Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1041

BRIEF VAN DE MINISTER VOOR RECHTSBESCHERMING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 juni 2023

Aandacht voor de omgang met sociale waarden en grondrechten bij de opkomst van nieuwe technologieën is een voorwaarde voor het succesvol benutten van de rijke kansen die zij bieden. Het kabinet anticipeert daarom op deze ontwikkelingen en zet er beleidsmatig op in dat onze grondrechten en waarden met de opkomst van nieuwe technologieën steeds goed zijn beschermd.[1] Daarom hebben wij het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) gevraagd om een tweetal onderzoeken te laten uitvoeren naar nieuwe technologieën en de vraag of het huidige juridische kader naar aanleiding van de opkomst van die technologieën dient te worden aangepast. Uit beide onderzoeken rijst het zorgwekkende beeld op dat deze nieuwe technologieën onder andere een ernstig risico vormen voor jonge vrouwen die tegen hun wil kunnen worden afgebeeld in deepnudes (pornografische deepfakes) die op het internet worden verspreid, of slachtoffer kunnen worden van online aanranding en verkrachting in Virtual Reality (VR). In deze brief bespreken wij deze, en andere, belangrijke bevindingen uit beide onderzoeken. Daarbij gaan wij ook in op de moties van en toezeggingen aan uw Kamer en de Eerste Kamer. In het bijzonder bespreken wij in deze brief de gewijzigde motie van het lid Rajkowski c.s. van uw Kamer over het tegengaan van bepaalde deepfaketechnologie.[2] Een uitvoerige toelichting op de reguleringsopties uit beide onderzoeken is toegevoegd als bijlage.

Deepfakes

Zogenoemde «deepfake technologie» maakt het mogelijk om niet of nauwelijks van echt te onderscheiden beeld, geluid of ander materiaal te genereren. Deze technologie ontwikkelt zich met rasse schreden en wordt voor steeds meer mensen toegankelijk, en blijkt zich in de praktijk te lenen voor zeer ongewenste toepassingen zoals desinformatie, maar ook het maken van deepnudes tegen de wil van degenen die daarin worden

[1] Kamerstuk 34 926, nr. 11; Kamerstuk 26 643, nr. 842 (herdruk).
[2] Kamerstuk 36 200 VII, 118.

kst-26643-1041
ISSN 0921 - 7371
's-Gravenhage 2023

afgebeeld. Uw Kamer heeft hiervoor terecht bijzondere aandacht gevraagd, en wij delen de zorgen over dit fenomeen.[3] Daarom heeft het kabinet, mede naar aanleiding van de motie van de voormalige Kamerleden Buitenweg en Van Toorenburg[4] en in het kader van de Agenda horizontale privacy,[5] opdracht gegeven tot het voorliggende onderzoek naar deepfakes. De centrale vraag is daarin of het recht goed beschermt tegen uitingsvormen van deze technologie. Het onderzoek toetst daarbij onder andere aan de Algemene verordening gegevensbescherming (AVG) of diens uitvoeringswet (UAVG), het burgerlijk (proces)recht en het straf(proces)recht. Wij waarderen in het bijzonder de zeer doorwrochte behandeling van het juridische kader dat beschermt tegen deepnudes. Naar de juridische bescherming tegen desinformatie is in het WODC-onderzoek minder aandacht uitgegaan, nu het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) daarnaar in 2019 onderzoek heeft gedaan en uw Kamer daarover heeft geïnformeerd.[6]

Hieronder gaan wij in op de belangrijkste conclusies en aanbevelingen uit het onderzoek. Tevens behandelen wij de gewijzigde motie van het lid Rajkowski c.s. van uw Kamer over het tegengaan van bepaalde deepfaketechnologie, en de toezegging aan uw Kamer tijdens het begrotingsdebat Justitie en Veiligheid om ook het Amerikaanse model te betrekken in het onderzoek.[7]

Het recht is goed toegerust

De eerste conclusie van het onderzoek luidt dat onwenselijk gebruik van deepfakes of deepfaketechnologieën via het huidige recht in algemene zin goed is te adresseren. Wij zien daarbij dat het gebruik van deepfaketechnologie als zodanig geen inbreuk maakt op de rechten van burgers; het gaat er immers om hoe deze technologie wordt gebruikt. Het kabinet waardeert in dit kader ook het genuanceerde beeld dat de onderzoekers schetsen, waarbij ook aandacht is voor de vele positieve toepassingen van deepfaketechnologie. Gedacht kan worden aan toepassingen in het onderwijs (bijvoorbeeld om historische personages tot leven te wekken); in de gezondheidszorg (om synthetische *Magnetic resonance imaging* (MRI) van hersenen met tumoren te maken, of om vanuit die beelden algoritmen te trainen om vroege vormen van kanker of hersenziekten zoals Alzheimer op te sporen), bij kunstuitingen; onschuldige en grappige filmpjes in de huiselijke sfeer; en (politieke) satire.

Waar deepfaketechnologie wordt misbruikt op een manier die de gerechtvaardigde belangen van individuen (zoals hun privacy) schaadt, biedt het recht middelen om daartegen op te treden. Dit geldt nadrukkelijk ook voor deepnudes, die vaak tegen de wil van degenen die erin worden afgebeeld, worden gemaakt en verspreid op het internet. Zo stelt artikel 139h Wetboek van Strafrecht (Sr) het zonder toestemming van de afgebeelde persoon openbaar maken van seksueel beeldmateriaal, waaronder ook deepfake beeldmateriaal valt, strafbaar. Het kabinet is van mening dat ook het enkele vervaardigen en voorhanden hebben van dat (deepfake)materiaal (zonder openbaring ervan) onacceptabel is, en

[3] Kamerstuk 35 570 VI, nr. 37; Kamerstuk 36 200 VII, nr. 118; Handelingen II 2022/23, nr. 24, item 11.
[4] Kamerstuk 35 570 VI, nr. 37.
[5] Kamerstuk 34 926, nr. 11.
[6] Naar het juridische kader voor de verspreiding van desinformatie heeft de Minister van Binnenlandse Zaken en Koninkrijksrelatie reeds eerder onderzoek laten doen. Zie: J. van Hoboken e.a., *Het juridisch kader voor de verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties,* Amsterdam: IViR 2019. Voor de *beleidsreactie* n.a.v. dat onderzoek, zie Kamerstukken 30 821 en 35 165, nr. 118.
[7] Kamerstuk 36 200 VII, 118; Handelingen II 2022/23, nr. 24, item 11.

strafbaar op grond van 139h (zie onze appreciatie van reguleringsoptie 1 in bijlage 1). Ook ander strafwaardig gedrag, zoals oplichting met behulp van deepfakes, kan volgens het onderzoek middels het huidige strafrecht goed worden geadresseerd. Het Openbaar Ministerie (OM) beziet momenteel de mogelijkheden voor de inzet van artikel 139h Sr in concrete gevallen waarbij sprake is van deepnude materiaal. De ontwikkelingen hieromtrent blijven wij, in gesprek met het OM, nauwlettend volgen. Over de ontwikkelingen kunnen we uw Kamer informeren in de voortgangsbrief over de aanpak van seksuele misdrijven die in december naar uw Kamer wordt gestuurd.

Het onderzoek concludeert verder dat ook buiten het strafrecht, het recht goed is toegerust om onwenselijke deepfakes tegen te gaan. Dit geldt bijvoorbeeld als een deepfake inbreuk maakt op de privacy van een erin afgebeelde persoon. Zo verbiedt de AVG het maken en verspreiden – buiten de huiselijke sfeer[8] – van deepfakes waarin persoonsgegevens zijn verwerkt zonder een verwerkingsgrondslag. In de praktijk is daardoor een deepfake die zonder toestemming is gemaakt, zeker als daarin gevoelige (bijvoorbeeld seksuele) content is te zien, strijdig met de AVG. Ook gelden de kaders van het civiele recht, bijvoorbeeld in het geval van een onrechtmatige daad (artikel 6:162 Burgerlijk Wetboek (BW)) of een schending van het portretrecht zoals bedoeld in het auteursrecht. Ook is het procesrecht toegerust op de mogelijkheid dat deepfakes worden gebruikt als nepbewijs (zie de appreciatie van reguleringsoptie 9 in bijlage 1).

De Minister van Justitie en Veiligheid heeft in het begrotingsdebat van Justitie en Veiligheid 2023 aan uw Kamer toegezegd om ook het Amerikaanse model in de beleidsreactie te betrekken.[9] Met betrekking tot het strafrecht kan dan worden gedacht aan de aanpak in de Amerikaanse staat Virginia zoals die ook in het WODC-onderzoek is omschreven. Daar is een wet aangenomen die het zonder toestemming maken en verspreiden van seksueel beeldmateriaal strafbaar stelt, en waarin, vrij vertaald, expliciet is opgenomen dat het niet uitmaakt hoe dit beeldmateriaal tot stand is gekomen.[10] Wij zijn van mening dat een aanpassing van de huidige wetgeving naar dit Amerikaanse model niet noodzakelijk is om deepfakes onder het bereik van de wet te brengen. Zoals het onderzoek bevestigt, is het bestaande juridische kader in Nederland zodanig technologieneutraal, dat het problematisch gebruik van deepfakes in horizontale verhoudingen daarmee reeds goed kan worden geadresseerd.

Handhaving en online content

De tweede conclusie van het onderzoek luidt dat de handhaving van de bestaande rechtsregels omvangrijk en complex is, ook omdat handhaving pas aan de orde komt als het kwaad al is geschied. Het kabinet merkt op dat dit vraagstuk omtrent handhaving, zoals ook in het onderzoek wordt geconstateerd, in meer algemene zin speelt bij het bestrijden van onrechtmatige en strafbare content online. Wij herkennen het beeld dat slachtoffers hier in de praktijk lastig mee uit de voeten kunnen en dat dit grote impact kan hebben. Naast de bestaande mogelijkheden om het recht online te handhaven, wordt daarom goed gekeken hoe slachtoffers nog betere handvatten kunnen worden geboden om deze laakbare content online te verwijderen. Zo onderzoekt het OM op dit moment de

[8] Zie voor een bespreking van het voorstel om van de huishoudelijke exceptie af te schaffen, reguleringsoptie 5.
[9] Handelingen II 2022/23, nr. 24, items 6 en 11.
[10] Deepfakes: De juridische uitdagingen van een synthetische samenleving, p. 243 en 247–248 (WODC-onderzoek), bijlage bij Kamerstuk 26 643, nr. 815.

mogelijkheden voor de inzet van artikel 139h Sr in concrete gevallen waarin sprake is van deepnude-materiaal. Ook zetten wij in het kader van zelfregulering in op de snelle verwijdering van illegale content door de internetsector, en werkt de Nederlandse overheid al jaren samen met de internetsector aan de bestrijding van illegale content online. In 2008 is er een Notice-and-Takedown (NTD) gedragscode overeengekomen tussen overheden, internetaanbieders, hostingbedrijven en andere tussenpersonen. Een slachtoffer kan deze content rapporteren bij de internettussenpersoon zoals een platform met een verzoek tot verwijdering. De snelheid hiervan hangt af van de aanbieder en het type content; zo is afgesproken dat in geval van meldingen van online seksueel kindermisbruik dit materiaal binnen 24 uur verwijderd moet worden.

Aanvullend faciliteert de overheid een aantal meldpunten om illegale content, met inbegrip van deepfakes en strafbare content, onder de aandacht te brengen van dienstverleners binnen de internetsector. Content die dienstverleners als «illegaal» betitelen wordt in dat kader in de meeste gevallen ook daadwerkelijk ontoegankelijk gemaakt. De komende jaren wordt ingezet op het verder optimaliseren van de opvolging van meldingen die door deze meldpunten ontvangen zijn, waardoor er nog sneller kan worden geacteerd om te voorkomen dat deze content zich verder verspreidt.

Het kabinet is daarnaast voornemens een laagdrempelige voorziening in het leven te roepen, waar evident onrechtmatige content gemeld kan worden. Op dit moment wordt gewerkt aan een pilot, om te zien welke content het meest gemeld wordt en hoe slachtoffers daarmee het beste geholpen kunnen worden. De verwachting is dat dit meldpunt begin 2024 van start kan gaan. Wij zullen uw Kamer op de hoogte houden van deze ontwikkelingen.

Strafbare content kan uiteraard ook bestreden worden door middel van opsporing en vervolging. In het geval van deepnudes gaat het om de vervolging van diegenen die deze content vervaardigen, ter beschikking hebben of openbaar maken. Als het noodzakelijk is ter beëindiging van het strafbare feit kan de officier van justitie – ook voordat een verdachte voor het strafbare feit is veroordeeld – in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Wetboek van Strafvordering (Sv), met een machtiging van de rechter-commissaris aan een aanbieder van een communicatiedienst bevelen om gegevens ontoegankelijk te maken (artikel 125p Sv).

Daarnaast kan een slachtoffer bij de civiele rechter een (kort geding) procedure starten waarin een vordering tot verwijdering van die content centraal staat. Dit wordt getoetst aan de voorwaarden van de onrechtmatige daad uit artikel 6:162 van het BW. Een voorbeeld hiervan is wanneer het gaat om (deepfake)content waarbij onrechtmatig persoonsgegevens zijn verwerkt. Ook kan een klacht worden ingediend bij de Autoriteit Persoonsgegevens (AP) wanneer het gaat om (deepfake)content waarbij onrechtmatig persoonsgegevens zijn verwerkt.

De motie Rajkowski c.s.

De gewijzigde motie van het lid Rajkowski c.s. verzoekt om, in lijn met de reguleringsopties die zijn beschreven in het WODC-onderzoek, een wetsvoorstel in procedure te brengen om bepaalde vormen van deepfake-technologie tegen te gaan.[11] In dit wetsvoorstel zou het volgens de motie in elk geval moeten gaan om het verbieden van het vervaardigen,

[11] Kamerstuk 36 200 VII, nr. 118.

aanbieden, verspreiden, downloaden of gebruiken van deepfaketechnologie of technologie die kan worden ingezet om deepfakes te genereren. Het kabinet onderschrijft geheel de onderliggende zorg van deze motie dat deepfakes voor slachtoffers ernstige gevolgen kunnen hebben. Ook onderschrijft het kabinet het onderliggende doel van de motie dat het van groot belang is dat we effectief kunnen optreden tegen de negatieve uitwassen van deepfaketechnologie. Het verdient daarom te worden benadrukt dat het vervaardigen van de meest onwenselijke deepfakes niet slechts strafbaar is op grond van artikel 139h Sr (vervaardigen afbeeldingen van seksuele aard) en artikel 240b Sr (kinderporno), maar, zoals hierboven is uiteengezet – daadwerkelijk ook hard wordt bestreden in het kader van de aanpak van onrechtmatige en strafbare content. Een algemener verbod op het gebruiken van deepfaketechnologie als zodanig is daarvoor niet noodzakelijk en heeft ook negatieve effecten. Van belang is tevens dat een eventueel breed verbod in strijd kan komen met verschillende (fundamentele) rechten zoals de vrijheid van meningsuiting of de vrijheid van kunsten en wetenschappen.

Voor wat betreft het voorstel in de motie om het vervaardigen, aanbieden, verspreiden en downloaden van de technologie als zodanig, bijvoorbeeld op de consumentenmarkt, te verbieden – hetgeen kan worden onderscheiden van een verbod op het gebruiken van de technologie – om zo de beschikbaarheid van deze technologie tegen te gaan, merkt het kabinet het volgende op. Zoals ook in het onderzoek naar voren komt, zal een algemeen verbod op het vervaardigen, aanbieden, verspreiden en downloaden van de technologie waarmee deepfakes kunnen worden gemaakt naar verwachting eenvoudig kunnen worden omzeild. Zoals wij argumenteren in onze de appreciatie van reguleringsoptie 10 in bijlage 1, zullen aanbieders die zich veelal in het buitenland bevinden moeilijk kunnen worden aangesproken. Het kabinet onderschrijft de zoektocht en het doel om de negatieve kanten van het gebruik van deze technologie, zoals tijdens het debat door uw Kamer naar voren gebracht, tegen te gaan. Daartoe steunt het kabinet ook de Europese aanpak van deepfakes zoals die wordt voorgesteld in de AI-verordening, die nu in onderhandeling is. Daarin wordt een transparantieverplichting voor deepfakes voorgesteld om het specifiek met deepfakes geassocieerde gevaar dat gemanipuleerd materiaal ten onrechte voor authentiek wordt gehouden, zo veel mogelijk (vooraf) te mitigeren. Bijvoorbeeld door de verplichting om bij materiaal waarvan de inhoud door AI is gegenereerd of gemanipuleerd, bekend te maken hoe deze tot stand is gekomen. Dit kan worden gerealiseerd op verschillende manieren, zoals door een watermerk bij deepfake beelden waar de VVD al vaker aandacht voor heeft gevraagd. Het kabinet zal alles in het werk stellen om de AI-verordening en de bijbehorende transparantieverplichting uit te voeren. Op die manier wil het kabinet tegemoetkomen aan het gezamenlijke doel en daarmee deze motie om de negatieve kanten van het gebruik van AI tegen te gaan.

De gewijzigde motie van het lid Rajkowski c.s. verzoekt verder om na te gaan op welke manier het beïnvloeden van verkiezingen of politieke besluitvorming middels het creëren of verspreiden van desinformatie door middel van deepfakes en AI expliciet strafbaar kan worden gesteld. Het kabinet is van mening dat voor het strafbaar stellen van deepfakes of andere artificiële intelligentie (AI) om verkiezingen te beïnvloeden, artikel 127 Sr volstaat (in bijlage 1 wordt hier bij aanbeveling 6, 7 en 8 nader op ingegaan). Zoals ook wordt toegelicht in de rijksbrede strategie effectieve aanpak van desinformatie door het Ministerie van Binnenlandse

Zaken en Koninkrijksrelaties (BZK), staat in het beleid tegen desinformatie het recht op vrijheid van meningsuiting voorop.[12]

Bewustwording

Goede voorlichting en communicatie, onder meer met het oog op preventie, kan bijdragen aan bewustwording over de gevaren van deepnudes. Daarom wordt in lijn met de aanbeveling om in publiekscommunicatie aandacht te geven aan nieuwe sociale normen zoveel mogelijk aangesloten bij de communicatieaanpak die in het kader van de implementatie van het wetsvoorstel seksuele misdrijven wordt ontwikkeld, en waar mogelijk bij voorlichtingsactiviteiten in het kader van het Nationaal Actieprogramma Aanpak Grensoverschrijding Seksueel Gedrag en Seksueel Geweld. In het laatstgenoemde actieprogramma wordt ingezet op een cultuurverandering waarmee seksueel grensoverschrijdend gedrag en seksueel geweld zoveel mogelijk worden voorkomen. Ook wordt nagegaan of de diverse slachtofferorganisaties, waar ook slachtoffers van bijvoorbeeld pornografische deepfakes of discriminatoire deepfakes terecht kunnen, extra gefaciliteerd dienen te worden om slachtoffers op praktisch, juridisch en emotioneel gebied goed te kunnen bijstaan.

Tot slot worden er in het kader van deepfakes nog de volgende maatregelen ondernomen:

- Bewustwording en praktische handvatten voor de omgang met gemanipuleerd materiaal in de keten tussen politie, (OM) en het Nederlands Forensisch Instituut (NFI), nu en met het oog op de toekomst. De politie heeft mede de aanzet gegeven tot een Rijksbrede Werkconferentie over de impact van synthetische media en deepfakes die in januari 2023 plaatsvond. Het NFI voert samen met de Universiteit van Amsterdam (UvA) een onderzoeksprogramma uit, om met het oog op de toekomst de mogelijkheden voor deepfakedetectie in de rechtspraktijk verder te verbeteren.
- Het in de AI-verordening, die momenteel in onderhandeling is, steunen van een transparantieplicht voor deepfakes, om de kans te reduceren dat gemanipuleerd materiaal ten onrechte voor «authentiek» wordt gehouden.
- Het bevorderen van regulering die de herkomst en de methoden van verspreiding van desinformatie op internetdiensten inzichtelijker maakt. Een instrument in deze ontwikkeling is de in juni 2022 herziene Europese praktijkcode tegen desinformatie (Code of Practice against Disinformation).

Voor een uitgebreide bespreking van alle reguleringsopties uit het onderzoek naar deepfakes, verwijzen wij naar bijlage 1.

Immersieve technologieën

Het tweede onderzoek gaat over de regulering van immersieve technologieën. Immersieve technologieën zijn technologieën die de realiteit aanpassen, of een nieuwe realiteit creëren. Het doel van deze technologieën is om een gevoel van onderdompeling (immersie) in een (deels) kunstmatige omgeving te creëren die de werkelijke omgeving aanpast of vervangt. Het onderzoek bespreekt de twee bekendste vormen van immersieve technologieën: Augmented Reality (AR) en Virtual Reality (VR). Bij AR wordt onze perceptie van de wereld uitgebreid doordat virtuele elementen worden toegevoegd aan de realiteit, bijvoorbeeld door middel van apparaten zoals AR-brillen of toepassingen zoals Pokémon Go. Bij VR wordt de fysieke wereld zo veel mogelijk vervangen door een

[12] Kamerstuk 30 821, nr. 173.

kunstmatige of virtuele werkelijkheid, bijvoorbeeld door een VR-bril. Immersieve technologieën zoals AR en VR kennen veel verschillende toepassingen: in de amusementssector, in de gezondheidszorg (in therapie bij de behandeling van pijn en psychische stoornissen), in het onderwijs en bij trainingen (om leersituaties na te bootsen), bij het voorkomen van recidive (gedragsverandering) en in de opsporing (het simuleren van de omstandigheden op een plaats delict). Deze relatief nieuwe technologieën bieden belangrijke kansen. Zoals reeds eerder bleek uit onderzoek dat in opdracht van het kabinet is uitgevoerd, kan de opkomst van deze technologieën echter ook gepaard gaan met risico's, zoals grensoverschrijdend gedrag in VR.[13] Deze zorg is, in lijn met de motie van de leden Van der Staaij en Van der Graaf, ook aanleiding geweest voor het kabinet om te laten onderzoeken of het recht in brede zin goed is toegerust op de opkomst van immersieve technologieën.[14]

Uit het onderzoek komt naar voren dat het huidige juridische kader in algemene zin goed is toegerust om de mogelijke negatieve effecten van immersieve technologie te adresseren.[15] Veel regelgeving is technologie-neutraal geformuleerd en daarom ook van toepassing op immersieve technologieën. Daarbij is in brede zin gekeken naar de mogelijk risico's waarmee de opkomst van immersieve technologieën gepaard kunnen gaan. Naast vragen omtrent de strafrechtelijke normering van ongewenste gedragingen in virtuele werelden (waarop wij hieronder nog nader ingaan), wordt in het onderzoek aandacht besteed aan afleiding en gevaarzetting door het gebruik van immersieve technologieën, de effecten van immersieve technologieën op mens en gedrag, sociaal maatschappelijke veranderingen, en misbruik van beelden van personen. Op dit moment, ziet het onderzoek, zijn immersieve technologieën in de samenleving nog beperkt geadopteerd in de samenleving.[16] Het onderzoek benoemt verder dat het moeilijk is om te voorspellen hoe deze technologieën zich zullen ontwikkelen en met welke daadwerkelijk gevaren en risico's dit in de toekomst gepaard zal gaan.

Het kabinet ziet dat het bij nieuwe technologieën vaak de vraag is op welk moment regulering wenselijk is om de ontwikkeling ervan in goede banen te leiden. Te vroeg ingrijpen, kan een rem zetten op innovatieve ontwikkelingen. Te laat ingrijpen, kan het ongedaan maken van ongewenste effecten juist lastiger maken.[17] Daarom is, in lijn met de aanbevelingen uit het onderzoek naar immersieve technologieën, in de onlangs aan uw Kamer aangeboden Werkagenda «Waardengedreven Digitaliseren» plaats ingeruimd voor het anticiperen op nieuwe digitale technologieën.[18] Er zal een beleidsagenda publieke waarden en nieuwe digitale technologie worden opgesteld met kaders voor de impact van deze technologie op publieke waarden. Daarbij worden kennisinstellingen, bedrijven en overheden betrokken. Daarnaast onderneemt het kabinet op diverse terreinen reeds actie om de ontwikkeling van deze technologieën, de lijn van de onderzoeksconclusies volgend, in goede banen te leiden. In bijlage 2 bij deze brief gaan wij op deze acties nader in.

---

[13] Kamerstuk 26 643, nr. 720.
[14] Kamerstuk 35 300 VI, nr. 73.
[15] *Regulering van immersieve technologieën,* p. 103 (WODC-onderzoek), bijlage bij Kamerstuk 26 643, nr. 778.
[16] Kamerstuk 26 643, nr. 720.
[17] D. Collingridge, *The Social Control of Technology*, New York: St. Martin's Press 1980.
[18] Kamerstuk 26 643, nr. 940.

Enkele voorbeelden hiervan zijn:
- Preventie en voorlichting omtrent problematisch gebruik van games en digitale media door middel van de Gamen Infolijn en het programma Helder Op School.
- Het volgen van ontwikkelingen en eventuele risico's door AR voor de verkeersveiligheid, waarbij de samenwerking wordt opgezocht met de industrie en brancheverenigingen NLdigital.
- Het opleggen van een verbod aan online platformen op het gebruiken van gegevens van minderjarigen en van bijzondere persoonsgegevens (zoals biometrische data) van alle gebruikers om gepersonaliseerde advertenties te tonen, middels de nieuwe EU-verordening digitale diensten (Digital Services Act, DSA), deze treedt in 2024 inwerking.

Grensoverschrijdende gedragingen in VR

Het kabinet waardeert zeer de aandacht die in het onderzoek is uitgegaan naar regulering van het gevaar dat bepaalde grensoverschrijdende gedragingen zoals virtuele aanranding in een VR-omgeving kunnen worden verricht. Deze zorg is immers, met de motie van de leden Van der Staaij en Van der Graaf, een belangrijke reden geweest waarom het kabinet opdracht heeft gegeven tot dit onderzoek. Wij vinden het dan ook zeer zorgwekkend dat nu in dit onderzoek wordt vastgesteld dat slachtoffers van virtuele aanranding een vergelijkbare emotie ervaren als bij een fysieke aanranding of verkrachting, en dat de onderzoekers verwachten dat naarmate de immersie en het gevoel van aanwezigheid in een virtuele omgeving groter wordt, de impact van virtueel grensoverschrijdend gedrag ook groter kan worden.[19] Ook is volgens het onderzoek niet ondenkbaar dat meer ernstige psychische schade kan ontstaan.[20] Dit zijn ernstige signalen en een donkere keerzijde van het gebruik van immersieve technologieën, waar hard tegen dient te worden opgetreden. Het is dan ook belangrijk om er geen misverstand over te laten bestaan dat het Wetboek van Strafrecht mogelijkheden biedt om tegen deze en andere strafwaardige, laakbare gedragingen in VR op te treden. Dit kan bijvoorbeeld als er sprake is van bedreiging (artikel 285 Sr). Daarvan kan sprake zijn als het virtueel verkrachten of aanranden van iemands avatar,[21] bijvoorbeeld door de avatar van een persoon die het slachtoffer in werkelijkheid kent, bij het slachtoffer de redelijke vrees opwekt dat die gedraging buiten VR kan worden gepleegd. De mogelijkheden om strafrechtelijk op te treden worden verder uitgebreid met het bij de Tweede Kamer aanhangige wetsvoorstel seksuele misdrijven, waarin seksuele intimidatie van een ander in het openbaar in het nieuwe artikel 429ter strafbaar wordt gesteld. Deze mogelijkheden worden in bijlage 2 bij deze beleidsreactie uitvoerig besproken. Voor een uitvoerige bespreking van alle reguleringsopties uit het onderzoek naar immersieve technologieën, verwijzen wij verder naar bijlage 2.

Wij zien verder dat over het aantal slachtoffers van deze grensoverschrijdende gedragingen in de virtuele wereld op dit moment erg weinig bekend is, hetgeen uitvraag bij onder andere Slachtofferhulp Nederland (SHN) heeft bevestigd. Het onderzoeksrapport over immersieve technologieën is daarom ook gedeeld met Slachtofferhulp Nederland (SHN), het Centrum Seksueel Geweld (CSG), het Expertisebureau Online Kindermisbruik (EOKM) en HelpWanted.

---

[19] *Regulering van immersieve technologieën,* p. 59 (WODC-onderzoek), bijlage bij Kamerstuk 26 643, nr. 720.

[20] Ibidem, p. 65.

[21] Een avatar is een afbeelding of figuur die symbool staat voor een persoon, bijvoorbeeld als alter ego waarmee je deelneemt aan een computerspel of een forum.

Ook gaat het kabinet, in lijn met de reguleringsopties uit het onderzoek, in gesprek met de sector om te bekijken of grensoverschrijdende gedragingen in de virtuele wereld door middel van technologie kunnen worden tegengegaan. Voor een uitvoerige bespreking van alle reguleringsopties uit het onderzoek naar immersieve technologieën, verwijzen wij verder naar bijlage 2.

Tot slot

Op basis van beide onderzoeken komen wij tot de conclusie dat het recht op dit moment voldoende mogelijkheden biedt om het meest onwenselijke gebruik en effecten van zowel immersieve als deepfake technologie in horizontale verhoudingen te adresseren. Desalniettemin is het belangrijk de introductie van dergelijke technologieën op een verantwoorde wijze in onze samenleving te begeleiden. Het is goed te constateren dat hier kabinetsbreed de nodige maatregelen toe worden genomen.

De Minister voor Rechtsbescherming,
F.M. Weerwind

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

Bijlage 1

– Deepfakes: De juridische uitdagingen van een synthetische samenleving

Deepfake is een verzamelnaam voor verschillende soorten content (beeld, geluid of ander materiaal) die geheel of gedeeltelijk zijn gemaakt met artificiële intelligentie (AI)-software. Vaak worden deepfakes gebruikt om iemand iets te laten doen of zeggen wat die persoon in werkelijkheid niet heeft gedaan of gezegd. Deze nieuwe technologie heeft veel waardevolle toepassingen: in het onderwijs (bijvoorbeeld om historische personages tot leven te wekken), in de gezondheidszorg (om synthetische MRI-beelden van hersenen met tumoren te maken, of om vanuit die beelden algoritmen te trainen om vroege vormen van kanker of hersenziekten zoals Alzheimer op te sporen), bij kunstuitingen, onschuldige en grappige filmpjes in de huiselijke sfeer, en (politieke) satire.

De mogelijkheid om beelden te manipuleren kan ook op onwenselijke, onrechtmatige en strafbare manieren worden gebruikt. Deepfakes kunnen bijvoorbeeld worden ingezet bij het verspreiden van desinformatie, of roepen vragen op over de privacy van de daarin afgebeelde personen. Terecht heeft uw Kamer aandacht gevraagd voor het fenomeen deepnudes: pornografische deepfakes die vaak tegen de wil van degenen die erin worden afgebeeld, worden gemaakt en geopenbaard.[22] Het kabinet deelt de zorgen over dit fenomeen, en heeft mede om die reden het WODC onderzoek laten uitvoeren naar de vraag of het recht daartegen goed beschermt. Het onderzoek richt zich primair op de vraag of de Algemene verordening gegevensbescherming (AVG) of diens uitvoeringswet de UAVG, het burgerlijk (proces)recht en het straf(proces)recht een adequaat beschermingsniveau bieden.

De eerste conclusie van het onderzoek luidt dat het meest onwenselijke gebruik van deepfakes of deepfaketechnologieën via het huidige recht goed is te adresseren. Het strafrecht is in algemene zin goed toegerust om strafwaardige deepfakes aan te pakken. Bijzondere aandacht verdient dat het zonder toestemming van de afgebeelde persoon openbaar maken van seksueel deepfake beeldmateriaal strafbaar is op grond van artikel 139h Sr. Zoals wij hierna bij de appreciatie van reguleringsoptie 1 toelichten, valt ook het vervaardigen en voorhanden hebben van dat materiaal (zonder openbaring ervan) binnen het bereik van die bepaling. Naar aanleiding van onze toezegging tijdens het debat over de begroting van Justitie en Veiligheid 2023, bespreken we ook de wijze waarop deepfakes in Virginia (de Verenigde Staten) binnen het bereik van het strafrecht worden gebracht.[23] Buiten het strafrecht, werpt de AVG obstakels op tegen het maken en verspreiden van deepfakes waarin persoonsgegevens zijn verwerkt zonder een verwerkingsgrondslag. Daarnaast gelden de kaders van het civiele recht, waar gedacht kan worden aan een actie grond van onrechtmatige daad (artikel 6:162 BW) of aan het portretrecht zoals bedoeld in de Auteursrecht. Tot slot volgt uit het onderzoek dat het procesrecht goed is toegerust op de mogelijkheid dat deepfakes worden gebruikt als nepbewijs (zie de appreciatie van reguleringsoptie 9).

De tweede conclusie van het onderzoek luidt dat de handhaving van bestaande regels complex kan zijn en aandacht verdient. Opmerking verdient in dit verband dat het bestaande recht – zoals het onderzoek beklemtoont – voor die handhaving weldegelijk mogelijkheden biedt. Strafbare content wordt vanzelfsprekend bestreden door middel van

[22] Kamerstuk 35 570 VI, nr. 37; Kamerstuk 36 200 VII, nr. 118; Aanhangsel Handelingen II 2022/23, nr. 719.
[23] Handelingen II 2022/23, nr. 24, item 11.

opsporing en vervolging; in het geval van strafbare deepnudes bijvoorbeeld van diegenen die deze content vervaardigen, ter beschikking hebben of openbaar maken. Ook kan een klacht worden ingediend bij de Autoriteit Persoonsgegevens (AP). Daarnaast is de aanpak gericht op de snelle verwijdering van deze content door de internetsector. Daarop gaan wij nader in bij: «3. Naleving en handhaving van het recht in een online omgeving», en in het bijzonder bij de appreciatie van reguleringsoptie 11.

De gewijzigde motie van het lid Rajkowski verzoekt om, in lijn met de reguleringsopties die zijn beschreven in het WODC-onderzoek een wetsvoorstel in procedure te brengen om bepaalde vormen van deepfaketechnologie tegen te gaan, waarbij in elk geval het vervaardigen, aanbieden, verspreiden, downloaden of gebruiken van deepfaketechnologie of technologie die kan worden ingezet om deepfakes te genereren wordt verboden.[24] In reactie op die motie, kan worden opgemerkt dat een verbod zich bij voorkeur richt op wat een gedraging onwenselijk maakt. Ook is regelgeving bij voorkeur technologie-neutraal geformuleerd zodat snelle technologische ontwikkelingen de wetgeving niet aantasten. Omdat het misbruik van deepfaketechnologie, zoals hierboven opgemerkt, reeds strafbaar of anderszins onrechtmatig zijn, en het kabinet daarnaast actief inzet op het verwijderen van onrechtmatige deepfake content van het internet, zien wij op dit moment nog geen aanleiding om het vervaardigen, aanbieden, downloaden en gebruiken van deze technologie als zodanig te verbieden. Dit lichten wij nader toe in onze de appreciatie van reguleringsoptie 10.

De gewijzigde motie van het lid Rajkowski verzoekt tevens om na te gaan of de manier van het beïnvloeden van verkiezingen of politieke besluitvorming middels het creëren of verspreiden van desinformatie strafbaar kan worden gesteld. Voor het strafbaar stellen van deepfakes of andere AI om verkiezingen te beïnvloeden, volstaat artikel 127 van het wetboek van Strafrecht (zie ook de appreciatie van aanbeveling 6, 7 en 8). Zoals ook wordt toegelicht in de rijksbrede strategie effectieve aanpak van desinformatiedoor het Ministerie van BZK, staat in het beleid tegen desinformatie het recht op vrijheid van meningsuiting voorop. [25] Een algemeen verbod op het verspreiden van desinformatie acht het kabinet niet wenselijk.

Tot slot willen we graag benadrukken dat goede voorlichting en communicatie, onder meer met het oog op preventie, bij kan dragen aan bewustwording bij potentiele daders over de gevolgen van strafbare deepfakes. Daar zetten wij ons voor in, zoals toegelicht bij de appreciatie van reguleringsoptie 12. Ook willen we ervoor zorgen dat slachtoffers van onrechtmatige of strafbare deepfakes goed geholpen worden en weten waar ze terecht kunnen. We lichten ook dit nader toe bij de appreciatie van reguleringsoptie 12.

Hierna volgt onze appreciatie van het twaalftal reguleringsopties uit het WODC-onderzoek op drie deelonderwerpen:

1. bescherming tegen deepfakes door middel van het materiële recht;
2. deepfakes in het procesrecht; en
3. naleving en handhaving van recht in een online omgeving.

[24] Kamerstuk 36 200 VII, nr. 118.
[25] Kamerstuk 30 821, nr. 173.

1. Bescherming tegen deepfakes door middel van het materiële recht

Strafrecht

Reguleringsoptie 1: Voer een debat over de vraag of het maken of bezitten van «intrinsiek» strafwaardige (moreel verwerpelijke) deepfakes strafbaar zou moeten worden gesteld.

In het onderzoek wordt geargumenteerd dat het vervaardigen van seksuele deepfakes zonder deze te openbaren buiten het bereik van de strafwet valt. Het maken van seksuele deepfakes, zou volgens de onderzoekers niet vallen onder artikel 139h, eerste lid, sub a, Sr («hij die opzettelijk en wederrechtelijk van een persoon een afbeelding van seksuele aard vervaardigt»), omdat deze bepaling blijkens de wetsgeschiedenis en systematiek slechts het doel zou hebben de privacy te beschermen door het maken van heimelijke afbeeldingen in de fysieke ruimte te verbieden. Nu dat laatste bij het vervaardigen van een seksuele deepfake, een zogenoemde deepnude, niet zonder meer aan de orde is, zou die gedraging volgens de onderzoekers niet onder het huidige bereik van artikel 139h, eerste lid, sub a, Sr vallen; daartoe zou deze bepaling moeten worden aangepast.

In de Amerikaanse staat Virginia is in een wet die het zonder toestemming maken en verspreiden van seksueel beeldmateriaal strafbaar stelt, – vrij vertaald – expliciet opgenomen «dat het niet uitmaakt hoe dit beeldmateriaal tot stand is gekomen».[26] Naar aanleiding van toezegging die is gedaan tijdens het debat over de begroting van Justitie en Veiligheid 2023 gaat de Minister van Justitie bij de bespreking van het voorstel tot herformulering van artikel 139h Sr, hierna, in op regeling die in Amerika is ontworpen.[27]

Het kabinet is van mening dat een herformulering van 139h Sr in Nederland niet noodzakelijk is, omdat artikel 139h Sr een bredere strekking heeft dan daaraan in het onderzoek wordt toegedicht. In de toelichting bij deze bepaling is benoemd dat het maken van seksuele afbeeldingen strafbaar is, «ongeacht de plaats waar dit gebeurt of het middel dat hiervoor wordt gebruikt».[28] In de wetsgeschiedenis van artikel 139h Sr komt verder naar voren dat in het geval dat zonder medeweten of toestemming van de afgebeelde persoon seksueel beeldmateriaal wordt vervaardigd, er sprake is van aantasting van de persoonlijke levenssfeer en dat de afgebeelde personen gelet op de intieme en gevoelige aard van het materiaal zelf moeten kunnen bepalen of dit tot stand komt.[29] Dat ook het maken van een seksuele deepfake strafbaar kan zijn op grond van artikel 139h Sr, eerste lid, sub a, Sr. wordt bevestigd door een uitspraak van de rechtbank Den Haag van 4 maart 2021 waarin de verdachte hiervoor is veroordeeld.[30] In de ogen van het kabinet is het ook wenselijk dat het beschermingsbereik van artikel 139h, eerste lid, sub a, Sr zich mede uitstrekt tot het vervaardigen van seksuele deepfakes. Het kabinet ziet dan ook geen aanleiding om de strafbaarstelling van artikel 139h eerste lid, sub a, Sr, bijvoorbeeld naar het model van eerdergenoemde wet uit de Amerikaanse staat Virginia, bij te stellen.

---

[26] Kamerstuk 26 643, nr. 815, p. 243, 247, 248.
[27] Handelingen II 2022/23, nr. 24, item 11.
[28] Kamerstuk 35 080, nr. 3, p. 22.
[29] Kamerstuk 35 080, nr. 3.
[30] Rb Den Haag 4 maart 2021, RBDHA:2021:1885.

Reguleringsoptie 2: Overweeg artikel 231b Sr aan te passen door de clausule «niet zijnde biometrische gegevens» te schrappen of aan te passen.

Deepfakes kunnen ook worden gezien als een vorm van identiteitsfraude. Zoals het onderzoek signaleert, biedt artikel 231a Sr soelaas wanneer voor identificatiedoeleinden wordt gebruikgemaakt van een deepfake, maar kan artikel 231b Sr niet altijd worden ingeroepen om identiteitsfraude met deepfakes waarbij enig nadeel kan ontstaan te bestrijden. Het kabinet ziet hierin echter geen aanleiding om over te gaan tot wetswijziging. Identiteitsfraude met deepfakes die nadeel tot gevolg hebben kunnen immers ook goed worden aangepakt op grond van veel andere strafbepalingen (zoals oplichting, smaad en laster), hetgeen wordt bevestigd door het OM. Zoals het onderzoek ook concludeert, zijn deze, en veel andere, strafbepalingen zodanig technologie-neutraal geformuleerd dat ze ook op deepfakes en andere toekomstige andere technieken van toepassing zijn. Wat betreft identiteitsfraude met deepfakes bestaat er daarom, voor zover nu bekend, geen lacune in de rechtsbescherming.

Gegevensbeschermingsrecht

Het onderzoek biedt een zeer doorwrochte analyse over de toepassing van de AVG in de context van deepfakes. Uit het onderzoek volgt dat wanneer de AVG van toepassing is op de verwerking van persoonsgegevens om een deepfake te maken er goede bescherming wordt geboden. De AVG stelt namelijk zodanig strenge eisen aan de rechtmatige verwerking van persoonsgegevens dat het onwaarschijnlijk is dat onwenselijke deepfakes waarbij persoonsgegevens worden verwerkt de toets ervan zullen doorstaan.

Zo dient op grond van de AVG, wanneer persoonsgegevens worden verwerkt, sprake te zijn van een legitiem doel en een rechtmatige verwerkingsgrondslag. Het onderzoek merkt op dat deze verwerkingsgrondslag kan liggen in toestemming van degenen wiens gegevens worden verwerkt, of (indien er geen toestemming is) als er sprake is van een gerechtvaardigd belang (van een derde). Het recht op vrijheid van meningsuiting van een derde kan in uitzonderlijke gevallen een gerechtvaardigd belang bieden voor verwerking van persoonsgegevens als de betrokkene daarvoor geen toestemming heeft gegeven, bijvoorbeeld in het geval van een satirische deepfake van een politicus. Wanneer daarbij privacygevoelige content zoals naaktbeelden wordt verwerkt, zal aan de voorwaarden daarvoor echter niet snel zijn voldaan.

Daarnaast moet voor rechtmatige verwerking van persoonsgegevens aan de beginselen van rechtmatige gegevensverwerking zijn voldaan. Deepfakes zijn volgens het onderzoek mogelijk zelfs per definitie in strijd met de AVG omdat het datakwaliteitsbeginsel vereist dat persoonsgegevens juist moeten worden verwerkt terwijl deepfakes naar hun aard een valse voorstelling van zaken geven. Dan zijn er ook nog de diverse rechten van het datasubject waar rekening mee moet worden gehouden, zoals het recht op inzage, hetgeen inhoudt dat mensen het recht hebben te weten welke persoonsgegevens van hen worden verwerkt. Hoewel elk geval op zichzelf moet worden beoordeeld, volgt duidelijk uit het onderzoek dat de AVG strenge eisen stelt aan het maken van deepfakes.

Zoals volgt uit het onderzoek, betekent een en ander uiteraard niet dat de AVG op alle deepfakes van toepassing is. Het onderzoek benoemt drie mogelijks situaties waarin de AVG niet van toepassing is op deepfakes, en reikt in dit verband drie reguleringsopties aan (reguleringsoptie 3, 4 en 5) die hieronder worden besproken.

Reguleringsoptie 3: Bekijk in hoeverre het creëren van wet- of regelgeving aangaande post-mortem privacy wenselijk is.

Het onderzoek stelt vast dat de AVG niet van toepassing is op deepfakes waarbij geen persoonsgegevens van nog levende mensen worden verwerkt.[31] Mede naar aanleiding van de mogelijkheden die deepfaketechnologie biedt om overledenen weer tot leven te wekken, roept het onderzoek de vraag op of de privacy van overledenen wel voldoende is beschermd. In reactie daarop, kan worden opgemerkt dat dergelijke deepfakes van overledenen, ook los van het bereik van de AVG, onrechtmatig of zelfs strafbaar kunnen zijn. Zo kan een strafbaar feit zoals smaad (artikel 261 Sr) – bijvoorbeeld door middel van deepfakes – ook ten aanzien van overledenen worden gepleegd.[32] Ook het portretrecht kan met een deepfake van een overledene in het geding zijn. Zoals ook het onderzoek vaststelt, kan het portretrecht, na het overlijden van de geportretteerde aan een nabestaande toekomen.[33]

De vraag of nieuwe wet- of regelgeving aangaande post-mortem privacy nodig is, is recentelijk in opdracht van het Ministerie van BZK onderzocht in twee onderzoeken over de omgang met gegevens (data, beelden, geluid) van overleden personen.[34] Die onderzoeken zijn ook van belang voor bescherming tegen deepfakes waarin materiaal van overledenen is verwerkt. In de beleidsreactie naar aanleiding van die onderzoeken, wordt in lijn met die onderzoeken geconcludeerd dat het voor nieuwe regelgeving op dit vlak nog te vroeg is. Het is immers onduidelijk of, en zo ja welke, maatschappelijke problemen burgers ervaren, welke oplossingen daarbij passen en wat hun wensen omtrent de digitale nalatenschap zijn.[35] Nut en noodzaak van nieuwe wettelijke maatregelen staan daarom nog onvoldoende vast.

Reguleringsoptie 4: Bekijk in hoeverre het creëren van wet- en regelgeving omtrent het gebruik van volledig door AI gegenereerde personen wenselijk is.

Het kabinet ziet dat het gebruik van volledig door AI gegenereerde personen risico's met zich meebrengt. Ook roept deze mogelijkheid ethische vragen op over het vervagende onderscheid tussen echt en nep. Het kabinet is daarom positief dat het ontwikkelen, aanbieden en gebruiken van AI-systemen die mogelijk een risico met zich mee brengen voor gezondheid, veiligheid en fundamentele rechten wordt gereguleerd in de voorgestelde Europese AI-verordening die momenteel nog in onderhandeling is. In die verordening zijn specifiek voor regelgeving die ziet op AI-gegenereerde personen twee bepalingen van belang. Volgens een bepaling moeten AI-systemen die interacteren met individuele personen aan een aantal eisen voldoen die het risico op manipulatie mitigeert. Zo dienen aanbieders van die AI-systemen te zorgen dat deze systemen personen in beginsel informeren dat zij met een AI-systeem interacteren. Een andere bepaling verplicht de makers van gemanipuleerde content, zoals deepfakes, om te openbaren dat het hier gaat om gemanipuleerde content.

Reguleringsoptie 5: Bekijk in hoeverre de herziening van de huishoudelijke exceptie binnen het gegevensbeschermingsrecht wenselijk is.

---

[31] Overweging 27 AVG.
[32] Deepfakes: De juridische uitdagingen van een synthetische samenleving, p. 60 (WODC-onderzoek), bijlage bij Kamerstuk 26 643, nr. 815.
[33] Ibidem, p. 110.
[34] Kamerstuk 30 696, nr. 52.
[35] Ibidem.

Het onderzoek constateert dat het bereik van de AVG zich vanwege de zogenoemde «huishoudelijke exceptie» niet uitstrekt tot de privésfeer. Ook het maken en verspreiden van deepfakes waarin persoonsgegevens worden verwerkt binnen de huishoudelijke sfeer, vallen daarom buiten de reikwijdte van de AVG. Het kabinet ziet dit niet als een probleem voor de aanpak van de meest onwenselijke deepfakes, nu het probleem daarvan primair gelegen is in de verspreiding ervan buiten de privésfeer van de maker ervan. Bovendien is het maken (ook als deze niet worden verspreid) reeds in het strafrecht geregeld. Zoals hiervoor besproken, is het kabinet van mening dat artikel 139h Sr eerste lid, sub a, Sr van toepassing is op het maken van deepfakes, waardoor het maken van deze seksuele deepfakes als zodanig reeds strafbaar is. Bovendien is, zoals ook het WODC-onderzoek constateert, het maken van deepfake-kinderporno (artikel 240b Sr) en deepfake-dierenpornografie (artikel 254a Sr) strafbaar, ook als het betreffende materiaal niet wordt verspreid.[36] Het kabinet is dan ook niet van mening dat de huishoudelijke exceptie in de weg staat aan de aanpak van onwenselijke deepfakes. Daarbij komt dat het heroverwegen van de huishoudelijke exceptie, een onwenselijke juridisering van het privéleven van burgers zou betekenen die veel verder reikt dan de gevallen waarin deepfakes worden gemaakt, nog daargelaten de vraag wat voor effectieve handhaving van de AVG achter de voordeur nodig zou zijn. Daarnaast heeft het kabinet niet de mogelijkheid om de AVG te wijzigen. Het recht van initiatief ligt bij de Europese Commissie en zij voorziet in de komende tijd geen noodzaak tot het doen van wijzigingsvoorstellen van de AVG.

Vrijheid van meningsuiting en recht op reputatie

Het onderzoek constateert dat de vaststelling van mogelijke onrechtmatigheid van een deepfake regelmatig een belangenafweging vergt, waarin het belang van het recht op vrijheid van meningsuiting zal moeten worden afgewogen tegen een ander belang dat tegen het openbaar maken van de deepfake pleit (bijvoorbeeld het recht op privacy). Het resultaat van die belangenafweging kan zijn dat bepaalde soorten onwenselijk te achten gebruik van deepfakes rechtmatig zijn. Naar aanleiding van die mogelijkheid, noemt het onderzoek drie reguleringsopties.

Reguleringsoptie 6: Bekijk in hoeverre het aannemen van wet- of regelgeving waarin nadere regels worden gesteld met betrekking tot uitingen over publieke figuren wenselijk is.

Het kabinet ziet dat de juridische instrumenten die bestaan om tegen onrechtmatige uitingen door middel van deepfakes op te treden, ook van toepassing zijn op publieke personen. Als er sprake is van een onrechtmatige daad, kan bij de rechter een schadevergoeding en verwijdering van de online content worden gevorderd. Wanneer er sprake is van strafbare discriminatie (artikel 137c Sr), smaad of smaadschrift, laster en belediging (artikel 261, 262 en 266 Sr) kan daartegen strafrechtelijk worden opgetreden. Zoals het onderzoek opmerkt, speelt ook het recht op vrijheid van meningsuiting bij de uitleg van deze bepalingen bij politici een belangrijke rol. Uit de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM)[37] volgt immers dat publieke personen een grotere inmenging in hun privéleven moeten dulden dan gewone burgers, en dat zij moeten accepteren dat er over hen en hun gedragingen

[36] Deepfakes: De juridische uitdagingen van een synthetische samenleving, p. 67 (WODC-onderzoek), bijlage bij Kamerstuk 26 643, nr. 815.

[37] Zie bijvoorbeeld: EVRM 8 juli 1986, ECLI:CE:ECHR:1986:0708JUD000981582 (Lingens t. Oostenrijk).

gepeperde en soms vergaande meningen worden verkondigd.[38] Dit is een kenmerk van een vrije samenleving, waarin burgers zich openlijk kritisch en satirisch kunnen uiten over de overheid, terwijl de grens tussen het ambt en de persoon die het ambt vervult niet scherp te trekken is. Daarbij geldt wel dat bestuurders, volksvertegenwoordigers en ambtenaren, hun ambt of functie te allen tijde op deskundige en integere wijze moeten kunnen uitvoeren. Als zij daarbij te maken krijgen met agressie en intimidatie kan dat veel en onnodig leed met zich meebrengen voor betrokkenen zelf en voor hun naasten. Dergelijke agressie en intimidatie is uiteraard altijd onaanvaardbaar.[39]

Reguleringsoptie 7: Bekijk in hoeverre het wenselijk is om wet- of regelgeving te creëren ten aanzien van evident onware, onjuiste of misleidende uitingen.

Het kabinet deelt de zorgen uit het onderzoek rondom de verspreiding van onware, onjuiste of misleidende informatie. Deepfakes kunnen bij uitstek worden gebruikt om onjuiste informatie te verspreiden. De oplossing van dit probleem is volgens het kabinet echter niet gelegen in nieuwe wet- en regelgeving anders dan in de hiervoor genoemde DSA. Zoals is uiteengezet in enkele recente Kamerbrieven, staan in het kabinetsbeleid tegen desinformatie de rechtsstaat en grondrechten als de vrijheid van meningsuiting voorop.[40] In 2019 heeft het Instituut voor Informatierecht (IViR) van de UvA in opdracht van het Ministerie van BZK onderzoek uitgevoerd naar de vraag of er wet- of regelgeving dient te worden ontwikkeld om evident onware, onjuiste of misleidende uitingen aan te pakken.[41] De beleidsreactie op dat onderzoek onderschrijft de conclusie dat het juridisch verbieden van bepaalde informatie alleen op grond van het feit dat informatie onjuist of misleidend is, zonder aanvullende eisen, moeilijk in overeenstemming te brengen is met het recht op vrijheid van meningsuiting.[42] Dit geldt in het bijzonder voor gevallen waarin misinformatie kwalificeert als een politieke uiting waardoor het brede bescherming binnen de vrijheid van meningsuiting geniet.

In lijn met het voorgaande, wil het kabinet regulering bevorderen die de herkomst en de methoden van verspreiding van desinformatie op internetdiensten inzichtelijker maakt. Een belangrijk instrument in deze ontwikkeling is de Europese praktijkcode tegen desinformatie (Code of Practice against Disinformation). Deze code is in juni van 2022 herzien. In deze herziening is er onder andere aandacht voor maatregelen om manipulatief gedrag en het gebruik van diensten voor de verspreiding van desinformatietegen te gaan. Ondertekenaars van de code zeggen bijvoorbeeld toe de hiervoor gebruikte technieken, zoals kwaadaardige deepfakes, bots en impersonatie, beter in kaart te brengen en eigen beleid in te stellen om dergelijk gedrag tegen te gaan. Daarnaast kan deze Code of Practice bij de inwerkingtreding van de DSA mogelijk een Code of Conduct worden, en daarmee één van de mogelijke instrumenten voor VLOPs (Very large Online Platforms) om te voldoen aan de risico mitigerende maatregelen die zij moeten nemen, bijvoorbeeld tegen desinformatie.

---

[38] Deepfakes: De juridische uitdagingen van een synthetische samenleving, p. 192 (WODC-onderzoek), bijlage bij *Kamerstuk* 26 643, nr. 815.
[39] *Kamerstuk* 28 844, nr. 247.
[40] Kamerstuk 30 821, nr. 112; Kamerstukken 30 821 en 35 165, nr. 118.
[41] Kamerstuk 30 821, nrs. 52 en 112.
[42] Kamerstuk 30 821, nr. 112; Kamerstukken 30 821 en 35 165, nr. 118.

Reguleringsoptie 8: Bekijk in hoeverre het wenselijk is om wet- of regelgeving te ontwikkelen ten aanzien van het beïnvloeden van verkiezingen of politieke besluitvorming middels het creëren of verspreiden van misinformatie.

Voor een antwoord op de vraag of specifiek tijdens verkiezingstijd aanvullende wetgeving nodig is, verwijzen wij graag naar de brief aan uw Kamer van 12 oktober 2021.[43] Het kabinet concludeert daarin, in lijn met de conclusie uit het IViR onderzoek naar het juridische kader rondom desinformatie, dat er tijdens verkiezingstijd reeds het nodige mogelijk is. In dit verband volstaat artikel 127 Sr, dat strafbaar stelt een bedrieglijke handeling, waardoor een stem van onwaarde wordt of een stem wordt uitgebracht op een ander dan de bedoelde persoon. Gedacht kan worden aan een deepfake waarin mensen moedwillig verkeerd geïnformeerd worden over de stemwijze, waardoor hun stem ongeldig wordt. Daarnaast kunnen er – bij misleidende informatie over campagnes partijen of kandidaten – juridische aangrijpingspunten zijn in het civielrecht of in het strafrecht indien er sprake is van een strafbaar feit als smaad of laster.

2. Deepfakes in het procesrecht

Reguleringsoptie 9: Bekijk in hoeverre er wet- en regelgeving of beleid dient te worden ontwikkeld of aangescherpt om (deep)fake bewijsmateriaal in de rechtszaal tegen te gaan.

De opkomst van deepfaketechnologieën roept vragen op over hoe om te gaan met mogelijk deepfake bewijsmateriaal. In reactie daarop, benadrukken wij graag de conclusie uit het onderzoek dat er, voor wat betreft de aanpak van deepfakes, geen juridische lacunes bestaan in het strafprocesrecht of civiele procesrecht. Procespartijen hebben de mogelijkheid om twijfels over de authenticiteit van bewijs bij de rechter aan de orde te stellen, en het is dan aan de rechter om daarover te oordelen. De rechter kan daarbij advies inwinnen van deskundigen, zoals de digitaal forensische deskundigen van het NFI die in deepfakes zijn gespecialiseerd.

Opmerking verdient dat er op dit moment uit de Nederlandse rechtspraktijk geen signalen zijn dat deepfakes als bewijs zijn gebruikt. Dit neemt niet weg dat waakzaamheid van groot belang is. Het procesrecht is immers gericht op waarheidsvinding, en voor een eerlijk proces is het essentieel dat goed kan worden onderzocht of ingebracht bewijsmateriaal authentiek is. Daarom zijn we er positief over dat het NFI samen met de UvA een onderzoeksprogramma uitvoert over het verbeteren van deepfakedetectie. In dat onderzoek is aandacht voor de vraag hoe efficiënt om te gaan met een mogelijk in de toekomst vanuit de rechtspraktijk toenemend aantal vragen over deepfakes, zodat bestaande onderzoekscapaciteit ten behoeve van de rechtspraktijk optimaal wordt benut en de rechtspraktijk niet onnodig wordt belast. Deze onderzoeken van de UvA en het NFI vinden plaats in afstemming met de politie, het openbaar ministerie en de rechtspraak. Nu deepfaketechnologieën, naar verwachting, de komende jaren beter en ook breder beschikbaar wordt, is het van belang om aandacht te blijven hebben voor voldoende kennis, expertise, capaciteit en *state-of-the-art*-instrumenten bij instanties als NFI, politie en OM.

[43] Kamerstukken 30 821 en 35 165, nr. 118, p. 3–4.

3. Naleving van het recht in een online omgeving

Het onderzoek signaleert dat de handhaving van bestaande regels complex is. Technologie waarmee illegale deepfakes kunnen worden gemaakt is vrijelijk beschikbaar op het internet, er zijn slechts beperkte technieken om deepfakes bij voorbaat te weren en gepubliceerde deepfakes kunnen eenvoudig worden gekopieerd en verder verspreid. Het onderzoek acht het daarom relatief eenvoudig om onrechtmatige deepfakes te maken en verspreiden, terwijl het ingewikkeld is om daartegen effectief op te treden.

Het kabinet herkent de huidige situatie in deze conclusie, maar benadrukt tevens dat het recht, zoals ook het onderzoek beklemtoont, weldegelijk mogelijkheden voor handhaving biedt. Strafbare content wordt vanzelfsprekend bestreden door middel van opsporing en vervolging – in het geval van deepnudes van diegenen die deze content vervaardigen, ter beschikking hebben of openbaar maken. Daarnaast is de aanpak gericht op de snelle verwijdering van deze content door de internetsector. Zo kan een slachtoffer van onrechtmatige online content, ervoor kiezen deze content te melden bij de internettussenpersoon zoals een platform, dan wel bij de civiele rechter een civielrechtelijke procedure te starten waarbij om een verwijderbevel wordt verzocht, teneinde deze gewraakte content verwijderd te krijgen van het internet. Aanvullend daarop faciliteert de overheid een aantal meldpunten om illegale (waaronder strafbare) content onder de aandacht te brengen van dienstverleners binnen de internetsector. Content die zij als «illegaal» betitelen wordt in dat kader in de meeste gevallen ook daadwerkelijk ontoegankelijk gemaakt. De komende jaren wordt ingezet op het verder optimaliseren van opvolging van meldingen van deze meldpunten en zal daarbij ook bezien voor welke andere vormen van illegale content een meldvoorziening dient te worden ingericht.

Tot slot is het kabinet voornemens een laagdrempelige voorziening in het leven te roepen, waarbij evident onrechtmatige content gemeld kan worden. Hiermee komen wij tegemoet aan de door de Tweede Kamer aangenomen motie van het lid Van Nispen, die oproept tot het oprichten van een laagdrempelige voorziening om (o.a.) het zonder voorafgaande toestemming online plaatsen van seksueel getint materiaal tegen te gaan.[44]

Reguleringsoptie 10: bekijk in hoeverre het wenselijk is om wet- of regelgeving te ontwikkelen waarin het vervaardigen, aanbieden, downloaden of gebruiken van deepfaketechnologie of technologie die kan worden ingezet om deepfakes te genereren, wordt verboden.

Het is zeer zorgelijk dat een groot deel van de deepfakevideo's volgens het WODC-onderzoek pornografisch is en gemaakt zonder wederzijds goedvinden.[45] Tegen die achtergrond is het niet onbegrijpelijk om de technologie waarmee deze deepfakes kunnen worden gemaakt te willen verbieden. In onze reactie daarop, willen wij daarom allereerst benadrukken dat het vervaardigen van de meest onwenselijke deepfakes als zodanig reeds is strafbaar gesteld in artikel 139h Sr (vervaardigen afbeeldingen van seksuele aard) en artikel 240b Sr (kinderporno). Een verbod op het *gebruik van de technologie* voor het vervaardigen als zodanig is daarom voor die gevallen niet noodzakelijk. Daarbij zou een verbod op het gebruiken van deepfaketechnologie, zoals voorgesteld door

[44] Kamerstuk 34 602, nr. 3.
[45] Deepfakes: De juridische uitdagingen van een synthetische samenleving, p. 37 (WODC-onderzoek), bijlage bij Kamerstuk 26 643, nr. 815.

het onderzoek, een breder bereik hebben en ook positieve toepassingen zoals satire kunnen raken. Een dergelijk verbod zou daarom mogelijk strijd opleveren met verschillende (fundamentele) rechten zoals de vrijheid van meningsuiting of de vrijheid van kunsten en wetenschappen. Dit acht het kabinet niet wenselijk.

Ook als het gaat om een verbod op het v*ervaardigen, aanbieden en downloaden* van deepfaketechnologie, zien wij ernstige bezwaren. De maatstaf die in Nederlands en Europees verband geldt wanneer een verbod wordt overwogen, is dat dit verbod gerechtvaardigd moet zijn wegens de bescherming van een dwingende reden van algemeen belang. Dit kan de bescherming van de openbare orde en openbare veiligheid zijn, waaronder ook valt criminaliteitsbestrijding en het beschermen van de goede zeden. Vereist is dan echter wel dat het verbod geschikt is om dat doel te bereiken en niet verder gaat dan noodzakelijk (proportionaliteit in enge zin).

Zowel de geschiktheid van een technologieverbod als de proportionaliteit ervan in enge zin, zijn twijfelachtig. Ten aanzien van de geschiktheid geldt dat een verbod heel eenvoudig kan worden omzeild. De handhaving ervan wordt in de praktijk bovendien snel ingewikkeld omdat een aanbieder van deze technologie in een andere lidstaat (of een derde land) niet of niet makkelijk kan worden aangesproken. In sommige situaties zal het bovendien lastig zijn de aanbieder überhaupt te identificeren. Intussen kan de software wel gemakkelijk worden gevonden en gedownload. Kortom, personen die deze technologie (op een kwaadwillende manier) willen gebruiken, zullen daar ook met een verbod relatief eenvoudig over kunnen beschikken.

Aan de eis van proportionaliteit in enge zin (dat het verbod niet verder gaat dan noodzakelijk) wordt evenmin voldaan. Het onderzoek stelt voor om het verbod slechts voor de consumentenmarkt te laten gelden omdat non-consensuele deepfakeporno vrijwel altijd door burgers zou worden gegenereerd. Het kabinet merkt op, dat er echter geen wetenschappelijk onderzoek is verricht of anderszins bewijs is overgelegd waaruit volgt dat burgers of consumenten in algemene zin verantwoordelijk kunnen worden gehouden voor strafbare deepfakeporno. Het WODC-onderzoek neemt cijfers over van een consultancybedrijf dat concludeert dat de deepfakes die dat bedrijf met deepfake identificatie software op het internet heeft gevonden, voor 96% pornografisch en «non-consensual» van aard zijn.[46] Hoewel het nadruk verdient dat iedere non-consensuele pornografische deepfake er één te veel is, kunnen deze het voorgestelde algemene verbod op deepfaketechnologieën niet legitimeren.

Wel steunt het kabinet een transparantieverplichting voor gebruikers van deepfaketechnologie, zoals ook op EU-niveau in de AI-verordening is voorgesteld. Een dergelijke plicht draagt ertoe bij dat het specifiek met deepfakes geassocieerde gevaar dat gemanipuleerd materiaal ten onrechte voor authentiek wordt gehouden zo veel mogelijk (vooraf) wordt gemitigeerd.

Reguleringsoptie 11: Bekijk in hoeverre het wenselijk is om wet- of regelgeving aan te nemen die ziet op de verplichte controle door internetproviders, burgers en/of de AP van content op de authenticiteit en de rechtmatigheid voordat die content wordt gepubliceerd en/of verspreid.

[46] Ibidem.

Ten aanzien van het voorstel in het onderzoek om aan internetproviders een plicht op te leggen om content voorafgaand op verspreiding ervan op rechtmatigheid te controleren, kan het volgende worden opgemerkt. In 2008 is tussen overheden, internetaanbieders, hostingbedrijven, en andere tussenpersonen een «Notice and Take Down» (NTD) gedragscode overeengekomen die ziet op vrijwillige verwijdering van illegaal (waaronder strafbaar) materiaal door de internetsector. Omdat de verplichtingen voor de sector en de overheid worden aangescherpt met de DSA, die in februari 2024 van toepassing wordt, zal de NTD-gedragscode de komende tijd nog eens tegen het licht worden gehouden vanuit een publiek-private samenwerking. De overheid faciliteert een aantal meldpunten om illegale (waaronder strafbare) content onder de aandacht te brengen van dienstverleners binnen de internetsector. Content die zij als «illegaal» betitelen wordt in dat kader in de meeste gevallen ook daadwerkelijk ontoegankelijk gemaakt. Het kabinet zet de komende jaren bovendien in op het verder optimaliseren van opvolging van meldingen van deze meldpunten en zal daarbij ook bezien voor welke andere vormen van illegale content een meldvoorziening dient te worden ingericht.

Daarnaast geldt dat aanbieders van diensten van de informatiemaatschappij die zelf voorzien in de inhoud van hun dienst, alsmede aanbieders van hostingdiensten (die de informatie die door een aanbieder van inhoud wordt verstrekt enkel opslaan op verzoek) die de inhoud van hun diensten modereren door middel van bijvoorbeeld de selectie van het materiaal dat wel en niet op de dienst wordt geplaatst, zich ervan dienen te vergewissen of de personen die figureren op beelden die worden gedeeld via hun website, platform of anderszins, expliciet toestemming hebben gegeven voor het openbaar maken van die beelden. Doen zij dat niet, dan kunnen zij civielrechtelijk aansprakelijk worden gesteld en eventueel worden gehouden tot betaling van een schadevergoeding en/of het verwijderen of ontoegankelijk maken van de gewraakte content.

Het onderzoek stelt tevens voor om aan burgers een plicht op te leggen vooraf de rechtmatigheid van een deepfake te toetsen door middel van een Data Protection Impact Assessment (DPIA).[47] Een DPIA is bedoeld om in (complexe) gevallen van gegevensverwerking de rechtmatigheid van de gegevensverwerking vast te stellen en de privacyrisico's voor betrokkenen zorgvuldig in kaart te brengen aan de hand van een risicoanalyse. Ook stelt het onderzoek voor om de AP te verplichten deepfakes vooraf *(ex ante)* op rechtmatigheid te controleren. We wijzen er in dit verband op dat de onafhankelijke toezichthouders (inclusief de AP) zelf bepalen wanneer zij een (rechtmatigheids)onderzoek doen en dat het aan de verwerkingsverantwoordelijke is om zelf de afweging te maken om al dan niet een DPIA uit te voeren.[48] Het is niet aan het kabinet om daarin normstellend te zijn. Ook bevat artikel 7 van de Grondwet een absoluut verbod op het door de overheid vereisen van voorafgaand verlof voor (online) uitingen. Daarbij komt, dat de meerwaarde om burgers te verplichten tot een dergelijk uitgebreid rechtmatigheidsonderzoek bij iedere deepfake, uiterst twijfelachtig is. Immers, ook zonder een dergelijk uitgebreid rechtmatigheidsonderzoek kan in de meeste gevallen (eenvoudig) worden vastgesteld dat een deepfake in strijd is met de AVG.

Ten aanzien van de vraag omtrent een voorgestelde toets, door diverse partijen, om de authenticiteit van content te toetsen, verwijzen we naar de appreciatie van reguleringsoptie 7. Het verplichten van een dergelijke toets staat op gespannen voet met artikel 7 van de Grondwet.

---

[47] Een DPIA wordt ook wel een gegevensbeschermingseffectbeoordeling (GEB) genoemd.
[48] Data protection impact assessment (DPIA) | Autoriteit Persoonsgegevens.

Reguleringsoptie 12: Start een publiekscampagne met informatie over de gevaren van deepfakes, waarin nieuwe sociale normen worden geëxpliciteerd en best practices worden benadrukt.

We onderschrijven het belang om via voorlichting en communicatie de bewustwording over welk gedrag ontoelaatbaar en strafbaar is te bevorderen. Het maken van een seksuele deepfake is namelijk niet alleen ontoelaatbaar maar ook strafbaar. Misbruik van seksueel beeldmateriaal, zoals het heimelijk vervaardigen of het openbaar maken van seksueel beeldmateriaal in de wetenschap dat een ander hierdoor kan worden benadeeld, is strafbaar op grond van artikel 139h van het Wetboek van Strafrecht. In het kader van de implementatie van het wetsvoorstel seksuele misdrijven wordt aan een communicatieaanpak gewerkt waarmee bekendheid aan het wetsvoorstel en de normen die daaraan ten grondslag liggen wordt gegeven. Het bevorderen van bewustwording rondom pornografische deepfake kan hierin worden meegenomen. In dit verband zal zoveel mogelijk worden aangesloten bij de bredere publiekscommunicatie en overige voorlichtingsactiviteiten waar in het kader van het nationaal actieprogramma seksueel grensoverschrijdend gedrag en seksueel geweld, onder coördinatie van de Ministers van Onderwijs Cultuur en Wetenschap (OCW) en Sociale Zaken en Werkgelegenheid (SZW), aan wordt gewerkt en dat naar verwachting begin 2023 zal worden gepresenteerd. Doel van het nationaal actieprogramma is bijdragen aan het voorkomen van seksueel grensoverschrijdend gedrag en seksueel geweld en het bereiken van een samenleving waarin ieder zich veilig voelt en zichzelf kan zijn. De aanpak zet in op een cultuurverandering.

Waar het gaat over bewustwording van normatieve kader van de AVG heeft het kabinet, zoals ook staat in de Kabinetsbrief over de stand van zaken van de uitvoering Agenda horizontale privacy, in een campagne «Denk 2x na voor je iets deelt» gepleit meer bewustwording rondom het delen van beeld en informatie van anderen.[49] Deze campagne werd onderschreven door de Politie, SHN en de AP.

Waar het gaat om het helpen van slachtoffers van strafbare feiten waarbij deepfakes worden gebruikt, neemt het kabinet via verschillende lijnen actie. Zo zijn diverse slachtofferorganisaties, waar ook slachtoffers van bijvoorbeeld bepaalde pornografische deepfakes of discriminatoire deepfakes terecht kunnen. Daar worden slachtoffers op praktisch, juridisch en emotioneel gebied bijgestaan. Een voorbeeld hiervan is Helpwanted.nl, onderdeel van het Expertisebureau Online Kindermisbruik (EOKM). Helpwanted is een anonieme hulplijn waar jongeren en volwassenen terecht kunnen voor advies als zij te maken krijgen met online seksueel geweld, ook wanneer het gaat om deepfakes. Bewustzijn bij burgers over de mogelijkheid dat bepaald materiaal mogelijk deepfake is, is ook van belang bij de bestrijding van fraude. Daarom biedt de website slachtofferwijzer.nl informatie over de gevaren van deepfakes en hoe die te herkennen. Ook werkt de politie intern aan bewustwording en praktische handvatten voor de omgang met gemanipuleerd materiaal, nu en in de toekomst. In de keten wordt door de politie met onder meer het NFI, OM en het kenniscentrum Cybercrime (Rechtspraak) gewerkt aan bewustwording en handvatten. Verder heeft de politie mede de aanzet gegeven tot een Rijksbrede werkconferentie over de impact van synthetische media en deepfakes die in januari 2023 plaatsvindt en ingaat op diverse maatschappelijke en beleidsmatige vraagstukken.

[49] https://veiliginternetten.nl/denkvoorjedeelt/.

Waar het gaat over bewustwording van deepfakes in het kader van desinformatie, is het uitgangspunt dat de burger zelf informatie op waarde kan schatten. Om de burger daarbij te helpen, heeft het Netwerk Mediawijsheid met subsidie van het Ministerie van BZK de website www.isdatechtzo.nl opgezet, waar onder andere informatie is te vinden over hoe deepfakes werken en hoe ze kunnen worden herkend.

– Regulering van immersieve technologieën

De centrale vraag in het onderzoek naar regulering van immersieve technologieën is of de verwachte doorbraak van deze technologie dient te leiden tot aanpassingen van de bestaande reguleringskaders en wettelijke voorschriften en zo ja, op welke wijze. Daartoe bespreekt het onderzoek allereerst de kansen en de risico's van deze technologieën. Immersieve technologieën kennen veel waardevolle toepassingen waarmee wordt geëxperimenteerd. Gedacht kan worden aan toepassingen in het entertainment, de gezondheidszorg (in therapie bij de behandeling van pijn en psychische stoornissen), in het onderwijs en bij trainingen (om leersituaties na te bootsen), bij het voorkomen van recidive (gedragsverandering) en in de opsporing (het simuleren van de omstandigheden op een plaats delict).

Waar wel risico's van immersieve technologieën op de loer liggen, ziet het onderzoek de volgende thema's:

1. de strafrechtelijke normering van ongewenste gedragingen in virtuele werelden;
2. afleiding en gevaarzetting door het gebruik van immersieve technologieën;
3. de effecten van immersieve technologieën op mens en gedrag;
4. sociaal maatschappelijke veranderingen; en
5. misbruik van beelden van personen.

Uit het onderzoek komt naar voren dat het huidige juridische kader in algemene zin goed is toegerust om de eventuele negatieve effecten van immersieve technologie te adresseren.[50] Veel regelgeving is technologieneutraal geformuleerd en daarom ook van toepassing op immersieve technologieën. Benadrukt wordt daarbij wel dat immersieve technologieën op dit moment in geringe mate zijn geadopteerd en op hun effecten zijn onderzocht. De reguleringsopties die het onderzoek voorstelt, zijn er daarom grotendeels op gericht om de introductie van immersieve technologieën in de samenleving goed te begeleiden. Het is daarbij de vraag op welk moment reguleren wenselijk is om ontwikkelingen in goede banen te leiden. Te vroeg ingrijpen, kan een rem zetten op innovatieve ontwikkelingen. Te laat, maakt het ongedaan maken van ongewenste effecten moeizaam.[51] Daarom is in de onlangs aan uw Kamer aangeboden Werkagenda plaats ingeruimd voor het anticiperen op nieuwe digitale technologieën.[52] Er zal een beleidsagenda publieke waarden en nieuwe digitale technologie worden opgesteld met kaders voor de impact van deze technologie op publieke waarden. Daarbij worden kennisinstellingen, bedrijven en overheden betrokken.

Een verantwoorde begeleiding van de introductie van immersieve technologie is geen zaak voor Nederland alleen. Dit thema krijgt en verdient ook aandacht in internationaal en Europees verband. Zo heeft de Europese Commissie – in het kader van het Europese Media en Audiovisuele Actieplan – een *Virtual and Augmented Reality Industrial Coalition* geïnitieerd. Beleidsmakers en verschillende kleine, middelgrote en een paar dominante vaak niet-Europese marktspelers, gaan daarin met elkaar in gesprek over de kansen, de risico's en het beste beleid omtrent de introductie van immersieve technologieën. Ook hier worden belangrijke stappen gezet naar de ontwikkeling van ethische, duurzame en inclusieve

---

[50] *Regulering van immersieve technologieën,* p. 103 (WODC-onderzoek), bijlage bij Kamerstuk 26 643, nr. 778.
[51] D. Collingridge, *The Social Control of Technology*, New York: Frances Pinter, 1980.
[52] Kamerstuk 26 643, nr. 940.

VR/AR. De bescherming van (digitale) rechten en sociale waarden en bewustwording van gebruikers (van kansen en risico's) zijn daarin eveneens centrale thema's.

Hieronder bespreken we de conclusies en reguleringsopties zoals die, per thema, in het onderzoek worden voorgesteld.

1. De strafrechtelijke normering van ongewenste gedragingen in virtuele werelden

Het eerste thema in het onderzoek is dat individuen zich in een VR-omgeving op een onwenselijke of zelfs strafbare en laakbare manier kunnen (gaan) gedragen. Veel van deze gedragingen kunnen via het nu geldende strafrecht worden aangepakt. Denk aan belediging (artikel 266 Sr), bedreiging en belaging (artikel 285 en 285b Sr), en diefstal van virtuele goederen (artikel 310 Sr)[53] in een VR-omgeving. Bepaalde grensoverschrijdende gedragingen in een VR-omgeving zijn op dit moment echter niet als zodanig strafbaar. Het gaat dan om virtuele verkrachting, virtuele aanranding, virtuele mishandeling en virtueel vandalisme.

Het onderzoek legt de vraag voor of deze virtuele gedragingen een aparte (nieuwe) strafbaarstelling verdienen. Wij zien dat over het aantal slachtoffers van deze grensoverschrijdende gedragingen in de virtuele wereld op dit moment erg weinig bekend is, hetgeen uitvraag bij onder andere Slachtofferhulp Nederland (SHN) heeft bevestigd. Het onderzoeksrapport over immersieve technologieën zal daarom worden gedeeld met Slachtofferhulp Nederland (SHN), het Centrum Seksueel Geweld (CSG), het Expertisebureau Online Kindermisbruik (EOKM), en HelpWanted, om te bekijken of bestaande dienstverlening aan slachtoffers van zedenzaken moet worden aangepast.

Virtuele aanranding en verkrachting

Het onderzoek roept de vraag op of een (juridische) gelijkstelling van virtuele, seksueel gedreven gedragingen met fysieke, seksueel grensoverschrijdende gedragingen wenselijk is. Bij verkrachting en aanranding in de reële wereld knoopt de strafrechtelijke bescherming echter aan bij de fysieke aantasting van de lichamelijke integriteit. Daarvan is in een virtuele wereld geen sprake, omdat de seksueel gedreven gedragingen waar het om gaat, gericht zijn tegen een avatar en niet tegen een fysiek persoon. Een volledig vergelijkbaar en gelijkwaardig strafrechtelijk beschermingsniveau ligt dan ook naar onze mening niet in de rede.

Dat neemt niet weg dat tegen strafwaardige gedragingen in de virtuele wereld adequaat moet kunnen worden opgetreden. Centraal staat bij die gedragingen de schending van de vrijheid van eenieder om onbelemmerd als virtueel subject te verkeren. Seksueel gedreven gedragingen die hierop inbreuk maken, kenmerken zich in de regel dan ook veeleer als seksueel intimiderende gedragingen. De strafwet biedt op dit moment al mogelijkheden om tegen dergelijke gedragingen op te treden, bijvoorbeeld als sprake is van bedreiging (artikel 285 Sr). Het is denkbaar dat het virtueel verkrachten of aanranden van iemands avatar, bijvoorbeeld door de avatar van een persoon die het slachtoffer in werkelijkheid kent, een zodanige audiovisuele weergave betreft die bij die persoon de redelijke vrees kan doen ontstaan dat die gedraging ook zou worden gepleegd. De mogelijkheden om strafrechtelijk op te treden worden verder uitgebreid met het bij de Tweede Kamer aanhangige wetsvoorstel seksuele

[53] HR 31 januari 2012,ECLI:NL:HR:2012:BQ925 *(Runescape).*

misdrijven, waarin seksuele intimidatie van een ander in het openbaar in het nieuwe artikel 429ter strafbaar wordt gesteld.

Virtuele mishandeling

De onderzoekers concluderen dat er tegen virtuele mishandeling beperkt strafrechtelijk kan worden opgetreden. Om van mishandeling te kunnen spreken moet er volgens art. 300 van het Wetboek van Strafrecht sprake zijn geweest van fysieke pijn of letsel bij het slachtoffer. Daarvan zal in een virtuele wereld doorgaans geen sprake zijn. Artikel 300 Sr biedt echter ook aanknopingspunten voor vervolging van psychisch geweld. Met mishandeling wordt gelijkgesteld opzettelijke benadeling van de gezondheid. In de lagere rechtspraak zijn verschillende voorbeelden terug te vinden van gevallen waarin is geoordeeld dat het hierbij naast de fysieke gezondheid ook om de psychische gezondheid kan gaan (voornamelijk met betrekking tot mishandeling van kinderen). Het kabinet erkent dat slachtoffers van virtuele mishandeling psychische gevolgen kunnen ondervinden van deze gedragingen. Het kabinet stelt psychische mishandeling niet apart strafbaar.[54] Het Wetboek van Strafrecht biedt naast artikel 300 Sr ook andere mogelijkheden tot strafrechtelijke vervolging bij psychisch geweld: artikel 284 (dwang), 285 (bedreiging) en 285b (stalking). Indien virtuele mishandeling (ernstig) psychisch trauma tot gevolg heeft, of gepaard gaat met dwang, bedreiging of stalking, dan biedt het Wetboek van Strafrecht grond voor vervolging. Daarbij komt dat de schade die door virtuele mishandeling wordt veroorzaakt reeds op de dader kan worden verhaald als er daarbij sprake is van een onrechtmatige daad.

Virtueel vandalisme

De onderzoekers geven aan dat gedragingen die kwalificeren als virtueel vandalisme momenteel niet of beperkt strafrechtelijk gesanctioneerd zijn. Het gaat dan bijvoorbeeld om het in AR aanbrengen van aanstootgevende content op daadwerkelijke fysieke locaties. Daardoor zouden mensen, bijvoorbeeld als zij zich door een fysieke stad bewegen, in AR op bepaalde fysieke locaties die virtuele content geprojecteerd kunnen zien. Er is in dit verband wel gesproken van een «hybride openbare ruimte, waarin fysiek en virtueel in elkaar overvloeien».[55] Het WODC-onderzoek stelt de vraag of virtueel vandalisme een aparte strafbaarstelling verdient.

Op basis van de delictsomschrijving van artikel 350, eerste lid, Sr (beschadiging goederen) is het erg moeilijk om virtueel vandalisme als vernieling te kwalificeren, nu er geen sprake is van schade aan een object of een verlies aan bruikbaarheid. Op grond van de onrechtmatige daad (6:162 Burgerlijk Wetboek (BW)) biedt het civielrecht echter voldoende mogelijkheden om op te treden tegen dergelijke gedragingen. Ook zijn er gevallen denkbaar waarin virtueel vandalisme de vorm aanneemt van beledigende of discriminerende uitlatingen. In die gevallen kan op grond van de artikelen 137c (belediging groep mensen) en 266, eerste lid, Sr (eenvoudige belediging) worden opgetreden tegen virtueel vandalisme. Het projecteren van aanstootgevende virtuele beelden op een fysieke locatie met behulp van AR kan mogelijk ook strafbaar zijn op grond van artikel 240 Sr (verspreiding pornografische geschriften). Daarom zien wij op dit moment geen aanleiding om virtueel vandalisme als zodanig apart strafbaar te stellen.

---

[54] Kamerstuk 28 345, nr. 260

[55] D. Snijders e.a., *Nep echt: Verrijk de wereld met augmented reality*. Den Haag, Rathenau Instituut 2020.

AR-naaktfilters

Met een «naaktfilter», zoals de term in het onderzoek wordt gebruikt, wordt een deepfake-filter bedoeld die een aangeklede persoon op beeldmateriaal «virtueel» kan ontkleden. De onderzoekers stellen de vraag of het gebruik van naaktfilters in AR strafbaar moet worden gesteld. Zoals hierna nog zal worden toegelicht in de beleidsreactie naar aanleiding van het WODC-onderzoek naar regulering van deepfakes (bij reguleringsoptie 1), stelt artikel 139h, eerste lid, sub a, Sr strafbaar het opzettelijk en wederrechtelijk van een persoon vervaardigen van afbeeldingen van seksuele aard. Dit betekent dat ook het vervaardigen van afbeeldingen van seksuele aard met behulp van een AR-naaktfilter in voorkomende gevallen strafbaar kan zijn. Een aparte strafbaarstelling van naaktfilters is daarvoor niet noodzakelijk.

2. Afleiding en gevaarzetting door het gebruik van immersieve technologieën

Door een AR-bril kan de «reële wereld» worden waargenomen, aangevuld met de digitale inhoud die aan de binnenkant van de glazen worden weergegeven. Het onderzoek stelt dat tegen gevaarzettend gedrag door het gebruik van immersieve technologieën zoals AR-brillen in het verkeer, slechts ten dele kan worden opgetreden.

Artikel 61a Reglement Verkeersregels en Verkeerstekens 1990 (RVV 1990), ook wel het smartphoneverbod genoemd, bepaalt dat bestuurders van voertuigen tijdens het rijden geen mobiel elektronisch apparaat mogen «vasthouden»; het «dragen» van een AR-bril valt daar dus niet onder. Tegen risicovolle gedragingen met apparatuur die niet wordt vastgehouden, kan – zoals het onderzoek ook opmerkt – echter worden opgetreden met de algemene gevaarzettingsbepaling van artikel 5 van de Wegenverkeerswet 1994 (WVW 1994). Ook het onveilig gebruik van een AR-bril of een *smartwatch* in het verkeer kan zo worden geadresseerd. In de onlangs aan de Kamer aangeboden evaluatie van artikel 61a RVV 1990 bleek de politie in de praktijk goed uit de voeten te kunnen met de huidige wet.[56]

Het kabinet ziet op dit moment geen signalen van een ontwikkeling naar het gebruik van *smart-glasses* in het verkeer. Wel is er een nieuwe trend van het gebruik van *AR in-car*-systemen. Deze systemen kunnen bijdragen aan het verbeteren van de verkeersveiligheid, bijvoorbeeld door verkeersgerelateerde informatie aan te bieden op een manier die niet afleidt, maar gaan ook gepaard met risico's. In deze fase ziet het kabinet dat de industrie zich bewust is van de risico's en dat daarmee bij de ontwikkeling van immersieve technologieën op een verantwoordelijke manier rekening wordt gehouden. Er worden met deze industriepartijen gesprekken gevoerd over wat voor type waarschuwingen bij welk urgentieniveau passen. Hierbij wordt tevens gewaakt voor eventuele risico's voor de verkeersveiligheid. Het kabinet volgt de ontwikkelingen en zoekt daarbij de samenwerking op met partijen als NLdigital (voorheen Nederland-ICT).

3. Effecten van immersieve technologieën op mens en gedrag

Er wordt breed ingezet op preventie en voorlichting van problematisch gebruik van games en digitale media door middel van de Gamen Infolijn en het programma Helder Op School van het Trimbos-instituut. Bij het programma Helder Op School wordt de focus gelegd op de digitale balans, waarbij kinderen al vroeg wordt geleerd om op een gezonde

[56] Kamerstuk 29 398, nr. 998.

manier om te gaan met digitale media. Deze proactieve aanpak waarbij wordt ingezet op preventie, is in lijn met eerdere onderzoeken van het WODC en het Trimbos-Instituut.[57] Het advies uit het voorliggende onderzoek is om in te zetten op nader onderzoek, voorlichting en bewustwording, wordt onder meer meegenomen bij activiteiten die het Trimbos-instituut met subsidie van het Ministerie van Volksgezondheid Welzijn en Sport (VWS) uitvoert. Het kabinet blijft alert of nieuwe ontwikkelingen die regelgeving vereisen en zal daar indien nodig op acteren.

4. Sociaalmaatschappelijke veranderingen

Het onderzoek benadrukt dat de lange-termijn sociaalmaatschappelijke gevolgen van immersieve technologieën op dit moment nog ongewis zijn. De vraag is onder meer hoe deze technologieën van invloed zullen zijn op waarden zoals waarachtigheid en vertrouwen en de omgang tussen mensen. In dit licht schenkt het onderzoek aandacht aan het fenomeen «hyperpersonalisatie». Bedoeld wordt daarmee dat gebruikers door middel van immersieve technologieën «hyperpersoonlijke» inhoud kan worden aangeboden die zeer sterk is aangepast aan de persoonlijke gegevens, biometrische gegevens en de voorspelde voorkeuren en interesses van de gebruiker.

In reactie op het vraagstuk over hyperspersonalisatie, kan worden verwezen naar de bescherming die huidige en toekomstige regelgeving daartegen biedt. Zoals het onderzoek beklemtoont, beschermt de AVG gezien de technologie-onafhankelijke redactie ervan goed tegen gebruik of misbruik van persoonsgegevens door middel van immersieve technologieën. Daarnaast kan worden gewezen op de DSA, die in 2024 in werking treedt. In die verordening wordt aan online platformen (die ook immersieve technologieën kunnen aanbieden) een verbod opgelegd op het gebruiken van gegevens van minderjarigen en van bijzondere persoonsgegevens (zoals biometrische data) van alle gebruikers om gepersonaliseerde advertenties te tonen. Dit is relevant omdat VR- en AR-toepassingen veel biometrische data kunnen verzamelen, zoals oog- en lichaamsbewegingen. Ook bevat de DSA extra waarborgen tegen onbewuste beïnvloeding bij digitale diensten en voor meer keuze en transparantie in online omgevingen. Zo moeten gebruikers de mogelijkheid krijgen om de diensten van zeer grote online platformen en zoekmachines te gebruiken zonder dat die gepersonaliseerd worden op basis van data over een gebruiker. Dit maakt de invloed van die personalisatie transparant en kan eraan bijdragen dat mensen ook in aanraking komen met informatie van buiten hun bubbel.

5. Misbruik van immersieve technologieën door derden

Zoals alle (nieuwe) technologieën, kunnen ook immersieve technologieën worden misbruikt. De onderzoekers leggen daarom de vraag voor of impersonatie moet worden verboden. Er zijn echter reeds ruimschoots middelen om via het gegevensbeschermingsrecht, het civiele recht en het strafrecht om tegen misbruik van beelden van personen op te treden.[58] Impersonatie met onrechtmatige doelen zoals oplichting is, ook volgens het onderzoek, via het strafrecht goed aan te pakken. Dit wordt bevestigd door het OM. Impersonatie in het algemeen kan bovendien vele doeleinden dienen en wordt zeker niet altijd negatief gewaardeerd. Ook onschuldige vormen van impersonatie – het onderzoek noemt het voor de gek houden van familie en vrienden – zouden met een algemeen

[57] Kamerstuk 26 643, nr. 948; Kamerstuk 24 557, nr. 180.
[58] Kamerstuk 26 643, nr. 815.

impersonatieverbod verboden worden. Een verbod op impersonatie maakt bovendien een forse inbreuk op rechten en vrijheden zoals het recht op vrijheid van meningsuiting en het recht op eerbiediging van het privéleven. Er moeten daarom gewichtige redenen zijn om impersonatie als zodanig te verbieden. Wij zien deze gewichtige redenen niet op dit moment.