnen hun dienst te waarborgen (artikel 28 DSA, eerste lid). De Autoriteit Consument & markt (ACM) en de AP zijn de beoogde toezichthouders op de naleving van een groot deel van de DSA waarbij de ACM digitaal diensten coördinator is. Beide toezichthouders zullen worden aangewezen in de uitvoeringswet DSA (uDSA). De uDSA is echter nog niet officieel aangenomen. Vooralsnog is de ACM aangewezen als voorlopige bevoegde autoriteit.

Zeer grote online platforms moeten daarnaast op grond van de DSA ook de systeemrisico's voor de bescherming van minderjarigen in kaart brengen en mitigeren. Het gaat hierbij onder andere om de werkelijke of voorzienbare negatieve effecten op de bescherming van minderjarigen. Een ander relevant systeemrisico in dit kader zijn ernstige negatieve gevolgen voor het lichamelijke en geestelijke welzijn van personen. Zeer grote online platforms moeten dus nadrukkelijk rekening houden met de negatieve effecten die hun algoritmes kunnen hebben op kinderen en zij moeten deze systemen zo nodig aanpassen. Zij moeten dit bovendien laten onderzoeken door externe auditors. De Europese Commissie (EC) houdt toezicht op de naleving van deze verplichtingen voor de zeer grote online zoekmachines en platforms, waar Instagram en Facebook onder vallen. Ook het Europees Centrum voor Algoritmische Transparantie is mede hiertoe opgezet.

Er zijn dus verschillende wettelijke verplichtingen die beogen kinderen online te beschermen. De DSA is een belangrijke stap voor de bescherming van kinderen in de online wereld. Deze verordening is echter recentelijk pas van toepassing geworden. De voor de DSA noodzakelijk nationale uDSA is bovendien vertraagd waardoor ook de start van het toezicht op de DSA nog niet volledig operationeel is. Het kabinet zal de uitwerking van de DSA in de praktijk monitoren. De verordening voorziet bovendien in een tweetal evaluaties; per 17 november 2025 en 17 november 2027. Het kabinet wil de uitkomsten van deze evaluaties afwachten voordat er een uitspraak kan worden gedaan of het voorgenomen stelsel met regulering via de DSA voldoende handvatten biedt.

De EC werkt daarnaast aan de uitwerking van richtsnoeren onder de DSA over de bescherming van minderjarigen online. Deze richtsnoeren zullen, zodra ze zijn aangenomen, advies geven over hoe onlineplatforms een hoog niveau van privacy, veiligheid en beveiliging voor minderjarigen online moeten implementeren. De EC heeft aangegeven hierbij in te willen zetten op een risico gebaseerde aanpak, gebaseerd op kinderrechten impact assessments.

Naast deze eerdergenoemde meer specifieke verplichtingen om kinderen te beschermen, moeten bedrijven zich richting alle consumenten, waaronder kinderen, houden aan het consumentenrecht. Zo mogen bedrijven consumenten niet misleiden (een vorm van een oneerlijke handelspraktijk). Wat een oneerlijke handelspraktijk is kan per situatie anders zijn. Daarbij wordt o.a. rekening gehouden met de kwetsbaarheid van consumenten. Sommige groepen, zoals kinderen, zijn extra kwetsbaar en vaak gevoeliger voor verleidingstechnieken.

De ACM houdt in Nederland toezicht op de naleving van het consumentenrecht door bedrijven en heeft in haar eerder gepubliceerde Leidraad

Bescherming online consument, invulling gegeven aan de norm voor online misleiding. Daarbij wordt ook ingegaan op praktijken gericht op kinderen.²

Vraag 3

Welke stappen heeft de overheid tot nu toe gezet om niet naleving van Tech bedrijven te handhaven? Zijn er inmiddels sancties uitgedeeld, zo ja welke? Kunt u deze uitsplitsen per bedrijf?

Antwoord 3

De toezichthouders hebben verschillende middelen en instrumenten tot hun beschikking om te handhaven. Zo is de EC onder de DSA eind april een nalevingszaak gestart naar TikTok, en medio mei naar Instagram en Facebook. Deze zaak ziet onder andere op de verslavende werking van deze diensten en het gebruik van informatiefuiken.³ Wanneer de EC na afronden van dit onderzoek vaststelt dat er sprake is van een inbreuk kan zij een boete opleggen van maximaal 6% van de totale wereldwijde jaaromzet. Het is aan de verschillende toezichthouders om toezicht te houden op de naleving van de eerdergenoemde regelgeving daar waar die competentie niet bij de EC ligt.

Eerder heeft de Autoriteit Persoonsgegevens (AP) een boete opgelegd aan TikTok⁴. De AP was destijds de bevoegde toezichthouder, voordat TikTok haar Europese hoofdvestiging naar Ierland verhuisde. Daarna heeft ook de Ierse Data Protection Commission (DPC) op 1 september 2023 aan TikTok een boete opgelegd van 345 miljoen Euro wegens meerdere schendingen van de AVG.⁵ Omdat de hoofdvestiging van TikTok in de EU in Ierland is gevestigd, was de DPC de competente toezichthouder. Dit onderzoek is in nauwe samenwerking met de AP uitgevoerd.

Naast handhaving zet de overheid ook in op het de ontwikkeling van instrumenten om ontwikkelaars van onlinediensten te ondersteunen bij het creëren van leeftijdsgeschiede ontwerpen, waarbij de risico's op schending van kinderrechten zoveel mogelijk worden beperkt. Zo heeft het vorige kabinet een kinderrechten impact assessment (KIA) ontwikkeld en een geactualiseerde Code voor kinderrechten opgesteld. Deze KIA's zullen jaarlijks worden uitgevoerd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, op sociale mediaplatformen die veel door kinderen worden gebruikt.⁶ De uitvoering van de eerste kinderrechten impact assessments is recent gestart. De eerste resultaten worden begin 2025 verwacht. Deze resultaten zullen na afronding met uw Kamer worden gedeeld.

Vraag 4

Welke sanctiemiddelen staan er nog steeds open die nog niet ingezet zijn en gaat u deze inzetten om naleving van de wet af te dwingen?

Antwoord 4

Zoals in het antwoord op vraag 3 is toegelicht, is er door de EC een onderzoek gestart onder de DSA en beoordeelt de AP, of de toezichthoudende autoriteit van de hoofdvestiging in een andere lidstaat, per geval en uit eigen beweging of er aan de AVG is voldaan en of er al dan niet handhavings- en onderzoeksbevoegdheden ingezet dienen te worden. Er bestaat hierin geen rol voor het ministerie, enkel de onafhankelijke toezichthouder heeft handhavings- en onderzoeksbevoegdheden. Deze handhavings- en onderzoeksbevoegdheden kunnen bestaan uit het doen van onderzoek naar de naleving van wetten die zien op het gegevensbeschermingsrecht, waarbij ingezet kan worden op het inzien van gegevensverwerkingen, bijvoorbeeld in de vorm van het inzien van het register of logging data wel het doen van audits. Daarnaast worden grote partijen die hun diensten ook aanbieden aan kinderen door de AP en haar Europese collega's bevestigd op de risico's voor

² Leidraad Bescherming online consument | ACM.nl).

³ Commissie leidt procedure in tegen TikTok in het kader van de wet inzake digitale diensten (europa.eu).

⁴ <https://www.autoriteitpersoonsgegevens.nl/documenten/boete-tiktok-recht-op-informatie>

⁵ <https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok>

⁶ Verzamelbrief Digitalisering juni 2024, Informatie- en communicatietechnologie (ICT) | Tweede Kamer der Staten-Generaal.

kinderen en hoe deze partijen risico's mitigeren om aan de wetgeving te voldoen. Tot slot heeft de AP dit jaar kritische vragen gesteld aan een groot techbedrijf dat een chatbot gericht op kinderen op de markt bracht.⁷ Ook heeft de AP de mogelijkheid om gegevensverwerkingen stop te zetten en kunnen dwangsommen of boetes worden opgelegd. Het is aan de toezichthouder of zij tot handhaving overgaat. Vanuit de DSA kan de AP optreden als het gaat om het verbod op profileren met gebruik van gegevens van kinderen (art. 28, tweede lid). De overheid, anders dan de eerdergenoemde toezichthouders, zoals genoemd in vraag 3, kan geen sanctiemiddelen inzetten. Zodra de ACM volledig bevoegd is om toezicht te houden op de DSA, kan zij handhavend optreden tegen online platforms bij overtreding van de open norm dat zij maatregelen moeten nemen om een «hoog niveau van privacy, veiligheid en bescherming van minderjarigen binnen hun dienst te waarborgen» (art. 28, eerste lid). Denk hierbij onder andere aan het opleggen van een boete of een last om een overtreding te staken. Deze handhavingsbevoegdheid beperkt zich tot aanbieders van online platforms met een hoofdvestiging of wettelijk vertegenwoordiger in Nederland. Als het online platform in een andere lidstaat gevestigd is, kan de ACM o.a. meldingen over overtredingen naar de digitale diensten coördinator van de desbetreffende lidstaat sturen of hen verzoeken handhavend op te treden.

Vraag 5

Bent u bekend met het toenemende bewijs dat social media een negatief effect heeft op jongeren? Wat vindt u ervan dat sociale mediabedrijven tot op heden nog niet aan wetgeving voldoen?

Antwoord 5

Het kabinet ziet dat er steeds meer onderzoeken uitwijzen dat problematisch gebruik van sociale media ten koste gaat van de mentale en cognitieve ontwikkeling van jongeren. Dit is zorgelijk. Om de negatieve effecten van onlinediensten voor minderjarigen te beperken, wordt er ook in nieuwere wetgeving steeds meer rekening gehouden met de kwetsbare positie van kinderen, juist ook bij het gebruik van onlinediensten. Een voorbeeld daarvan is de in het antwoord op vraag 2 genoemde DSA. Dit ziet het kabinet als een goede stap in de bescherming van kinderen tegen de schadelijke effecten van bijv. sociale mediadiensten te beschermen.

Het is uiteindelijk aan de onafhankelijke toezichthouders om vast te stellen of sociale mediabedrijven aan de in de wet- en regeling gestelde wettelijke eisen voldoen en in een voorliggend geval onrechtmatig handelen. Dat is niet aan het kabinet.

Vraag 6

Is het volgens u wel haalbaar om ouderlijk toezicht onder 16 jaar te handhaven? Zo nee, hoe kijkt u naar de mogelijkheid om deze uitzondering niet meer mogelijk te maken en een social media-account pas vanaf 16 toe te staan?

Antwoord 6

Het kabinet erkent dat het in de praktijk moeilijk kan zijn om te bepalen wanneer ouderlijke toestemming vereist is, omdat er sprake is van een gebruiker, die jonger is dan zestien jaar. Dit betekent echter niet dat sociale media-gebruik tot 16 jaar moet worden verboden. Uit wetenschappelijk onderzoek⁸ blijkt dat sociale media voor jongeren ook positieve effecten kunnen hebben. Zo kan het kinderen helpen op een veilige manier te oefenen met sociale relaties en is er op sociale media een schat aan informatie te vinden over verschillende onderwerpen. Het is echter wel belangrijk dat sociale mediabedrijven ervoor zorgen dat de online omgeving veilig is voor kinderen en dat zij niet worden blootgesteld aan onwenselijke praktijken, zoals schadelijke content, cyberpesten of verslavende elementen. Daarnaast is het van belang dat de toestemming van ouders wordt gevraagd in alle gevallen waarin dat wettelijk verplicht is. Hiervoor is het belangrijk dat online

⁷ <https://autoriteitpersoonsgegevens.nl/actueel/ap-eist-duidelijkheid-techbedrijf-over-ai-gericht-op-kinderen>

⁸ Koning & Vossen (2023) Handreiking beleid digitale mediagebruik door jongeren. Vrije Universiteit Amsterdam en Universiteit Utrecht.

platforms op een adequate manier de leeftijd van kinderen vaststellen, zonder hiermee inbreuk te maken op de privacy van gebruikers. Dit risico bestaat bijvoorbeeld bij het gebruik van biometrie of het uploaden van een kopie van het identiteitsbewijs om leeftijd vast te stellen. Om kinderen beter te beschermen, heeft de voormalige Staatssecretaris Koninkrijksrelaties en Digitalisering een raamwerk leeftijdsverificatie laten ontwikkelen, dat ontwikkelaars van onlineproducten en diensten voor kinderen kan helpen om te komen tot een adequate vorm van leeftijdsverificatie voor hun onlineproduct of dienst.

Vraag 7

Hoe staat het met de ontwikkeling van het wetsvoorstel naar aanleiding van de aangenomen motie van de leden Ceder en Six Dijkstra voor een wetsvoorstel voor het borgen van wettelijke leeftijdsverificatie? Wanneer worden de contouren hiervan naar de Kamer gezonden?⁹

Antwoord 7

Verschillende betrokken ministeries zijn momenteel aan het uitwerken hoe wettelijke borging van adequate leeftijdsverificatie in de verschillende situaties vorm zou kunnen krijgen. Zo is het Ministerie van VWS al enige tijd bezig met het uitwerken van de eisen waar een betrouwbaarder leeftijdsverificatiesysteem bij de online verkoop van alcohol aan moet voldoen. De Staatssecretaris Jeugd, Preventie en Sport bereidt momenteel een wijziging van het Alcoholbesluit voor ten behoeve van het invoeren van een betrouwbaarder leeftijdsverificatiesysteem bij de online verkoop. Het streven is om begin 2025 de internetconsultatie te starten waarna het ontwerpbesluit in het kader van de voorhangprocedure wordt aangeboden aan beide Kamers. Daarnaast heeft de Minister van Financiën de Kamer op 19 juni jl. in zijn antwoorden op Kamervragen van de leden Mohandis en Ceder over de noodzaak tot verplichte leeftijdscontrole bij *Buy Now Pay Later (BNPL)*-diensten geïnformeerd dat hij momenteel samen met de Staatssecretaris Participatie en Integratie en de Staatssecretaris Rechtsbescherming uitwerkt hoe leeftijdsverificatie door BNPL-aanbieders bij alle klanten wettelijk kan worden afgedwongen.¹⁰ In de tussentijd heeft ook het interdepartementale onderzoek problematische schulden aanbevolen een leeftijdsverificatie verplicht te stellen voor BNPL-aanbieders.¹¹ De verkenning van mogelijke beleidsopties zal na de zomer met de Kamer worden gedeeld. Voor sociale mediadiensten zijn er geen voornemens om online leeftijdsverificatie verder wettelijk te borgen. Online leeftijdsverificatie wordt in de DSA genoemd als mogelijke maatregel die online diensten kunnen nemen ten behoeve van de bescherming van de rechten van het kind. Verdere uitwerking hiervan zal, gezien de maximaal harmoniserende werking van de DSA, op Europees niveau moeten gebeuren. Hierbij is het wel belangrijk dat er bij Europese standaardisatie de afweging van belangen als privacy, non-discriminatie, inclusiviteit, veiligheid en betrouwbaarheid in acht worden genomen en dat dit niet leidt tot het verwerkingen van aanvullende persoonsgegevens teneinde de meerderjarigheid van afnemers van een dienst vast te stellen. Ik blijf dit internationaal onder de aandacht brengen.

Vraag 8

In hoeverre acht u zero proof knowledge identity proof technologie als betrouwbaar en middel om verplicht te stellen, dan wel via de wet dan wel via lagere regelgeving?

Antwoord 8

De toepassing van zero knowledge proof technologie voor online leeftijdsverificatie is nog niet op grote schaal onderzocht en het is daarom nog niet met voldoende zekerheid te zeggen dat deze toepassing voldoende betrouwbaar zal zijn voor online leeftijdsverificatie. Het zal daarbij ook per situatie kunnen verschillen welke betrouwbaarheid wenselijk is. Daarnaast moet worden opgemerkt dat het over het algemeen wenselijk is om wetgeving techniek-

⁹ Kamerstuk 26 643, nr. 1163.

¹⁰ Aanhangsel Handelingen II 2023/24, nr. 2019.

¹¹ Kamerstukken II 2023/2024 2024D27539

onafhankelijk op te stellen, aangezien technologische ontwikkelingen elkaar in rap tempo opvolgen. Het is dan ook ongewenst om specifieke technologieën in wetgeving vast te leggen. In lagere wet- en regelgeving kunnen wel vereisten worden vastgelegd, maar het is niet aan de wetgever om te bepalen welke specifieke technologie hierbij gebruikt moet worden.