

Jaargang 10
Editie 1
2023/2024

ONLINE MISLEIDING

E-MAGAZINE



LISA Law & ICT
Students' Association

- 04** Rechten van de Gedeeptakete
persoon
- 08** Interview met advocaat mr.
H. Ellemers
- 13** Regulering en handhaving van
online desinformatie
- 16** Een blik op de nieuwe Digital
Services Act en Digital Markets Act

VOORWOORD

Beste lezer,

In een tijd dat het internet grenzeloos lijkt, vervaagt de grens tussen realiteit en fictie. De opkomst van deepfakes en online desinformatie compliceert de belangrijkste fundamenteën van betrouwbaarheid. Hoe kan de oplettende internetgebruiker zich hedendaags nog beschermen tegen onmerkbare illusies en valstrikken?

In dit e-magazine onderzoeken wij deze wereld van online misleiding. We kijken naar de rechten van de slachtoffers van deepfakes, wiens identiteit gebruikt wordt als schijn in een spel van digitale manipulatie. We kijken naar desinformatie die de mening en wil van de overheid en Nederlanders pal tegenover elkaar zet. We diepen in de Digital Services Act (DSA) en de Digital Markets Act (DMA). Zij beloven een omwenteling teweeg te brengen in hetgeen online platformen nu nog onbegrensd lijken te mogen doen, maar leveren deze verordeningen een veilige online omgeving op?

In september heeft zich een nieuwe commissie gevormd genaamd de Carrièrecommissie, die het werk van de redactiecommissie zal overnemen. Afgelopen tijd is er hard gewerkt gewerkt aan het creëren van een e-magazine omtrent de wereld van misleiding en bedreiging op het internet. Ik wil mijn commissie bedanken voor hun inzet en toewijding de afgelopen weken. Met trots presenteren wij het eerste E-magazine van het collegejaar 2023-2024: 'Online Misleiding'.

Ik wens de lezer veel leesplezier en hoop dat de stukken wellicht wat houvast kunnen geven in de grenzeloze wereld van de online misleiding.

Namens de Carrièrecommissie,

Esther Bergsma
Voorzitter

- **Voorzitter** Esther Bergsma
- **Secretaris** Manon Hospers
- **Hoofdredacteur** Chris Truong
- **Commissaris extern** Roos den Boogert
- **Commissaris Promotie** Nathan Porsoufi



NORD

Rechten van de Gedeepfake te persoon

Op het internet circuleert een welbekend videoclipje van voormalig president Barack Obama waarschuwend voor het gevaar van deepfakes. Ter versterking van het betoog blijkt echter dat de voormalige president deze uitspraken nooit heeft gedaan; het betrof een deepfake. Dat het risico van deepfakes eveneens doordringt tot de Nederlandse rechtsorde, manifesteert zich overtuigend in een strafzaak van afgelopen november. De rechtbank Amsterdam oordeelde dat een verspreide wraakporno video, vervaardigd middels een deepfake, valt onder de reikwijdte van artikel 139h van het Wetboek van Strafrecht (hierna Sr).¹ Dit is uiteraard een ruime en interessante interpretatie, gezien het feit dat een deepfake in beginsel een fictieve creatie is en het slachtoffer van de deepfake niet feitelijk aanwezig is in de video.

We kunnen uit dit actuele voorbeeld opmaken dat deepfakes een nieuwe frontier openen in de maatschappij. Ook de Nederlandse rechtsorde blijft niet ongedeerd. Het is van essentieel belang te begrijpen dat deepfakes een verfijnde manipulatie vertegenwoordigen, waarmee de grenzen tussen realiteit en fictie op subtiele wijze worden vervaagd. Dit roept een cruciale vraag op: welke stappen kunnen belanghebbenden ondernemen als 'slachtoffer' van een ongewenste deepfake jegens de publicist/maker? Ten eerste zal kort uitgelegd worden wat een deepfake inhoudt. Ten tweede zullen wij pogen de hiervoor gestelde onderzoeksvraag te beantwoorden vanuit een analyse van twee juridische invalshoeken: het auteursrecht middels het portretrecht en het privacyrecht. Wij blijven in dit artikel binnen het kader van wat een slachtoffer kan ondernemen tegen een ander private persoon krachtens het privaatrecht. Wij laten daarom het strafrecht voor wat het is.

Definiëring deepfake

Wat verstaan we precies onder deepfakes? Diep vervalste mediaproducties, beter bekend als deepfakes, representeren geavanceerde kunstmatige creaties die voortkomen uit de symbiose van deep learning en vervalsing. In essentie zijn deepfakes gemanipuleerde beelden, geluiden, of een combinatie van beide, die

dankzij kunstmatige intelligentie (AI) worden gegenereerd. Deze manipulaties resulteren in realistische visuele en auditieve ervaringen, waarbij doorgaans een identificeerbaar persoon wordt gepresenteerd die handelingen uitvoert of uitspraken doet die in werkelijkheid niet hebben plaatsgevonden. De totstandkoming van deepfakes berust op deep learning, een moderne technologische benadering die haar fundament vindt in de complexiteit van menselijke neurale netwerken. Door middel van dit proces wordt een computermodel getraind om autonoom patronen te herkennen in uitgebreide datasets, bijvoorbeeld de wijze waarop een menselijke mond beweegt wanneer hij/zij bepaalde woorden uitsprekt. Het resultaat is het produceren van bedrieglijk authentieke creaties.



Portretrecht

Het gaat voor de reikwijdte van dit artikel te buiten om uitvoerig in te gaan op de auteursrechtelijke status van deepfakes. Wij zullen in dit stuk volstaan met een verwijzing naar de conclusie van Trouborst, Vrendenbarg en Visser, die tot de conclusie zijn gekomen dat een deepfake in beginsel te kwalificeren is als een auteursrechtelijk beschermd werk.²

¹ Rb. Amsterdam 2 november 2023, IEF 21758, IT 4418; ECLI:NL:RBAMS:2023:6923.

² Trouborst, Vrendenbarg & Visser, *NJB* 2022/93, p. 101-110.

Daarmee is het uiteraard nog geen vrij spel voor een deepfake. Het portretrecht van artikel 21 Auteurswet (hierna: Aw) gooit mogelijk zand in de machine, als beperking van het auteursrecht. Met een beroep op het portretrecht kan een geportretteerde met een redelijk belang zich verzetten tegen de openbaarmaking van het portret. Dit zou tot gevolg kunnen hebben dat een gedeeptefakte persoon zich met deze route kan verzetten tegen een publicatie van een deepfake.

Is een deepfake een portret?

De eerste vraag die we in dit kader moeten beantwoorden, is of een gedeeptefakte persoon kan worden gekenmerkt als 'geportretteerde' als bedoeld in artikel 21 Aw. De literatuur beantwoordt bevestigend: het hiervoor genoemde trio van auteurs schrijven dat indien een deepfaketechniek doelbewust wordt ingezet om een specifiek bestaande persoon te genereren, er inderdaad sprake is van een portret in de zin van artikel 21 Aw.³ Wij sluiten aan bij het standpunt dat een deepfake kan worden gekwalificeerd als portret. Dit valt onzes inziens af te leiden uit onder andere het Max Verstappen/PicNic-arrest.⁴ De rechtspraak heeft bevestigd dat ook het gebruik van 'lookalikes' in plaats van de personen die worden geïmiteerd, zoals het geval was in Max Verstappen/PicNic, nog steeds kan leiden tot een portret in de zin van artikel 21 Aw. Dit betekent dat een deepfake ook in beginsel leidt tot een portret, aangezien ook hier een bestaand persoon wordt geïmiteerd.

Wat betreft het vereiste van doelbewuste opzet, kunnen wij volstaan met een verwijzing naar het arrest Portret Millecam.⁵ Hierin had de rechter geconcludeerd dat een toevallig onbewuste gelijkenis onvoldoende is om van een portret te spreken in de zin van artikel 21 Aw. Het moet dus in de bewuste deepfake wel om de desbetreffende persoon gaan, en niet om iemand die er toevallig op lijkt.

3 Idem.

4 HR 22 april 2022, ECLI:NL:HR:2022:621 (Max Verstappen/PicNic).

5 Rb. Amsterdam (pres.) 22-12-1994, ECLI:NL:RBAMS:1994:AK2163 (Portret Millecam).

Redelijk belang van een gedeeptefakte persoon

Uit de rechtspraak volgen vele voorbeelden waaruit blijkt dat het vereiste van een redelijk belang om het portretrecht in te kunnen roepen breed wordt uitgelegd. Bijvoorbeeld een louter financieel/commercieel belang van een geportretteerde met een verzilverbare populariteit kan worden aangemerkt als een redelijk belang.⁶ Andere aspecten die meespelen zijn de bekendheid van de geportretteerde persoon: een onbekend persoon kan zich al snel verzetten tegen het commercieel gebruik van zijn portret dat zonder toestemming is gemaakt.⁷

Echter, Trouborst, Vrendenburg & Visser betogen dat in het geval van misleidende deepfakes er al snel sprake is van een redelijk belang van een geportretteerde, waardoor de hiervoor genoemde 'traditionele' redelijke belangen niet toegepast hoeven te worden. De schrijvers betogen dat alle personen ongeacht hun bekendheid in beginsel het redelijk belang hebben om niet misleidend dan wel verwarrend geportretteerd te worden middels een deepfake.⁸ Zij berusten dit argument op het feit dat misleidende deepfakes in principe van rechtswege schade toebrengen op het moment dat deze persoon wordt herkend. De dusdanig schadelijke gevolgen zouden volgens de auteurs rechtvaardigen dat het portretrecht een karakter krijgt van een absoluut verbodsrecht waarmee de geportretteerde zich kan verzetten tegen de deepfake.⁹ Indien de rechtspraak deze interpretatie van artikel 21 Aw volgt, zou dit leiden tot een nieuw precedent omdat het portretrecht tot op het heden altijd het karakter van een absoluut verbodsrecht heeft vermeden wegens de belangenafwegingen die dienen plaats te vinden in het kader van het bepalen of sprake is van een redelijk belang.¹⁰

De soep wordt echter niet zo heet gegeten. Trouborst, Vrendenburg en Visser continueren hun betoog door te wijzen op een aantal bijzondere

6 HR 19 januari 1979, ECLI:NL:HR:1979:AC6461, *NJ* 1979/383, m.nt. L. Wichers Hoeth ('t Schaep met de Vijf Pooten).

7 HR 2 mei 1997, ECLI:NL:HR:1997:ZC2364 (Disco-danser).

8 Trouborst, Vrendenburg & Visser, *NJB* 2022/93, p. 101-110.

9 Idem.

10 Geerts 2023, p. 84.

uitzonderingen die gehanteerd dient te blijven op dit verbodsrecht.¹¹ Zo zou bijvoorbeeld de parodie-exceptie gehanteerd blijven in het geval van duidelijk herkenbare parodieën, en kan de vrijheid van meningsuiting desalniettemin prevaleren.¹² Echter blijft de conclusie dat artikel 21 Aw een zeer sterk bescherming geeft aan slachtoffers van een deepfake portret.



Privacyrecht

Allereerst verdient de opmerking dat ook portretten in de zin van artikel 21 Aw onder de bescherming kunnen vallen van de Algemene Verordening Gegevensbescherming (hierna: AVG). Echter, de heersende consensus in de literatuur lijkt te zijn dat deze bescherming vanuit het privacyrecht weinig aanvulling geeft op de bescherming die al bestaat op grond van het portretrecht.¹³ Voor dit artikel zullen wij met deze observatie met betrekking tot het overlappende gebied tussen het privacyrecht en het portretrecht laten rusten.

Bredere reikwijdte

Het portretrecht lijkt als zodanig dus een sterke positie te geven aan het slachtoffer van een deepfake, maar dit kan toch tot teleurstelling leiden. Het portretrecht van artikel 21 Aw stuit tegen een belangrijk probleem aan: de beperkte reikwijdte. Er dient sprake te zijn van een herkenbaar gelaat van een persoon.¹⁴ Deepfakes zijn er

echter in allerlei soorten, waardoor ze niet allemaal onder het portretrecht vallen. Dit betekent dat het portretrecht geen soelaas zou kunnen bieden aan het slachtoffer. Deepfakes kunnen immers veel meer produceren dan slechts visuele beelden, maar bijvoorbeeld ook auditieve voice clones waarmee een stem van een bestaand persoon als ware wordt gekopieerd. Een dergelijke creatie valt uiteraard niet onder de definitie van artikel 21 Aw, waardoor het portretrecht geen soelaas biedt.

In dergelijke situaties lijkt een beroep op de Algemene Verordening Gegevensbescherming (hierna: AVG) voor de hand te liggen.¹⁵ De AVG biedt immers volgens artikel 1 lid 1 in juncto met artikel 4 lid 1 AVG bescherming tegen de verwerking van alle persoonsgegevens waarmee een natuurlijke persoon kan worden geïdentificeerd. Deze wettelijke terminologie is dus breder dan de reeds besproken definitie van een portret in de zin van het portretrecht. Dat betekent dat bijvoorbeeld stemfragmenten van een persoon ook worden beschermd als persoonsgegevens.¹⁶ Volgens de literatuur kan hieruit worden opgemaakt dat auditieve deepfakes in de vorm van een stem van een bestaand persoon ook onder diezelfde reikwijdte valt.¹⁷

Deepfakes als verwerking van persoonsgegevens

Artikel 4 lid 2 AVG geeft een zeer brede definitie van de term 'verwerken' van persoonsgegevens. Onder meer het opslaan en gebruiken van persoonsgegevens vallen hieronder. Dit betekent dat het genereren en verspreiden van deepfakes waarin een identificeerbaar natuurlijk persoon te zien is, in beginsel wordt gereguleerd door de AVG.¹⁸ Dit biedt het slachtoffer van een deepfake een breed pakket aan beschermingsmiddelen die onder andere vloeien uit artikel 6 AVG. Bijvoorbeeld dat een geldige rechtsgrond is vereist voor de verwerking van persoonsgegevens. Er kan dan worden gedacht aan het vereiste van

11 Trouborst, Vrendenbarg & Visser, *NJB* 2022/93, p. 101-110.

12 Idem.

13 Vreeling, *IER* 2021/29, p. 276-283; Trouborst, Vrendenbarg & Visser, *NJB* 2022/93, p. 101-110.

14 HR 30 oktober 1987, ECLI:NL:PHR:1987:AD0034 (Naturistengids).

15 Trouborst, Vrendenbarg & Visser, *NJB* 2022/93, afl. 2, p. 101-110.

16 Rb. Midden-Nederland 9 januari 2020, ECLI:NL:RBMNE:2020:24, *AMI* 2020/3-4, m.nt. A.M. van Aerde (Stemfragment).

17 Trouborst, Vrendenbarg & Visser, *NJB* 2022/93, afl. 2, p. 101-110.

18 Idem.

een ondubbelzinnige toestemming van de identificeerbare persoon die wordt gedeepfake. Zonder deze toestemming is in beginsel sprake van een onrechtmatige verwerking van persoonsgegevens. Er kan in dat geval door de betrokkene handhavend worden opgetreden door bijvoorbeeld het recht op vergetelheid als bedoeld in artikel 17 AVG in te roepen.

Wel moet in het achterhoofd worden gehouden dat ook in het privacyrecht de fundamentele rechten van de producent/publicist van de deepfake een rol kunnen spelen met een belangenafweging ten gevolge, zo blijkt uit artikel 6 lid 1 sub f AVG.

Conclusie

De De definitie van deepfakes, als geavanceerde kunstmatige creaties voortkomend uit deep learning en vervalsing, onthult de verfijnde manipulatie die de grenzen tussen realiteit en fictie subtiel doet vervagen. In het bijzonder hebben juristen die geen achtergrond in techniek hebben, de taak om te begrijpen dat deepfakes verder gaan dan slechts fictieve creaties; zij introduceren een nieuw spectrum van juridische vraagstukken. In het kort kunnen wij concluderen dat een slachtoffer van een deepfake diverse invalshoeken heeft waarop hij of zij zich kan beroepen.

Binnen het auteursrecht, ondanks het feit dat deepfakes potentieel als auteursrechtelijk beschermd werk kunnen worden beschouwd, biedt het portretrecht (artikel 21 Aw) een interessante invalshoek voor het slachtoffer om verzet aan te tekenen tegen de publicatie van een deepfake. De kwestie van herkenbaarheid en het redelijk belang van het geportretteerde individu spelen hierbij een essentiële rol. Wij constateren dat er geluiden binnen de literaire cirkels bestaan die van mening zijn dat een dergelijk redelijk belang van rechtswege sprake is in het geval van misleidende deepfakes. Het portrecht zou in dit kader zelfs een absoluut verbodsrecht zijn. Wel zou er nog ruimte bestaan voor uitzonderingen in bijzondere gevallen in het kader van de vrijheid van meningsuiting.

Het privacyrecht, specifiek de AVG, breidt de bescherming uit naar alle persoonsgegevens waarmee een natuurlijke persoon kan worden geïden-

tificeerd. Dit omvat niet alleen visuele beelden maar ook auditieve aspecten zoals stemfragmenten, die niet vallen onder de reikwijdte van het portretrecht. Hierdoor ontstaat een breder arsenaal aan beschermingsmiddelen voor slachtoffers, waaronder het vereiste van geldig rechtsgrond voor de verwerking van persoonsgegevens en het recht op vergetelheid. Maar ook hier geldt dat uitzonderingen op zijn plaats kunnen zijn, bijvoorbeeld in het geval van een prevalerende vrijheid van meningsuiting van de publicist/producent van de deepfake.

In de complexe wereld van deepfakes dienen juristen zich bewust te zijn van de gelaagde juridische aspecten, en het voorgestelde juridische onderzoek biedt een eerste stap naar het begrijpen en aanpakken van de uitdagingen die deze technologische revolutie met zich meebrengt. Het pad naar een adequaat juridisch kader voor deepfakes is een voortdurende en evoluerende reis, waarbij de bescherming van individuen tegen deze vorm van digitale manipulatie een centrale rol moet spelen in de voortdurende ontwikkeling van het rechtssysteem.

Namens de Carrièrecommissie,

Chris Truong.

Een interview met mr. H. (Hester) Ellemers



Hester Ellemers is advocaat bij TRIP. Ze is gespecialiseerd in het intellectuele eigendomsrecht, privaatrecht en ICT-recht. In Groningen heeft ze zowel de bachelor als master IT-recht gevolgd.

Kunt u misschien wat over uw studieverloop vertellen?

Ik heb de bachelor IT-recht in drie jaar afgerond. Ik vond het wat snel gaan en heb toen een tussenjaar genomen. In dit tussenjaar heb ik drie stages gelopen. Waarvan twee in het noorden, waaronder bij TRIP, en eentje op de Zuidas bij De Brauw Blackstone Westbroek. Ik stond voor een dilemma: welke master ga ik doen? Uiteindelijk kreeg ik tijdens mijn stages te horen: het maakt niet uit welke master je kiest, als je cijfers maar goed zijn. Ik heb daarom gekozen voor wat mij het leukste leek: IT-recht. Vervolgens kwam corona, ik ben toen hard gaan werken om mijn scriptie af te ronden en aan het werk te kunnen. Studeren was toch niet meer hoe ik het gewend was.

Zowel in het noorden als op de Zuidas heeft u stage gelopen. Kunt u ons meer vertellen over de verschillen tussen advocatenkantoren op de Zuidas en het noorden?

Op de Zuidas is het ontzettend leuk dat je constant werkzaam bent voor bekende bedrijven. De grote namen zitten vaak bij deze kantoren. Dat sprak mij heel erg aan. Minder leuk vond ik dat je zelf weinig daadwerkelijk voor de cliënt doet. Je moet al veel ervaring hebben, voordat je zelf zaken oppakt of contact hebt met de cliënt. In het noorden krijg je sneller meer verantwoordelijkheden. Al snel krijg je je eigen dossiers. Ik heb wel serieus getwijfeld. Het hangt ervan af waar je passie ligt, denk ik. Wil je heel juridisch overal diep induiken; alles tot de puntjes uitzoeken of wil je een dossier behandelen?

En waarom heeft u uiteindelijk toch gekozen voor een kantoor in het noorden?

Ik was al werkzaam bij TRIP op de sectie IE-recht en IT-recht en vond het een ontzettend leuk kantoor. Het is inmiddels alweer twee jaar geleden dat ik fulltime in dienst ging. Het beviel mij heel goed bij TRIP: de sfeer met de collega's is goed en ik kom ook uit het noorden. Uiteindelijk heb ik de keuze gemaakt om te blijven.

U heeft de master IT-recht gevolgd. Is de master een goede aansluiting op de praktijk? Word je in het diepe gegooid? En heeft u nog een tip voor de beginnende masterstudent IT-recht?

Je wordt in het diepe gegooid. Dat ligt alleen niet aan de master IT-recht. Dat vloeit voort uit de rechtenstudie ten opzichte van het daadwerkelijk werkende leven. Daarom raad ik het ontzettend aan om stage te lopen. Zo leer je bedrijven kennen en kom je erachter wat het werk inhoudt. En of je het leuk vindt. Ook bij verschillende bedrijven. Zo leer je wat voor kantoor bij je past. Daarnaast hoeft je niet per se advocaat te worden met deze master. Als ik naar studenten kijk in mijn tijd, doet iedereen van alles en nog wat. Het voelt misschien of je met IT-recht een hele specifieke richting kiest, wat soms ook spannend kan zijn. Alleen ons vak wordt steeds groter en belangrijker. Daarom heb ik nooit gedacht: 'Had ik me maar breder opgeleid.'

IT-recht is een vrij niche opleiding. Nog geen 100 mensen doen de master in Groningen. Is er veel concurrentie op de arbeidsmarkt als IT-jurist?

Het worden er uiteraard steeds meer. In Amsterdam heb je nu ook de master informatierecht en volgens mij zelfs in Nijmegen. De bachelor IT-recht heb je echter nergens anders. Wat betreft de concurrentie hangt het ervan af waar je naartoe wilt. Een groot deel van de masterstudenten in Amsterdam wil waarschijnlijk in de stad en op de Zuidas werken. Ik kan mij voorstellen dat daar meer concurrentie is. Naar het noorden gaan is voor veel mensen een bewuste keuze. Maar concurrentie is er in elk rechtsgebied.

Recent is er ophef ontstaan over de bekende cromptouce, U bent zelf gespecialiseerd in het IE-recht. Om alvast vooruit te lopen op de zaken. Wat is uw juridische mening over de cromptouce? Kan het beschermd worden door het IE-recht?

Ik heb mij er niet in verdiept, dus ik heb daar geen mening over. Echter heb ik wel het nodige op internet voorbij zien komen, dus mijn antwoord kan ik puur daarop baseren. Volgens mij is er überhaupt onduidelijk wie het heeft bedacht. Is het beschrijvend voor de aard van het product? Zou het merkenrecht standhouden? Ik denk wel dat het mooi is dat je ziet wat een merkregistratie doet. Iemand registreert het gewoon een keer en ik las dat de Jumbo de term al niet meer gebruikt. Wat dat betreft, is het altijd slim om iets te registreren als je ermee bezig bent.

Wat zijn onderwerpen waar u veel mee te maken heeft binnen het IE-recht?

Dat is super divers. Ik doe IE-recht, maar ook ICT-recht en privacy. Die afwisseling vind ik ook leuk. ICT-zaken zijn vaak langdurige trajecten met een cliënt, terwijl IE vaak acuter is. In de meeste gevallen, zo niet altijd, heb je een spoedeisend belang op het moment dat de sommatiebrief ofwel wordt verstuurd ofwel wordt ontvangen. Bij IE zijn de zaken ook divers. Vaak auteursrecht op producten, merkenrecht, modellenrecht en IE-recht op software. Octrooirecht doen we wat minder.

Doen jullie wellicht octrooirecht minder doordat deze worden behandeld door het westen van het land?

Octrooirechtzaken worden vaak behandeld door nichekantoren. Dit betreffen niet per se de Zuidas-kantoren. Vanwege de technische aard van deze zaken zie je dat er gezocht wordt naar kantoren met specialistische kennis. Het komt ook vaak voor dat octrooibureaus hun eigen advocaten of juristen in dienst hebben.

Heeft u nog een favoriet onderwerp?

Ik vind ICT-zaken heel erg leuk, omdat ik de cliënten dan zo goed leer kennen. Je hebt een langdurige relatie. Met een IE-zaak kan het zo zijn dat je elkaar alleen op een scherm hebt gezien. Dat is natuurlijk niet erg, maar met ICT-zaken duurt het vaak zo lang dat je toch met elkaar aan de tafel komt en vaak onderhandelingen hebt. Dat spreekt mij enorm aan.

In ons magazine gaan we onder andere in op deepfakes en andere vormen van online zaken. Ook deepfakes kunnen mogelijk een inbreuk maken op het IE-recht. Heeft u toevallig al te maken gehad met zaken met betrekking tot deepfakes of andere content gegenereerd door kunstmatige intelligentie?

Ik heb hier nog niet eerder mee te maken gehad op kantoor. Hoewel AI opkomt, is het allemaal nog onduidelijk. Daarom merk je ook dat mensen nog niet daadwerkelijk actie ondernemen. Bovendien heb je de AI-verordening, die eraan komt maar nog niet in werking is.

Heeft u zelf al een mening over de ontwikkeling dat AI steeds dominanter wordt in onze samenleving?

Lastig. Aan de ene kant zie ik dat het natuurlijk veel waarde heeft. Aan de andere kant is het een grijs gebied. Persoonlijk merk ik dat ik het nog nauwelijks gebruik, aangezien ik er nog niet op durf te vertrouwen. Als ik het gebruik is het meer voor de grap, om te kijken wat eruit rolt. Ik zou het op dit moment niet in combinatie met mijn werk gebruiken. Ik heb de app ook nog maar twee maanden. Het voelt toch wat spannend, vooral omdat je niet precies weet wat er met je gegevens gebeurt en waar het naartoe gaat.

De AI-verordening dreigt te worden afgezwakt door onder andere lobbyisten uit Duitsland, Frankrijk en Italië. Vanuit uw ogen als een IT-jurist, maakt u zich zorgen over de juridische ontwikkeling van AI?

Vooralsnog maak ik mij er geen zorgen over. Wat mij betreft moet er duidelijkheid komen en een meer uniform beleid gelden. Nederland loopt ook niet voorop met AI heb ik het idee. We moeten het wel in de gaten houden en er moeten afspraken worden gemaakt, het liefste zonder lobbyisten.

Er zijn advocatenkantoren, ook in Nederland, die een interne variant van Chat GPT ontwikkelen om te ondersteunen bij zaken. Ziet u hier ook heil in?

Wij houden natuurlijk de ontwikkelingen in de gaten. Dit zou ook uniform moeten worden geregeld, zoals een Legal Intelligence of Wolters Kluwer waar wij echt op kunnen vertrouwen. Dan kan het ontzettend waardevol zijn. Het lijkt mij niet handig om allemaal zelf intern als advocatenkantoor ermee aan de slag te gaan. Modellen moet je in een AI-systeem kunnen zetten. Het mooist is als dat gedaan kan worden door een onafhankelijke partij, zoals een Legal Intelligence of Wolters Kluwer. Daar zou ik meer vertrouwen in hebben. Anders ben ik bang dat je het gaat sturen op je eigen informatie. Kijk je dan wel genoeg verder? Hoe breder, hoe beter zou ik zeggen.

Om verder in te gaan op privacy. Kunt u ons vertellen wat u en het kantoor doen qua zaken op het gebied van privacy?

Zeker. De AVG wordt steeds bekender, waardoor ik minder privacy statements hoef op te stellen dan toen ik begon in 2020. Toch blijf je vragen houden over bijvoorbeeld de doorgifte van gegevens buiten de EER, het uitwisselen van gegevens tussen bedrijven, de verwerkersovereenkomsten en wat gebeurt er met gegevens als een bedrijf failliet gaat of wordt overgenomen? Dat loopt eigenlijk wel door.

Er worden steeds grotere boetes uitgedeeld door de AP en andere toezichthouders. Wordt het daardoor meer serieus genomen?

Ik denk eigenlijk niet dat het daaruit voortvloeit. Hoewel de boetes hoger worden, blijft de werkdruk gigantisch hoog bij de AP. Voordat jij degene bent die wordt gecontroleerd, hoe groot is die kans? Ik denk eerder dat wij als kantoren, consumenten en particulieren er meer mee bezig zijn. Daarom zijn bedrijven er ook meer mee bezig. Het steekt elkaar aan. Als jij een verwerkersovereenkomst moet tekenen, waarom iemand anders dan niet? Het is een balletje wat is gaan rollen heb ik het idee.

De technologische ontwikkelingen volgen elkaar razendsnel op. Is er in uw optiek een verschil, in bijvoorbeeld de onderwerpen van de zaken, toen u net begon in 2018 en nu, anno 2023?

Ik hoef bijvoorbeeld minder privacy statements op te stellen. Inmiddels heeft iedereen de basis van de AVG aardig in huis, heb ik het idee. Het is misschien voor mij ook lastig te beoordelen. Je leercurve is zo steil op het moment dat je begint als advocaat-stagiair. Je ontwikkelt je razendsnel. Het type zaken wordt sowieso anders. Komt het door de tijd of door de ervaring?

Zijn er in de afgelopen jaren in uw ervaring meer IT gerelateerde zaken geweest nu de techniek steeds dominanter wordt in de samenleving?

Ja, dat denk ik wel. Ook in combinatie met bijvoorbeeld het aanbestedingsrecht. Eerst was iedereen blij dat er überhaupt IT was. Men ging allerlei contracten aan. Nu denkt men meer: 'Ik wil ook zelf het IE-recht'. Je ziet dat bedrijven zich daar bewuster van worden. Ook zijn er meer alternatieven gekomen op de IT-markt. Je kan ook met andere bedrijven samenwerken die iets voor je kunnen realiseren, in plaats van de IT-leverancier waar je al jaren mee samenwerkt. Ik denk dat dat steeds meer naar voren komt, dat iedereen dat nu meer in eigen handen wilt hebben. Vroeger was het zo ongrijpbaar dat je het graag uit handen gaf. Het is wel over een langer tijdsbestek zo gekomen, niet slechts de afgelopen drie jaar. Het is een ontwikkeling.

Nu we het einde van het jaar naderen kan de top2000 niet ontbreken, welk nummer moet volgens u op nummer 1?

Ik heb geen idee. Doe maar een kerstliedje, daar houd ik van.

Mariah Carey?

Helemaal goed.

Nu we weer handschoenen en mutsen dragen, als afsluiter nog een stelling. Bent u een wintermens of een zomermens?

Een wintermens. Ik houd van kerstliedjes. Ik ga altijd op wintersport. En ik houd van kaarsjes aan binnen, de kerstboom, gezelligheid. Het is moeilijker opstaan, maar het is wel gezellig.

Namens de Carrièrecommissie,

Manon Hospers, Nathan Porsoufi en Chris Truong

De regulering en handhaving van online desinformatie

'Desinformatie tast het vertrouwen in instellingen en in de digitale en traditionele media aan en schaadt onze democratieën door het vermogen van burgers om beslissingen te nemen te belemmeren.' Dit stuk uit een document van de Europese Commissie verduidelijkt dat de

online misleiding die wij als internetgebruikers kennen in de vorm van phishing en identiteitsfraude niet het enige gevaar vormt op het internet.¹ Uit een onderzoek van het Sociaal en Cultureel Planbureau blijkt dat bijna de helft van de Nederlanders zich redelijk tot veel zorgen maakt om foutieve of misleidende informatie op het internet.² Daarnaast vindt bijna de helft van de Nederlanders dat van het recht op vrijheid van meningsuiting moet worden geweken bij desinformatie en dat de overheid of de EU tegen dit soort gevaarlijke informatie moet optreden.³

Desinformatie reguleren of toch toelaten blijkt een uiterst lastige kwestie. Als gebruiker van het internet roept deze problematiek de volgende vraag op: in hoeverre wordt de Nederlandse internetgebruiker beschermd tegen online desinformatie en op grond van welke juridische bronnen wordt deze informatie strafbaar gesteld?

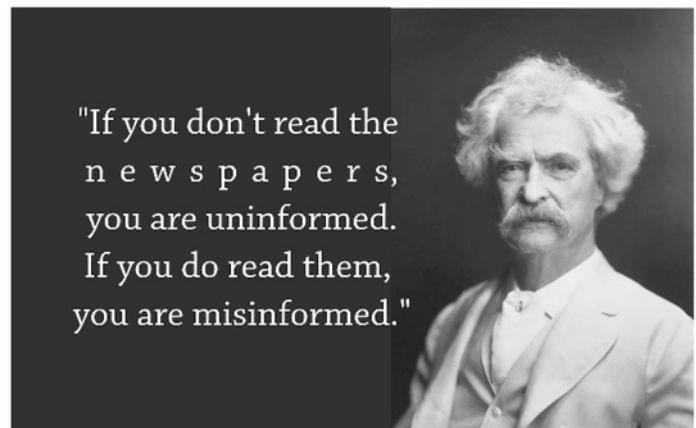
Deze vraag zullen wij in dit onderzoek beantwoorden door desinformatie te definiëren in het licht van hetgeen is vastgesteld en gehanteerd door de overheid en de Europese Unie. Vervolgens wordt er gekeken naar de huidige regulering van desinformatie, in het kader van de Nederlandse wetgeving, specifiek het straf- en privaatrecht en andere relevante Nederlandse- en EU-documenten. Er wordt ten slotte gekeken naar de handvaten die internetdocumenten bieden om zelf desinformatie te leren onderscheiden.

Definiëring desinformatie

De Nationaal Coördinator Terrorismebestrijding en Veiligheid heeft als taak om de gezamenlijke inzet op het gebied van nationale veiligheid te coördineren in Nederland. In een door hen opgesteld document, genaamd: 'Heb ik te maken met desinformatie?' wordt desinformatie als volgt gedefiniëerd: 'Het doelbewust verspreiden van misleidende

informatie, met het doel om schade toe te brengen aan het publieke debat, democratische processen, de open economie of nationale veiligheid'.⁴ 'Desinformatie hoeft niet alleen onjuiste informatie te bevatten. Het kan een combinatie zijn van feitelijke, aantoonbaar onjuiste of deels onjuiste informatie, maar altijd met de intentie om te misleiden en te schaden'.⁵

De impact van desinformatie kan verschillen per samenleving, maar kan ook afhankelijk zijn van opleidingsniveau, democratische cultuur, vertrouwen in de instituties en sociale en economische ongelijkheden.⁶ Onderscheid maken tussen desinformatie, misinformatie en malinformatie is in het licht van dit onderzoek van belang.⁷ Misinformatie heeft niet als doel om schade aan te richten, waardoor parodieën, satire, roddels en kritiek niet vallen onder desinformatie.⁸ Malinformatie daarentegen is niet fictief, maar heeft wel als doel om schade aan te richten.⁹



Juridische definiëring desinformatie

Desinformatie valt onder de vrijheid van meningsuiting in de zin van artikel 7 van de Grondwet, artikel 10 van het Europees Verdrag voor de Rechten van de Mens en artikel 11 van het Handvest van de Europese Unie.¹⁰ Vrijheid van meningsuiting betekent op grond van artikel 11 van het Handvest van de grondrechten van de Europese Unie het recht 'een mening te hebben en de vrijheid kennis te nemen en te geven van informatie of ideeën, zonder inmenging van enig openbaar gezag en ongeacht grenzen.'

De voornaamste taak van overheden met betrekking

1 Europese Commissie, 'Tackling online disinformation: a European Approach, COM(2018) 236 final', par. 1

2 'Helft Nederlanders bezorgd over online gedrag en misinformatie', scp.nl, 31 augustus 2023.

3 M. Albers, 'Nederlanders bezorgd over misinformatie op sociale media, grote meerderheid wil dat overheid ingrijpt', *Volkscrant* 31 augustus 2023.

4 *Kamerstukken II* 2019/20, 30821, nr. 91.

5 Handreiking heb ik te maken met desinformatie.

6 COM/2018/236 final.

7 In dit onderzoek zal enkel worden ingegaan op de door de Rijksoverheid gehanteerde definitie van 'desinformatie'

8 Handreiking omgaan met desinformatie.

9 Wardle & Derakhshan, 2017, p. 20.

10 Handleiding omgaan met desinformatie par. 2.2.

tot vrijheid van meningsuiting is om zich te onthouden van inmenging en censuur en ervoor te zorgen dat er een juist klimaat is voor het publieke debat.¹¹ Het recht op vrijheid van meningsuiting is in beginsel onbeperkt, tenzij er gepropageerd wordt met geweldgebruik of er wordt aangezet tot discriminatie, haat of nodeloze belediging.¹²

Juridische regulering desinformatie

Desinformatie kent in het Nederlandse recht geen zelfstandige juridische definitie, maar vindt zijn wettelijke begrenzing in verschillende wetten. Zo kan desinformatie vallen onder strafrechtelijke delicten, zoals propaganda van geweldgebruik en het aanzetten tot discriminatie, haat of nodeloze belediging. Desinformatie kan ook strafbaar gesteld worden bij een geslaagd beroep op privaatrechtelijke gronden, zoals de onrechtmatige daad en het intellectueel eigendomsrecht.¹³ Hierbij is van belang om te bepalen of de uiting strafbaar is. Indien de uiting gedefinieerd wordt als strafbaar, doordat het bijvoorbeeld aanzet tot geweld in de zin van artikel 137d eerste wetboek van Strafrecht is het mogelijk om aangifte hiertegen te doen bij de politie of een verzoek tot vervolging bij het Openbaar Ministerie in te dienen. Op grond van het civielrecht kan worden gedacht aan een procedure op grond van onrechtmatige daad wegens reputatieschade.¹⁴ Indien we kijken naar de huidige regulering op Europees niveau, moet de internetgebruiker beschermd worden tegen desinformatie door de invoering van de Europese Digital Service Act (hierna: DSA), die in werking is getreden in november 2022. De DSA geldt voor grote online platformen, zoals Booking.com, Apple, Google en AliExpress. De 'Act' verplicht deze grote online platformen om gericht de desinformatie die via hun diensten wordt verspreid aan te pakken en hiertegen maatregelen te nemen. Bij overtreding van de DSA krijgt het bedrijf een boete ter hoogte van zes procent van hun wereldwijde jaaromzet of dwangsommen die tot vijf procent van hun gemiddelde dagelijkse inkomsten zullen kosten. Vanaf februari 2024 zullen deze regels ook gelden voor andere veel gebruikte online marktplaatsen, zoekmachines, internetproviders etcetera.¹⁵

Hoe kan de internetgebruiker zichzelf beschermen tegen desinformatie?

Zoals hierboven is beschreven, biedt nationale en Europese wetgeving bescherming aan de internetgebruiker tegen desinformatie. Overheden hechten in de praktijk grote waarde aan grondrechten, waaronder de vrijheid van meningsuiting. Dit belang blijkt uit een Kamerbrief van oktober 2019.¹⁶ Deze Kamerbrief betreft het beleid van de overheid omtrent bescherming van de democratie tegen desinformatie. Het uitgangspunt van dit beleid is dat de vrijheid van meningsuiting en de pers voorop staan en de verantwoordelijkheid voor het aanwijzen van desinformatie ligt bij de media en factcheckers. In een aanvulling op dit beleid in een Kamerbrief uit december 2022 komt een nieuwe strategie voor het beschermen van het vrije en open publieke debat tegen desinformatie aan het licht. Deze strategie heeft twee uitgangspunten: het versterken van het vrije en open publieke debat en het verminderen van de invloed van desinformatie. Als wij kijken naar het eerste uitgangspunt is het doel om de nadruk te leggen op het behouden van het pluriforme medialandschap. Daarnaast ligt de nadruk op de weerbaarheid van burgers te versterken en gebruik te maken van publieke alternatieven voor online platformen. Het verminderen van de invloed van desinformatie moet plaatsvinden door een stel maatregelen afhankelijk van vier gronden: de inhoud van de desinformatie, de producent of verspreider, de verantwoordelijkheden van sociale en traditionele media en ten slotte op meer overkoepelende kennisontwikkeling.¹⁷ Ondanks deze initiatieven vanuit de overheid, zal de internetgebruiker zichzelf ook moeten beschermen tegen de invloeden van desinformatie. Maar hoe kan je jezelf beschermen tegen online desinformatie?



De overheid biedt de internetgebruiker ondersteuning met een online checklist. Zo vind je op de site van de Rijksoverheid de checklist 'Is die informatie

11 COM/2018/236 final.

12 Handreiking omgaan met desinformatie.

13 Rapport het juridisch kader voor de verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties 2019.

14 Lestrade en Kouwenberg, 2022.

15 'DSA: verplichtingen voor en toezicht op allergrootste online platforms ingegaan', Rijksoverheid.nl.

16 Kamerbrief over beleidsinzet bescherming tegen desinformatie.

17 Kamerbrief rijksbrede strategie effectieve aanpak van desinformatie.

echt?'.¹⁸ Hierin worden tips gegeven om berichtgeving kritisch te onderzoeken. Er worden video's gedeeld waarin informatie wordt gegeven over hoe je 'deepfakes' kunt herkennen. Ook wordt er verwezen naar sites die informatie van het internet kunnen onderzoeken op de feitelijkheid, zoals de site: 'Isdatechtzo.nl'. Daarnaast heeft de NCTV een handreiking opgesteld genaamd: '*Heb ik te maken met desinformatie?*'. Deze handreiking is ter ondersteuning voor het signaleren van desinformatie en bevat onder andere een beoordelingsformulier en een voorbeeldcasus.¹⁹ Aan de hand van het beoordelingsformulier is de internetgebruiker in staat om nauwkeurig te bepalen of er desinformatie wordt verspreid of niet en door de casus krijgt hij een beter idee hoe dit beoordelingsformulier gehanteerd moet worden. Al met al een nuttig en bruikbaar bestand in de strijd tegen desinformatie.

Tegenwoordig zijn er ook onafhankelijke organisaties die ondersteuning willen bieden aan de internetgebruiker. Psychologen van de universiteit van Cambridge en Bristol maakten animatiefilmpjes met uitleg over manipulatie en desinformatie. Na experimenten bleek dat door gebruik van deze animatiefilmpjes kijkers twee keer zo goed de desinformatie konden herkennen.²⁰

Wellicht zouden deze filmpjes een oplossing kunnen bieden, nu de drempel voor het kijken van een kort filmpje minder hoog is dan het afgaan van een beoordelingsformulier. De vraag blijft alleen of grootschalige toepassing hiervan mogelijk is.

Conclusie

De overheid en de bevolking van Nederland lijken pal tegenover elkaar te staan in de strijd tegen desinformatie. Waar de overheid zich lijkt vast te klemmen aan de grondrechten, ziet de internetgebruiker zich verliezen in de schijn van realiteit van online informatie. Deze desinformatie valt onder de definitie van vrijheid van meningsuiting. De grondrechtelijke aard hiervan maakt het echter lastig voor de internetgebruiker om dit recht te beperken.

Om een zekere rechtszekerheid te bieden kan de internetgebruiker zich bij desinformatie in bijzondere gevallen beroepen op verschillende strafrechtelijke en privaatrechtelijke wetten. De Europese Unie probeert de internetgebruiker op zijn eigen manier te beschermen. Met de recente invoering van de DSA

worden grote online platformen gesanctioneerd, indien zij bescherming tegen desinformatie onvoldoende handhaven. Nu het aantal diensten die vallen onder de DSA per februari 2024 wordt vergroot, lijkt deze 'Act' een weldegelijk handvat te bieden ter bescherming.

Het internet zelf biedt, hoe ironisch dat wellicht klinkt, zelf ook handvaten aan de gebruiker om desinformatie te onderscheppen. Zo zijn er checklists, beoordelingsformulieren en zelfs voorbeeldcasussen te vinden om als gebruiker een kritisch oog te 'kweken' ten aanzien van de informatie die zij online tegenkomen. Deze informatie wordt aangeboden vanuit verschillende overheidsinstanties, wellicht als tegenprestatie voor hetgeen de Nederlandse bevolking prioriteert. Onafhankelijke internationale organisaties proberen zelfstandig de strijd tegen desinformatie aan te pakken, door informatieve video's te produceren en experimenten af te nemen.

Concluderend uit ons onderzoek blijft de kwestie rondom desinformatie lastig. Het voortouw om desinformatie te onderscheiden van de werkelijkheid lijkt voornamelijk nog bij de gebruiker zelf te liggen. Wij betwijfelen of in de snelgroeiende wereld van het internet de overheid in staat zal zijn om de internetgebruiker geheel juridisch te beschermen tegen desinformatie, waardoor het belang van zelfregulering door online platformen en de verspreiding van kennis omtrent dit onderwerp bij gebruikers zelf in onze ogen de prioriteit moet krijgen.

Namens de Carrièrecommissie,

Esther Bergsma

18 'Checklist 'Is die informatie echt'', Rijksoverheid.nl.

19 Handreiking heb ik te maken met desinformatie?

20 S. de Jong, 'Met korte filmpjes vooraf kun je mensen bestand maken tegen online desinformatie', NRC 24 augustus 2022.

Een blik op de nieuwe Digital Services Act en Digital Markets Act.

'Meerdere Oostenrijkers opgenomen na gebruik vervalste diabetesmedicijn' kopte RTL-nieuws afgelopen oktober. De Oostenrijkers zouden last hebben gehad van een zogenaamde 'hypo' waarna zij onwel werden. De oorzaak: het gebruik van vervalste Ozempic-pennen. Zonder directe medische hulp kan het gebruik van zulke valse pennen zelfs leiden tot de dood.¹ Ozempic is een medicijn dat gebruikt wordt door diabetespatiënten, maar afgelopen tijd was het ook een enorme hit op TikTok. Door het verminderen van de eetlust zou het namelijk kunnen helpen bij het afvallen.² In Nederland kan Ozempic alleen met recept worden afgehaald worden bij de apotheek³, steeds vaker is het ook online verkrijgbaar bij webshops zoals AliExpress.⁴ Uit onderzoek van de Consumentenbond uit 2022 blijkt dat op dat moment de helft tot tweederde van de producten bij populaire buitenlandse webwinkels niet voldoen aan de Europese veiligheidseisen.⁵ Het kan dus maar zo zijn dat je net als de Oostenrijkers een medicijn koopt dat niet aan de (Europese) eisen voldoet. Eerder dit jaar waarschuwde medicijnautoriteit CBG daarom al om het medicijn niet zonder toezicht van een arts te gebruiken.⁶ Ook waarschuwde Eurocommissaris voor de Interne Markt Thierry Breton al voor het feit dat er steeds meer 'valse en potentieel levensbedreigende medicijnen' te koop zijn in webwinkels als AliExpress.⁷

Na goedkeuring van de richtlijn inzake elektronische handel in 2000 is het rechtskader voor

- 1 'Meerdere Oostenrijkers opgenomen na gebruik vervalst diabetesmedicijn', rtlnieuws.nl, 24 oktober 2023.
- 2 'How is TikTok's #Ozempic trend impacting diabetes patients?', newsmedical.net, 5 oktober 2023.
- 3 'Semaglutide', apotheek.nl, 3 mei 2023.
- 4 'Brussel wil opheldering AliExpress over nepmedicijnen', nieuws.nl, 6 november 2023.
- 5 'Onveilige producten bij buitenlandse webshops', consumentenbond.nl, 21 januari 2022.
- 6 'Aanhoudend tekort diabetesmedicijn Ozempic', cbg-med.nl, 17 november 2023.
- 7 'Brussel wil opheldering AliExpress over nepmedicijnen', nieuws.nl, 6 november 2023.

digitale diensten van de EU niet meer veranderd. Terwijl de technologie zich de afgelopen twintig jaar onwils heeft ontwikkeld. Als antwoord hierop heeft de Europese Commissie zowel de Digital Services Act (hierna: DSA) als de Digital Markets Act (hierna: DMA) opgesteld.⁸ Zo probeert de DSA de grondrechten van de gebruikers te beschermen in een online omgeving, zoals door het tegengaan van de verkoop van valse medicijnen als valse Ozempic-pennen.⁹ De DMA heeft als doel de sterke economische positie van grote digitale platforms aan te pakken. Dat moet bijdragen aan een goede werking van de interne markt.¹⁰ Wij zullen u in dit artikel meenemen langs beide verordeningen. Wij zullen eerst ingaan op de vraag wat de DSA inhoudt. Vervolgens zullen wij uiteenzetten voor wie de DSA nu geldt. Daarna zullen wij uiteenzetten voor wie de DSA in de toekomst zal gelden. We ronden de DSA af met een stuk over handhaving van de DSA. Na de DSA zal de DMA worden behandeld. Deze zal net als de DSA eerst uitgelegd worden, daarna wordt ingegaan op de handhaving ervan. Het artikel wordt afgesloten met een conclusie.



Wat houdt de DSA in?

Digitale diensten hebben op allerlei manieren onze levens beïnvloed en vergemakkelijkt. We gebruiken ze als communicatiemiddel, bij

- 8 'Digitale dienstenverordening (DSA) definitief vastgesteld', ecer.minbuza.nl, 1 november 2022.
- 9 Verordening (EU) 2022/2065.
- 10 'Digital Markets Act: concurrentieregels grootste digitale platforms van start', rijksoverheid.nl, 1 mei 2023.

het boeken van hotels, om online te shoppen, enzovoort. Echter, er zijn ook problemen. Zoals de uitwisseling van en handel in illegale goederen, online inhoud en diensten. Ook kunnen de diensten worden misbruikt door algoritmische systemen voor de verspreiding van desinformatie en andere kwaadaardige bedoelingen.¹¹

Het doel van de DSA is het creëren van een voorspelbare, veilige en betrouwbare digitale ruimte waarin van alle gebruikers van onder de DSA vallende diensten de grondrechten worden beschermd en de verspreiding van illegale online inhoud en de maatschappelijke risico's die horen bij de verspreiding van desinformatie of andere inhoud worden aangepakt.¹² Daarbij is illegale inhoud een breed begrip. Voorbeelden van illegale inhoud zijn het zonder toestemming delen van privébeelden, de verkoop van namaakproducten, het onbevoegd gebruik van auteursrechtelijk beschermd materiaal en het delen van beelden van seksueel misbruik van kinderen.¹³ Met bijna 100 artikelen probeert de DSA dit doel te verwezenlijken.¹⁴ Wij zullen niet alle artikelen behandelen, maar de belangrijkste punten op een rijtje zetten.

- Jaarlijkse rapportage. Op zijn minst één keer per jaar moet de aanbieder een rapport opstellen en publiceren over de inhoudsmoderatie. Hierin staat onder andere vermeld hoeveel bevelen het van de autoriteiten heeft gekregen, het aantal accounts dat (tijdelijk) zijn verwijderd of geblokkeerd en het gemiddeld aantal gebruikers van het platform per Europese lidstaat.
- Duidelijkheid in algemene voorwaarden. Daarin moet worden neergelegd wat de procedures, het beleid, de maatregelen en instrumenten zijn voor de inhoudsmoderatie. Bijvoorbeeld bij pestgedrag, aanstootgevende informatie en extreme

politieke opvattingen.

- Aanpakken van dark patterns. Bij dark patterns wordt het vermogen van een gebruiker verstoord om een eigen en weloverwogen keuze te maken. Met de DSA mogen aanbieders niet hun dienst zodanig ontwerpen dat gebruikers daarin worden misleid of gemanipuleerd.
- Transparantie. Er wordt meer transparantie geëist bij onder andere aanbevelingssystemen (dit systeem wordt gebruikt om bepaalde informatie onder aandacht te brengen van een gebruiker; bijvoorbeeld For You op TikTok) en reclame. De aanbieders moeten aangeven wat de belangrijkste parameters zijn voor het systeem en welke opties de gebruiker heeft om dit aan te passen. Daarnaast moeten ze invloed kunnen uitoefenen door bijvoorbeeld een voorkeursoptie. Verder moet er bij reclame worden aangegeven dat het om reclame gaat, waarom en namens wie de reclame aan de gebruiker wordt getoond.¹⁵
- Geen personalisatie op basis van bijzondere persoonsgegevens. Advertenties mogen niet langer gepersonaliseerd worden op basis van persoonsgegevens die betrekking hebben op de politieke voorkeur, gezondheidsinformatie, seksuele geaardheid, geloofsovertuiging of ras.
- Betere bescherming minderjarigen. Aanbieders van tussenhandeldiensten die zich richten of voornamelijk worden gebruikt door minderjarigen dienen zichzelf uit te leggen in een taal die voor minderjarigen begrijpelijk is. Daarnaast dienen diensten die toegankelijk zijn voor minderjarigen een hoog niveau van privacy, bescherming en veiligheid te hebben en er geldt voor die platforms een verbod op reclame door middel van hun persoonsgegevens.¹⁶
- Aanwijzing van een centraal contactpunt. Via dit contactpunt kan er met de autoriteiten over de communicatie worden

11 'Het pakket digital services act', digital-strategy. ec.europa.eu.

12 Beleidskompasformulier voor internetconsulatie bij Uitvoeringswet digitale dienstenverordening.

13 'Praktische gevolgen van de nieuwe EU regels over de digitale diensten en markten', seeds.law.nl, 8 mei 2023.

14 'The final text of the Digital Services act', ec.europa.eu, 27 oktober 2022.

15 'Een veilige en transparante Europese markt: Digital Services Act', vpn.gids.nl, 6 februari 2023.

16 'Digitale dienstenverordening (DSA) definitief vastgesteld', ecer.minbuza.nl, 1 november 2022.

gecommuniceerd. De autoriteiten stellen vragen aan dit contactpunt na bijvoorbeeld meldingen van illegale inhoud.¹⁷

- Melding strafbare feit bij nationale instantie. Op het moment dat uit informatie kan worden afgeleid dat er een strafbaar feit is gepleegd.¹⁸

Naar aanleiding van de oorlog in Oekraïne die onder andere gekenmerkt wordt door desinformatie en schending van mensenrechten is ook de 'crisis response mechanism' opgenomen in de DSA. Dit systeem maakt het mogelijk te analyseren wat de impact van de zeer grote online platforms en zeer grote zoekmachines is op de crisis. Naar aanleiding hiervan kan besloten worden effectieve en proportionele maatregelen te nemen voor de eerbiediging van de fundamentele rechten.

Voor wie geldt de DSA nu?

Sinds afgelopen augustus moeten zeventien zeer grote onlineplatforms en twee zeer grote onlinezoekmachines al voldoen aan de DSA. Dit zijn diensten met maandelijks meer dan 45 miljoen actieve Europese gebruikers, berekend als gemiddelde over een periode van zes maanden. Hierbij heeft de zoekmachine Google Search het grootste aantal actieve maandelijkse Europese gebruikers. Verder gaat het onder meer om Meta (eigenaar van Instagram en Facebook), Apple, LinkedIn, TikTok, YouTube, AliExpress, Booking.com, X en Zalando.¹⁹ Afgelopen juni heeft laatstgenoemde de classificatie aangevochten bij het Europese Hof van Justitie. Zalando heeft onder andere aangevoerd dat zij niet aangemerkt kan worden als zeer groot onlineplatform zoals is neergelegd in de DSA. Ze zouden niet de vereiste 45 miljoen actieve maandelijkse Europese gebruikers bereiken. Daarnaast zou de gebruikte methode om het aantal gebruikers te berekenen onduidelijk zijn en leiden tot ongelijke behandeling van de online platforms. Er is nog geen uitspraak in de zaak geweest. Op dit moment conformeert

Zalando zich dan ook niet aan de voorschriften van de DSA.²⁰ Ook Amazon zette vraagtekens bij hun plek op de lijst van zeer grote onlineplatforms. Amazon heeft dan ook een verzoek ingediend tot opschorting van deze aanduiding en andere (tijdelijke) maatregelen bij het Europese Hof van Justitie. Volgens Amazon zou specifiek artikel 39 van de DSA er onder andere voor zorgen dat vertrouwelijke informatie over zowel Amazon als zijn adverteerders onthuld zouden worden. Daarmee zouden derde partijen inzicht krijgen in cruciale bedrijfsgeheimen over de advertentiestrategieën van Amazon. Dit zou weer kunnen leiden tot onherstelbare schade stelt het bedrijf. Naar aanleiding van dit verzoek werd voor Amazon dit artikel van de DSA tijdelijk opgeschort door de President van het Europese Hof van Justitie, Marc van der Woude. De belangen van Amazon hebben prioriteit gekregen, tenminste totdat beslist is in de hoofdzaak. Op het moment van schrijven geldt deze opschorting alleen voor Amazon.²¹



Daarnaast gelden door het grote aantal maandelijkse Europese gebruikers voor de zeer grote online platforms en zeer grote zoekmachines nog extra strenge regels. Zo dienen ze onder andere (i) gebruikers een systeem aan te bieden voor aanbevolen content dat niet gebaseerd is op profilering en (ii) risico's die ze creëren te analyseren en aan te pakken. Dit zijn risico's met betrekking tot verspreiding van desinformatie, negatieve effecten op verkiezingen en fundamentele rechten, illegale inhoud, gendergerelateerd geweld of de geestelijke gezondheid.²² Verder dienen zij jaarlijks een rapport op te stellen waarin zij onder an-

17 *Kamerstukken II 2020/21, 22 112, nr. 3049.*

18 *Kamerstukken II 2020/21, 22112, nr. 3050.*

19 Verordening (EU) 2022/2065.

Mededelingen en bekendmakingen, p. 9 t/m 11.

20 'Zalando stapt naar de rechter: 'Wij willen niet geassocieerd worden met techreuzen, nos.nl, 27 juni 2023.

21 Gerecht EU 27 september 2023, ECLI:EU:T:2023:589 (*Amazon Services Europe v Commission*)

22 'Digitale dienstenverordening (DSA) definitief vastgesteld', ecer.minbuza.nl, 1 november 2022.

dere informatie geven over de beoordeling van de dienst op het risico van het verspreiden van illegale inhoud en negatieve effecten op fundamentele rechten, volksgezondheid, openbare inhoud. Daarnaast moeten ze ten minste één keer per jaar worden gecontroleerd door een externe partij (op eigen kosten) op hoe ze de wet uitvoeren. Tot slot kunnen de Europese Raad voor digitale diensten en de Europese Commissie op eigen initiatief onderzoek doen. De dienst dient dan informatie te verstrekken als daar om wordt verzocht.

De DSA in de toekomst

Vanaf februari 2024 geldt de DSA voor alle aanbieders van online 'tussenhandelsdiensten'. Tussenhandelsdiensten zijn online diensten waarbij communicatie tussen gebruikers mogelijk is, bijvoorbeeld online marktplaatsen, socialmediadiensten, online platforms en internetaanbieders. Niet alle digitale diensten vallen daarbij onder de DSA. Daarnaast wordt er gekeken naar de diensten, niet zozeer om de entiteit van de aanbieder. Het kan dus zijn dat een aantal diensten van de aanbieder eronder vallen, maar niet alle.

Verder gaat het om aanbieders van tussenhandelsdiensten die worden verleend aan gebruikers (natuurlijke personen of rechtspersonen) die gevestigd zijn in de Europese Unie of zich daar bevinden.²³ De aanbieder moet zich aan de DSA houden als er sprake is van een reële band met de Europese Unie. Kenmerken hiervan zijn onder andere dat een groot aantal gebruikers zich bevindt in één of meerdere Europese lidstaten, de dienstverlener heeft een vestiging in de Europese Unie en je producten kan bestellen vanuit de Europese Unie. In principe is het niet van belang waar de aanbieder zich bevindt. De DSA maakt daarbij nog onderscheid tussen drie verschillende tussenhandelsdiensten: mere conduitsdiensten, hostingdiensten en cachingdiensten. Het zijn kort gezegd diensten waar het opslaan en doorgeven van informatie van gebruikers centraal staat.²⁴ Wij zullen niet ingaan op de verschillende tussenhandelsdiensten in verband met de grootte van het artikel.

23 Verordening (EU) 2022/2065.

24 Kamerstukken II 2020/21, 22112, nr. 3050.

Als je verder inzoomt op de DSA wordt duidelijk dat de DSA bestaat uit een gelaagde structuur die te vergelijken is met een piramide van vier lagen. De breedste, onderste laag van de piramide is van toepassing op *alle* tussenhandelsdiensten. Daarboven bevindt zich een laag die alleen van toepassing is op hostingdiensten. De daaropvolgende laag heeft betrekking op de onlineplatforms. De bovenste laag heeft betrekking op de zeer grote onlineplatforms en zeer grote zoekmachines. Hierbij wordt er gekeken naar de grootte van de dienst, niet naar de aard van de dienst. Verder verdient opmerking dat de DSA cumulatief is wanneer een dienst in een laag overlapt met een andere laag. Zo kan een zeer groot onlineplatform onder alle categorieën vallen. Dat betekent dat alle verplichtingen van zowel *alle tussenhandelsdiensten*, *hostingsdiensten*, *onlineplatforms* en *zeer grote onlineplatforms* van toepassing zijn.

Handhaving van de DSA

Om de DSA te handhaven dient iedere Europese lidstaat een of meer bevoegde autoriteiten aan te wijzen die verantwoordelijk zijn voor toepassing van de DSA. Daarbij zal één van deze autoriteiten optreden als coördinator voor digitale diensten. Deze coördinator is verantwoordelijk voor het toepassen en handhaven van de DSA. In Nederland zal vanaf 17 februari 2024 de Uitvoeringswet digitaaldienstenverordening ingaan om uitvoering te geven aan de DSA. In deze wet is de Autoriteit Consument & Markt (hierna: ACM) aangewezen als digitale dienstencoördinator en als toezichthouder voor het grootste deel van de DSA. De ACM heeft hierbij zowel handhavings- als onderzoeksbevoegdheden.²⁵ Verder is de Autoriteit Persoonsgegevens (hierna: AP) aangewezen als andere bevoegde toezichthouder.²⁶

In beginsel is de autoriteit van de lidstaat van de hoofdvestiging van de betrokken aanbieder exclusief bevoegd voor het onderzoek. Als

25 'ACM bereidt zich voor op toezicht nieuwe EU-regels digitale economie', acm.nl, 14 april 2023.

26 Advies Uitvoeringswet digitaaldienstenverordening 2023, p.1.

Google dus in Nederland zijn verplichtingen uit de DSA niet nakomt dient de coördinator aan de Ierse autoriteit (waar de hoofdvestiging staat) te vragen een onderzoek in te laten stellen. De Ierse autoriteit heeft vervolgens twee maanden om de kwestie te onderzoeken. Als na twee maanden het onderzoek niet is afgerond, kan de coördinator direct naar de Europese Commissie. Als het gaat om DSA-verplichtingen die uitsluitend gelden voor de zeer grote online-platforms en zeer grote zoekmachines is de Europese Commissie exclusief bevoegd. Bij alle overige DSA-verplichtingen zijn zowel de Europese Commissie als de lidstaat bevoegd. Hierbij heeft de Europese Commissie voorrang.²⁷

Wat houdt de DMA in en voor wie geldt het?

Vanaf maart 2024 moeten 6 digitale platforms met 22 van hun diensten aan de DMA voldoen. Het gaat hierbij om Alphabet, Amazon, Apple, ByteDance, Meta en Microsoft. Hier vallen onder andere TikTok, Appstore, Facebook en Whatsapp onder.²⁸ Deze platforms zijn op basis van onderzoek en cijfers aangewezen als zogenaamde 'poortwachters' door de Europese Commissie. Hiervoor moet het aan drie voorwaarden voldoen: (i) sterke positie op de Europese markt. (ii) Het platform heeft al lange tijd een sterke positie op de markt. (iii) Sprake van een kernplatformdienst (bijv. een videoplatform, zoekmachine of online advertentiedienst). Deze poortwachters hebben zo'n omvang dat gebruikers er nauwelijks omheen kunnen; een zogenaamde poortwachterspositie.²⁹

Minister Micky Adriaansens (Economische Zaken en Klimaat): "Deze Europese regels geven ondernemers van klein tot groot meer groeikansen, bevorderen eerlijke concurrentie en beschermen consumenten beter. We zijn door de DMA straks ook minder afhankelijk van deze 6 allergrootste platforms en hun diensten. Daardoor kunnen ondernemers beter zaken doen via het internet en kunnen consumenten gemakke-

*lijker producten kopen en verkopen."*³⁰

In de DMA zijn allerlei gedragsregels en verplichtingen opgelegd voor de platforms om aan deze doelstelling te voldoen. Voorbeelden zijn:

- Eindgebruikers moeten gemakkelijk hun instellingen kunnen wijzigen.
- Eigen diensten van de poortwachter mogen niet bevoordeeld worden ten opzichte van soortgelijke diensten van derden op het platform van de poortwachter door ze bijvoorbeeld bovenaan de zoekresultaten te zetten.
- Het platform mag de gebruiker niet verplichten een ondersteunende dienst van de poortwachter te gebruiken bij afname van de kernplatformdienst van die poortwachter.

Handhaving

Anders dan bij de DSA is de Europese Commissie als enige bevoegd de DMA te handhaven. Het kan daarbij wel samenwerken met nationale mededingingsautoriteiten. Boetes en sancties kunnen oplopen tot 10% van de wereldwijde omzet van een onderneming en zelfs tot 20% in geval van herhaling. Daarnaast kan de Europese Commissie marktonderzoeken verrichten.³¹

Conclusie

Samenvattend gaat de DSA proberen een veilige, voorspelbare en betrouwbare online omgeving te creëren. Op dit moment geldt de DSA voor zeventien zeer grote onlineplatforms en twee zeer grote zoekmachines. Aan deze platforms en zoekmachines zijn naast de algemene vereisten ook extra strenge regels gesteld. Vanaf volgend jaar februari geldt de DSA voor alle tussenhandelsdiensten met een reële band met de Europese Unie. De verplichtingen dienen gehandhaafd te worden door de

27 'Een veilige en transparante Europese markt: Digital Services Act', vpn.gids.nl, 6 februari 2023.

28 'About Digital Markets Act', ec.europa.eu, z.d.

29 'Digital Markets Act': commission designates six gatekeepers', ec.europa.eu, z.d.

30 'Digitale Markets Act: concurrentieregels grootste platforms van start', rijksoverheid.nl, 1 mei 2023.

31 Verordening (EU) 2022/1925.

autoriteiten van de lidstaat, in Nederland is dat de AP en voornamelijk de ACM. Verder heeft de Europese Commissie de bevoegdheid om een onderzoek in te stellen.

Vanaf maart 2024 geldt ook voor 6 digitale platforms de DMA. De DMA probeert de machtspositie van de poortwachters onder controle te houden. Dit probeert de DMA te doen door allerlei gedragsregels en verplichtingen. De Europese Commissie heeft de exclusieve bevoegdheid de DMA te handhaven.

Niet alle platforms dienen al te voldoen aan de DSA en DMA. Het is daarom te vroeg om te zeggen wat de daadwerkelijke effecten zijn van de DSA en DMA. Wij hebben ook slechts een korte blik gegeven op de verordeningen. Daarbij hebben wij mogelijke kritiek op de verordeningen niet behandeld in het artikel. Daar is het artikel simpelweg te klein voor. Het is te optimistisch om te stellen dat er volledig sprake zou zijn van een veilige, voorspelbare en betrouwbare omgeving, maar na 20 jaar zonder nieuwe wetgeving voor digitale diensten zijn de DSA en DMA in ieder geval belangrijke stappen vooruit. Wellicht over een aantal maanden, als er voldaan moet worden aan beide verordeningen, dat wij meer kunnen zeggen over de effecten van de verordeningen. Wie weet komen wij dan bij u terug met betrekking tot de DSA en de DMA.

Namens de Carrièrecommissie,

Manon Hospers